Jenna Andersson

Organisaation hyvä tietoturvan sääntely-järjestelmä

ACTA WASAENSIA 536

Vaasan yliopisto
UNIVERSITY OF VAASA

Copyright © Vaasan yliopisto ja tekijä.

ISBN 978-952-395-149-5 (painettu)
978-952-395-150-1 (verkkoaineisto)

ISSN 0355-2667 (Acta Wasaensia 536, painettu)
2323-9123 (Acta Wasaensia 536, verkkoaineisto)

URN http://urn.fi/URN:ISBN:978-952-395-150-1

Hansaprint Oy, Turenki, 2024.

VÄITÖSKIRJA

joka Vaasan yliopiston laskentatoimen ja rahoituksen akateemisen yksikön suostumuksella esitetään julkisesti tarkastettavaksi perjantaina 11. lokakuuta 2024, kello 12.

Monografiaväitöskirja,

Laskentatoimen ja rahoituksen akateeminen yksikkö

Talousoikeuden oppiaine

Tekijä	Jenna Andersson
Ohjaajat	OTT, KTT, professori Vesa Annola Vaasan yliopisto. Laskentatoimen ja rahoituksen akateeminen yksikkö, talousoikeus.
	OTT, oikeustieteen professori (emeritus) Asko Lehtonen Vaasan yliopisto. Laskentatoimen ja rahoituksen akateeminen yksikkö, talousoikeus.
	KTT, immateriaalioikeuden yliopistonlehtori (emerita) Brita Gyllenbögel Vaasan yliopisto. Laskentatoimen ja rahoituksen akateeminen yksikkö, talousoikeus.
Kustos	OTT, KTT, professori Vesa Annola Vaasan yliopisto. Laskentatoimen ja rahoituksen akateeminen yksikkö, talousoikeus.
Esitarkastajat	OTT, yksityisoikeuden professori (emeritus), Ahti Saarenpää Lapin yliopisto. Oikeustieteiden tiedekunta, oikeusinformatiikan instituutti.
	OTT, LT, terveysoikeuden professori Lasse Lehtonen Helsingin yliopisto. Lääketieteellinen tiedekunta, kansanterveystieteen osasto.
Vastaväittäjä	OTT, yksityisoikeuden professori (emeritus), Ahti Saarenpää Lapin yliopisto. Oikeustieteiden tiedekunta, oikeusinformatiikan instituutti.

Tiivistelmä

Tietoturvallisuuden merkitys on kasvanut teknologian kehittymisen, digitalisoitumisen ja globalisaation myötä. Kybertoimintaympäristöömme kohdistuu uhkia, joilla on merkittäviä vaikutuksia organisaatioiden toimintaan, yhteiskunnan toimivuuteen ja yksilöiden oikeuksiin. Nykyisessä, järjestelmäriippuvaisessa verkkoyhteiskunnassa tulee olla sellainen organisaatioiden tietoturvan sääntelyjärjestelmä, joka suojaa tehokkaasti yksilöiden henkilötietoja ja muita oikeuksia sekä organisaatioiden luottamuksellisia tietoja ja jatkuvuutta. Tässä tutkimuksessa muodostetaan ja määritellään voimassa olevan lainsäädännön nojalla organisaatioiden hyvä tietoturvan sääntelyjärjestelmä. Tutkimuksessa kootaan yhteen ja systematisoidaan lukuisat organisaatioiden tietoturvaa koskevat säännökset, joita arvioidaan organisaatioiden hyviä tietoturvakäytänteitä ja käytännesääntöjä vasten. Näin tutkimuksessa esitetään lainsäädännön hyvän tietoturvatavan muodostama kokonaisuus. Tutkimustehtävän toteuttaminen edellyttää nykyisen tietoturvan sääntelyjärjestelmän sisällön ja tehokkuuden sekä yleisen tietoturvalain säätämistarpeen arviointia. Tutkimuksessa esitetään kaksi tutkimuskysymystä: 1) onko nykyinen organisaatioiden tietoturvan sääntelyjärjestelmä hyvä ja 2) onko Suomessa tarpeen kansallinen tietoturvalaki? Tässä oikeusdogmaattisessa tutkimuksessa on myös ongelmakeskeisen lainopin ja *de lege ferenda* -tutkimuksen piirteitä. Tutkimus on sekä säännöstutkimusta että lainsäädäntötutkimusta.

Tutkimuksessa tunnistetaan elementtejä organisaatioiden hyvälle tietoturvan sääntelyjärjestelmälle, joita käytetään kriteereinä tutkimuskysymyksiin vastatessa. Näitä ovat: *teknologianeutraalisuus, proaktiivisuus, hyvien käytänteiden huomioiminen, kohtuullisuus ja oikeudenmukaisuus, tavoitettavuus ja ymmärrettävyys, johdonmukaisuus ja yhtenäisyys sekä yksilöiden ja perusoikeuksien huomioiminen*. Tutkimuksen eräs havainto on se, että nykyinen organisaatioiden tietoturvan sääntelyjärjestelmä ei ole hyvä näiden kriteerien valossa. Hajanainen sääntely johtaa epäjohdonmukaiseen ja epäyhtenäiseen sääntelyyn sekä vaikeuttaa tietoturvasäännöksien tavoitettavuutta ja ymmärrettävyyttä. Organisaatioita koskevien tietoturvasäännöksien ja hyvien tietoturvakäytänteiden välillä on myös eroavaisuuksia. Tutkimuksen perusteella kansallinen tietoturvalaki on tarpeen, sillä tällöin tietoturvan sääntelyjärjestelmä suojaa paremmin organisaatioiden luottamuksellisia tietoja, yksilöiden oikeuksia sekä toimii proaktiivisemmin alati muuttuvassa yhteiskunnassamme.

Asiasanat: tietoturvalainsäädäntö, tietosuojalainsäädäntö, tietoturva, tietosuoja, kyberturvallisuus, henkilötietojen käsittely, hyvä tietoturvatapa

Abstract

The importance of information security has increased with technological development, digitalization and globalization. Our cyber environment is subject to threats that have significant impacts on the operations of organizations, the functioning of society and the rights of individuals. In today's system-dependent network society, there must be a regulatory system for information security in organizations that effectively protects individuals' personal data among other rights, as well as organizations' confidential information and continuity. This study forms and defines a good information security regulatory system for organizations that are based on effectual legislation. This study aggregates and systematizes numerous information security provisions for organizations that are evaluated against organizations' good information security practices and codes of conduct. This is how the study presents a big picture of legislative good information security practices. The implementation of the research task requires for an assessment of the content and effectiveness of current information security regulatory system, as well as the need of national information security law. The study presents two research questions: 1) is current organizations' information security regulatory system good and 2) is national information security law necessary in Finland? This legal study combines problem-centered legal doctrine and *de lege ferenda* -study.

This study identifies elements for organizations' good information security regulatory system, which are used as criteria when answering research questions. These elements are: *technology neutrality, proactivity, taking good practices into account, moderateness and fairness, accessibility and understandability, consistency and unity; as well as taking individuals and fundamental rights into account*. One finding of the study is that current organizations' information security regulatory system is not good in the light of these criteria. Fragmented regulation leads to inconsistent, heterogeneous regulation and makes information security regulation's accessibility and understandability more difficult. There are also differences between information security provisions that apply to organizations and good information security practices. According to the study, national information security law is needed because then information security regulatory system will better protect organizations' confidential information, the rights of individuals and acts more proactively in our constantly changing society.

Keywords: information security legislation, personal data protection legislation, information security, personal data protection, cyber security, processing of personal data, good information security practice

ESIPUHE JA KIITOKSET

”Hankaluuden keskellä lojuu mahdollisuus” -Albert Einstein

Tämän tutkimuksen tekoon on mahtunut monta elämänvaihetta ja tunnetilaa vuosien 2015-2024 aikana. Elämäni on muuttunut kuluneiden vuosien varrella, mutta niin on muuttunut myös maailma ja tietoturvalainsäädäntö. Tätä tutkimusta on tehty pääsääntöisesti ”töiden ohella”, mutta sitä on myös tehty eri maissa ja mantereilla, eri kaupungeissa, lentokoneessa, junassa, autossa, kotona, kavereilla, aamulla, yöllä, arkena, lomalla ja perhevapailla. Jossain vaiheessa tuntui siltä, että tutkimuksen teko ei lopu ikinä. Sitten yhtäkkiä olikin aika lähettää tutkimus julkaisuprosessiin ja siitä tuli kirja. Nyt on tullut aika kiitosten.

Haluan osoittaa suuret kiitokset kolmelle ohjaajalleni, joilla on ollut taito kannustaa vaikeina hetkinä sekä samalla ohjata minua oikeaan suuntaan tutkimukseni kehittämisessä. Näin pitkä projekti on vaatinut kaikilta kärsivällisyyttä ja pitkäjänteisyyttä. Kiitos, että olette vuodesta toiseen malttavaisesti auttaneet minua pääsemään tutkimukseni kanssa eteenpäin. Työskentelytapamme ovat olleet ainutlaatuisia, sillä niissä on korostunut paljon etätyöskentely ja minun tiukassa olevat ajalliset resurssini: lähtökohtaisesti työskentelyaikani on ollut aina iltaisin klo. 20:sta eteenpäin. Kiitos ohjaajilleni joustavuudesta. Olen erittäin kiitollinen vastuuohjaajalleni professori Vesa Annolalle, joka on auttanut minua kehittymään tutkijana sekä terävöittämään tutkimustani etenkin tutkimuksellisuuden osalta. Erityinen kiitos emeritusprofessori Asko Lehtoselle, jonka ICT-juridiikan syväosaaminen ja erinomaiset, selkeät kommentit ovat auttaneet tutkimuksen sisällön parantamisessa. Lämpimät kiitokset KTT, immateriaalioikeuden yliopistonlehtorille (emerita) Brita Gyllenbögelille, jonka rohkaisusta lähdin alun perin kirjoittamaan tätä tukimusta: olen kiitollinen Britan kannustuksesta ja tutkimustyöni tukemisesta sen eri vaiheissa.

Väitöskirjani esitarkastajina ovat toimineet emeritusprofessori Ahti Saarenpää ja professori Lasse Lehtonen. Kiitän esitarkastajia tutkimukseni kriittisestä tarkastelusta ja asiantuntevista kommenteista. Nämä inspiroivat kommentit auttoivat minua tutkimuksen viimeistelyssä. Kiitän myös emeritusprofessori Ahti Saarenpäätä lupautumisestaan vastaväittäjän tehtävään.

Haluan kiittää myös tutkimukseni alkuvaiheen rahoituksesta Erkki Paasikiven säätiötä, Liikesivistysrahastoa sekä Jenny ja Antti Wihurin rahastoa.

Kiitos kuuluu myös Vaasan yliopiston talousoikeudellisen informaation tutkimusryhmän jäsenille – on ollut merkityksellistä kuulua osaksi tutkimusyhteisöä. Erityisesti kiitos yliopisto-opettaja, KTT Siru Kaunistolle kannustamisesta, ajatustenvaihdosta tutkimuksen tekoon liittyen ja tutkimukseni oikolukemisesta. Positiivinen asenteesi ja huumorisi ovat olleet hyvää vertaistukea.

Mielestäni elämä koostuu pitkistä ja lyhyistä kohtaamisista, jotka muokkaavat polkua, jota kuljet. Erityisiä kohtaamisia ovat ne, jotka vaikuttavat myös ajatteluusi. Tunnistan, että elämässäni on ollut paljon tällaisia merkityksellisiä kohtaamisia ja koen olevani onnekas niiden myötä. Käytännön työn ja kohtaamisten kautta olen saanut alun perin kipinän väitöskirjan tekemiselle sekä inspiraatiota jatkaa kirjoittamista. Näin ollen haluan kiittää myös kaikkia asiantuntijakollegoitani. Heidän kanssaan olen käynyt mielenkiintoisia keskusteluita ja oppinut paljon käytännön tietoturvasta ja tietosuojasta. Siispä kiitos kuuluu entisille kollegoilleni, jotka työskentelevät tai ovat työskennelleet tietoturva- ja tietosuoja-asiantuntijoina KPMG:llä ja Tampereen korkeakouluyhteisössä. Yhtä lailla haluan kiittää myös nykyisiä kollegoitani Valtorilla.

Lopuksi haluan koko sydämestäni kiittää perhettäni ja ystäviäni, jotka ovat olleet merkittävässä roolissa tämän tutkimuksen edistämisessä tukien erityisesti tutkijan henkistä hyvinvointia. Kiitos kannustamisesta, myötäelämisestä sekä ilojen ja surujen kuuntelemisesta. Erityinen kiitos äidilleni Ritvalle huolenpidosta, tuesta ja lasten hoitoavusta. Suuri kiitos rakkaalle puolisolleni Matille, jonka tuki ja kannustaminen ovat olleet vankkumatonta vauva- ja ruuhkavuosien keskellä. Kiitos vastuunotosta arjen pyörittämisessä, kun minun on täytynyt priorisoida työskentelyäni. Olet aina uskonut minuun ja siihen, että iltaisista naputteluäänistä läppärillä kehkeytyy vielä jonain päivänä väitöskirja. Olet osannut huumorisi kautta tuoda naurua kiireen ja väsymyksen keskelle – kiitos siitä. Kiitos kuuluu myös rakkaille lapsilleni, jotka auttavat minua päivittäin irtaantumaan tietoturva-asioista ja muistamaan, mikä maailmassa on tärkeintä. Kiitos lapsilleni kärsivällisyydestä. Esikoiseni sanoi vuosi sitten, että ”kirjoita jo se kirjasi valmiiksi ketun nopeudella, niin päästään etelään”. Arvata saattaa, mitä aiomme tehdä seuraavaksi.

Omistan väitöskirjani Elealle ja Bealle.

Hämeenlinnassa 26.8.2024

Jenna Andersson

Sisältö

Kuviot

Taulukot

Keskeiset lyhenteet

CSIRT	Computer Security Incident Response Team
Dnro	diaarinumero
DPIA	Data Protection Impact Assessment eli tietosuojaa koskeva vaikutustenarviointi
EDPB	European Data Protection Board
EIS	Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi eli Euroopan ihmisoikeussopimus, Rooma 4.11.1950
EIT	Euroopan ihmisoikeustuomioistuin
EN	Europan neuvosto
EOAK	eduskunnan oikeusasiamiehen kanslia
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
EV	eduskunnan vastaus
EY	Euroopan yhteisö
FINAS	Finnish Accrediation Service, kansallinen akkreditointielin
GDPR	Euroopan unionin yleinen tietosuoja-asetus 2016/679/EU
HAO	hallinto-oikeus
HaVM	hallintovaliokunnan mietintö
HE	hallituksen esitys
ICT	Information Communication Technology
IEC	the International Electrotechnical Commission
IoT	Internet of Things eli esineiden internet
IP	Internet Protocol
ISO	The International Organization for Standardization
IT	information technology

JulkL	laki viranomaisten toiminnan julkisuudesta eli julkisuuslaki 21.5.1999/621
Julkri	julkisen hallinnon tietoturvallisuuden arviointikriteeristö
Katakri	kansallinen tietoturvallisuuden auditointikriteeristö
KHO	korkein hallinto-oikeus
KKO	korkein oikeus
KP-sopimus	YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus, New York 16.12.1966
LiVM	liikenne- ja viestintävaliokunnan mietintö
LVM	liikenne- ja viestintäministeriö
MFA	Multi-factor Authentication (monivaiheinen tunnistautuminen)
NIS 1 -direktiivi	Euroopan parlamentin ja neuvoston verkko- ja tietoturvadirektiivi 2016/1148/EU
NIS 2 -direktiivi	Euroopan parlamentin ja neuvoston kyberturvallisuusdirektiivi 2022/2555/EU 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
NIST	National Institute of Standards and Technology
OA	oikeusasiamies
OECD	The Organization for Economic Co-operation and Development
OM	oikeusministeriö
PeVL	perustuslakivaliokunnan lausunto
PeVM	perustuslakivaliokunnan mietintö
PiTuKri	pilvipalveluiden turvallisuuden arviointikriteeristö
PL	Suomen perustuslaki 11.6.1999/731
RL	rikoslaki 19.12.1889/39
SFS	Suomen Standardisoimisliitto
SopMenL	laki sopimattomasta menettelystä elinkeinotoiminnassa 22.12.1978 /1061

SVPL	laki sähköisen viestinnän palveluista 7.11.2014/917
TaVM	talousvaliokunnan mietintö
TTA	valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681 (Tietoturvallisuusasetus)
TT	työtuomioistuin
TVT	tieto- ja viestintätekniikka
VAHTI	Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
VTS	Vessel Traffic Service, alusliikennepalvelu
vp	valtiopäivät
YK	Yhdistyneet kansakunnat
YksTL	laki yksityisyyden suojasta työelämässä 13.8.2004/759 (työelämän tietosuojalaki)

1 JOHDANTO

1.1 Tutkimuskohteen kuvaus

Nopeasti kehittynyt teknologia on ollut nykyisen yhteiskuntamme ja toimintamme kulmakivi[1]. Aikaisemmin organisaatiot sekä työ- ja elinkeinoelämä rakentuivat pitkälti lainalaisuuksiin ja rakenteisiin, joissa ihmisten välinen vuorovaikutus ja toiminta onnistuivat parhaiten fyysisesti kohtaamalla. Tähän on kuitenkin tullut muutos, sillä teknologian kehitys on mahdollistanut uusien toimintatapojen synnyn. Nopea muutostahti on synnyttänyt sekä nykyisten että uusien, teknologisen kehityksen tarjoamien mahdollisuuksien välille kuilun, jonka kuromista kiinni on kutsuttu *digitalisaatioksi*. [2] Digitalisaatio on yhteiskunnallinen prosessi, jossa hyödynnetään teknologian kehittymisen mahdollisuuksia sekä digitaalitekniikan integrointia osaksi elämän jokapäiväisiä toimintoja[3]. Näin ollen teknologian kehittyminen ja yhteiskunnan digitalisoituminen voidaan nähdä kulkevan rinnakkain[4]. Nopea yhteiskunnan muuttuminen vaatii organisaatioilta kykyä muokkautua ja vastata toimintaympäristönsä haasteisiin, kuten esimerkiksi uuden teknologian omaksumisesta nousseisiin tietoturvauhkiin. Haasteista huolimatta uudet toimintatavat ja uuden teknologian hallinta luovat kilpailukykyä organisaatioille.

Organisaatioiden liiketoiminnan arvo kasvaa teknologiaa hyödyntämällä. Parhaimmillaan teknologia ja siihen liittyvät palvelut muuttavat valtavasti yhteiskunnan rakenteita ja toimintaa. Tässä muutoskierteessä parhaiten menestyvät ne toimijat, jotka pystyvät tarjoamaan luotettavia ja laadukkaita tietotekniikkaa hyödyntäviä tuotteita ja palveluita asiakkaiden tarpeita kuunnellen sekä samaan aikaan mahdollisimman kannattavasti. Tuotteen tai palvelun luotettavuusaspektin myötä hyödykkeen tulee olla turvallisen käyttökokemuksen lisäksi tietoturvallinen.[5] Turvallisuus on myös katsottu olevan organisaatioille merkittävä kilpailutekijä[6].

---

[1] Järvinen & Rousku 2017: 5–6.
[2] Valtiovarainministeriön julkaisu 10/2017: 84.
[3] Alasoini 2015: 26.
[4] Ainakin toistaiseksi näyttäisi sieltä, että digitalisoituminen ja sen tuomien muutosten kehityskulku jatkuu vielä pitkään. Muutosten ensimmäisinä omaksujina ovat olleet luonnollisesti kehittyneet maat. Nähtäväksi jääkin, minkälaiseksi nyky-yhteiskuntamme muuttuu, kun kehittyvät maat omaksuvat täysin digitalisaation tuomat muutokset ja mahdollisuudet.
[5] Suomen tietoturvallisuusstrategia 2016: 15–18.
[6] Elinkeinoelämän keskusliitto 2018: 8.

Teknologian jatkuva kehittyminen ja digitalisoituminen luovat paljon mahdollisuuksia[7] yhteiskunnalle ja organisaatioille, mutta myös paljon uhkia ja riskejä. Sekä mahdollisuudet että uhat vaikuttavat yhtäaikaisesti organisaatioiden talouteen ja toimintaan. Esimerkiksi teknologian kehittymisen positiiviset puolet voivat näkyä organisaation toiminnan tehostamisena, asiakaskasvuna ja voiton maksimointina. Vastakohtaisesti teknologian kehittymisen negatiiviset puolet voivat tulla ilmi häiriöinä[8], jotka kasvattavat kuluja sekä näkyvät myös luottamuspulana ja asiakaskatona. Häiriöiden lisäksi tahattomista vahingoista tai tahallisista teoista aiheutuvat turvallisuuspoikkeamat ovat viime vuosina lisääntyneet ja ne voivat häiritä muun muassa yhteiskuntamme keskeisten palvelujen (esimerkiksi terveydenhuolto, sähkönjakelu ja vedenjakelu) tarjontaa[9]. Digitalisoitumisen kehittyessä ja ihmisten tullessa yhä riippuvaisemmiksi sähköisistä palveluista, myös tietoturvapoikkeamat laajenevat koskemaan yhä useampaa organisaatiota ja samalla niiden vaikutukset luonnollisiin henkilöihin kasvavat suuriksi ja näkyvimmiksi.

> *Yksi esimerkki tietoturvapoikkeamien negatiivisesta vaikutuksesta on kyytipalvelu Uberin tietomurtouutisointi vuodelta 2017. Tapauksesta paljastui hakkereiden saaneen 57 miljoonan käyttäjän ja kuljettajan kryptaamattomat tiedot jo lokakuussa 2016. Uber yritti peittää tämän ja maksoi hakkeroijille 100.000 dollaria datan poistamisesta ja hiljenemisestä loukkauksen suhteen. Tapaus päätyi kuitenkin julkisuuteen ja siitä on paljon opittavaa, sillä Uberin olisi lainmukaisesti pitänyt ilmoittaa tietomurrosta.[10] Tapahtuma ja siitä seurannut tiedottaminen ja uutisointi vaikutti selkeästi negatiivisesti kuljettajien ja asiakkaiden luottamukseen Uberin tarjoamaa kuljetuspalvelua kohtaan ja siten myös yrityksen imagoon.*

Tietoturvauhkiin ja -loukkauksiin liittyvät organisaatioiden kustannuskasvut, maineen heikkenemiset ja varallisuuden menetykset ovat teknologian kehittymisen ja digitalisoitumisen varjopuolia. Tietoturvaloukkausten vaikutukset organisaatioiden maineelle, varallisuudelle, toiminnalle ja sidosryhmäsuhteille voivat olla erittäin merkittävät. Esimerkiksi yksittäiset vahinkotapaukset ovat saattaneet

---

[7] Digitalisaatio tarjoaa merkittäviä mahdollisuuksia parempaan elämänlaatuun, talouskasvuun ja kestävyyteen. Ks. Euroopan unionin neuvosto, EU:n digitaalipolitiikan tulevaisuus – Neuvoston päätelmät 21.5.2024, s. 4.

[8] Tällaiset häiriöt voivat usein liittyä esimerkiksi uuden teknologian käyttöönottoon taikka kehittämisen yhteydessä tapahtuviin virhetilanteisiin (konfigurointivirheet ym.). Häiriöitä voivat aiheuttaa myös luonnonkatastrofit, jonka seurauksena tietoturvallisuus voi vaarantua. Ks. Euroopan unionin kyberturvallisuusstrategia 2013: 3.

[9] Euroopan unionin kyberturvallisuusstrategia 2013: 3.
Kriittiseen infrastruktuuriin kohdistuvat haitalliset iskut ovat merkittävä maailmanlaajuinen riski. Ks. Euroopan unionin kyberturvallisuusstrategia 2020, s. 2.

[10] The Guardian 2017.

aiheuttaa suuryrityksille miljoonavahingot ja kymmenien miljoonien asiakastietojen menetykset. Myös tietoturvaongelmilta suojautuminen aiheuttaa yhä kasvavissa määrin kustannuksia. Vahinkovakuutusten osuus on kasvamassa ja esimerkiksi EU:n yleisen tietosuoja-asetuksen velvoitteet voivat aiheuttaa joillekin organisaatioille vuosittaisia lisäkustannuksia. Edellä mainittujen vaikutusten ohella markkinoilla saattaa ilmetä luottamuspulaa, esimerkiksi 28 000 haastatellusta eurooppalaisesta 88 % on muuttanut toimintatapojansa internetissä tietoturvahuolien vuoksi.[11]

Teknologian kehittymisen ja digitalisoitumisen ilmiöihin liittyy vahvasti globalisaatio, sillä tiedot ja palvelujen tuottaminen sijaitsevat harvoin enää ainoastaan kotimaassa. Kaikki tämä vaatii organisaatioilta toimintaprosessien uudelleen miettimistä, riskinottohalua sekä uudistumis- ja innovaatiokykyä.[12] On huomioitava, että verkon uhat eivät tunne maantieteellisiä rajoja verkottuneessa digitaalitaloudessa ja yhteiskunnassa[13]. Globalisoitumisen sekä 90-luvun internetin kehityksen ja informaatiotietovarantojen kasvun myötä myös kyberrikollisuus on lisääntynyt huomattavasti. Kyberrikollisuuden kasvun seurauksena organisaatioiden turvallisuuden fokus on alkanut keskittymään nopeasti muuttuviin ulkoisiin uhkiin sisäisten uhkien sijaan.[14] Teknologian kehittyminen ja digitalisaatio mahdollistavat uusien kilpailijoiden pääsyn markkinoille, mutta ne jättävät myös aukkoja globaaleille toimijoille, joiden tarkoituksena ei ole kilpailla markkinoilla vaan hyötyä muiden menestyksestä rikollisin keinoin. Näin ollen globalisaatio itsessään on kiihdyttänyt kyberrikollisuuden kasvua.

Kyberrikolliset - kutsutaan myös tietoverkkorikollisiksi - ovat muuttaneet perinteisen rikollisuuden muodot (esimerkiksi kidnappaukset, kiristäminen, murrot, ryöstöt) digitaaliseksi rikollisuudeksi. Tällöin rikokset tapahtuvat kybertoimintaympäristöissä eli tietoverkoissa ja sähköisissä toimintaympäristöissä. Rikollisten tavoitteet ovat kuitenkin samat kuin ennenkin, joista yleisin on rahallinen hyöty. Valtiollisessa tiedustelussa tavoite voi olla myös arkaluontoisen, valtiollisen tiedon saaminen omaksi hyödykseen. Kyberterroristeilla tavoite voi olla epäjärjestyksen ja vahingon aiheuttaminen.[15] Kybertoimintaympäristöön kohdistuvat uhat

[11] Suomen tietoturvallisuusstrategia 2016: 17–26. Myös valtioiden mittava verkkovalvonta nähdään luottamuspulaa kasvattavana tekijänä.
[12] Järvinen & Rousku 2017: 12.
[13] Euroopan unionin kyberturvallisuusstrategia 2013: 18. Vastaavaa on todettu myös päivitetyssä Euroopan unionin vuoden 2020 kyberturvallisuusstrategissa. Lähes kaikkien rikostyyppien tutkinnassa on havaittavissa digitaalinen komponentti. Kyberturvallisuus on välttämätöntä verkkoyhteyksille sekä maailmanlaajuiselle ja avoimelle internetille. Ks. Euroopan unionin kyberturvallisuusstrategia 2020, s. 3–4:
[14] OECD 2012, *The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy*: 5–8.
[15] Järvinen & Rousku 2017: 7–9.

ovat muuttuneet vaikutuksiltaan vaarallisemmiksi niin yritysten kuin yksityisten henkilöiden sekä koko yhteiskunnan kannalta. Tämän lisäksi toimijat ovat ammattimaisempia ja usein valtiollisia toimijoita.[16] Organisaatioiden uudistaessa ja vahvistaessa omia puolustusmekanismejaan tietoturvarikoksia vastaan, kyberrikolliset muodostavat entistä monimutkaisempia ja älykkäämpiä tapoja murtautua organisaation tietojärjestelmiin[17]. Näin ollen mitä enemmän teknologia kehittyy, sitä todennäköisemmin myös kyberrikokset kehittyvät[18]. Tällöin organisaatioilla tulee olla tietoturvaosaamisen ohella muita työkaluja, joiden avulla on mahdollista ennalta ehkäistä tunnistettuja tietoturvauhkia sekä reagoida uudenlaisiin tietoturvapoikkeamiin ja -loukkauksiin. Lainsäädännön tulisi olla yksi tällainen työkalu.

Tietotekniikan kehittymisen alkuvaiheiden jälkeen tietoturvallisuuden kriittinen merkitys on nyky-yhteiskunnassamme kasvanut ja samalla aiheuttanut merkittävän sääntelyongelman. Teknologia on muuttunut parin viime vuosikymmenen aikana hurjaa vauhtia. Uudet rikollisuuden muodot ovat lisääntyneet. Lisäksi teknologian kehittymisen seurauksena tietoa on paljon saatavilla, jolloin oikeudellisen tiedonhaun hallitseminen vaikuttaa suuresti oikeudellisen työn laatuun ja onnistumiseen. Tietoturvalainsäädännön poikkitieteellisyyden takia lainsäätäjillä tulisi olla myös teknistä tietämystä.[19]

Uudet uhat ja riskit luovat uusia lainsäädännöllisiä, oikeustieteellisiä ja lakiteknisiä haasteita. Digitalisaation myötä laajentunut digitaalinen toimintaympäristö on ollut muun muassa oikeuskulttuuriamme muuttava tekijä. Lisäksi lainsäädäntö on kansainvälistynyt, sillä nykyisessä verkkoyhteiskunnassa tietoverkkojen ja tietotekniikan käyttö on levinnyt globaalisti. Lainsäädännön kehitys seuraakin yleensä yhteiskunnan kehitystä jälkijunassa. Nopeat muutokset aiheuttavat *lainsäätäjäriskin*, mikä tarkoittaa sitä, että lainsäätäjä ei ole oikealla tavalla tai ajoissa havahtunut lainsäätämistarpeeseen.[20] Tällöin myös käytännön toiminnassa saattaa ilmetä paineita tulkita puutteellisia taikka vanhentuneita säännöksiä laajentavasti[21]. Toisaalta oikeusvaltio ei voi automaattisesti suoltaa sääntelyä jokaiselle uudelle ilmiölle tai välineelle[22]. Eräänlaisena digitalisaatioon ja yhteiskunnan kehittymiseen liittyvänä sääntelyn haasteena onkin ollut muuttuvan tekniikan seuraaminen sekä laajempien tai suurivaikutteisten ilmiöiden tunnistaminen, jotka on

Internet on myös varsin tehokas terrorismirikosten valmistelu- ja edistämisväline. Ks. Lohse 2012, s. 22.
[16] Andersson 2018: 1; Suomen kyberturvallisuusstrategia 2013: 1.
[17] Järvinen & Rousku 2017: 7–9.
[18] Konkreettisena esimerkkinä tästä on muun muassa tekoälyn ja kielimallien hyödyntäminen kyberrikollisuudessa.
[19] Saarenpää 2016a: 57–58, 77–78, 96, 127–128, 236; Sepel 2004: 120.
[20] Saarenpää 2016a: 82–83, 87–88, 239; Saarenpää & Riekkinen 2023: 201–202.
[21] Riekkinen 2019: 5.
[22] Saarenpää 2018: 18.

pitänyt huomioida osana teknologianeutraalia sääntelyä. Lainsäädäntö, joka ei ota huomioon yhteiskunnan digitalisointia ja tekniikan kehitystä riittävällä tasolla, johtaa soveltamistilanteissa ei-toivottuihin tuloksiin uudessa teknologisessa ympäristössä[23].

Teknologian kehittymisen, digitalisoitumisen ja globalisoitumisen myötä myös organisaatioiden on yritettävä pysyä lainsäädännöllisen kehityksen perässä. Se on haasteellista, sillä digitalisoituvassa yhteiskunnassa uusiutuva lainsäädäntö on ennemminkin sääntö kuin poikkeus. On huomioitava se, että tietoturvallisuusnormit eivät ole ainoastaan juristien tulkittavaksi, sillä esimerkiksi tietotekniikan ammattilaiset soveltavat tietoturvallisuusnormeja tietojärjestelmien suunnittelu-, rakentamis- ja ylläpitovaiheissa[24].

Vaikka yhteiskunnan muutoksien myötä tapahtuva lainsäädännön kehittyminen on lähtökohtaisesti positiivinen asia, organisaatiot saattavat katsoa lainsäädännön kehityksen olevan yksi toimintaan kohdistuva riski: muuttuva lainsäädäntö ja vaatimusten hajanaisuus useampaan eri säädökseen aiheuttavat haasteita organisaatioille. Näistä yksi merkittävimmistä on ”*compliance*”-haaste eli velvollisuus toimia määräysten ja säädösten mukaan, joita nyky-yhteiskunnassamme on paljon[25]. Määräysten ja säädösten vastoin toimimisesta aiheutuu usein sanktioita[26] ja mainehaittaa. Samassa yhteydessä voidaan puhua myös *sääntelyriskistä*, mikä tarkoittaa uhkaa siitä, että sääntely ja oikeusnormit itsessään saattavat aiheuttaa tarkoittamattomia kustannuksia ja muita epäedullisia vaikutuksia yksilöille, taloudellisille toimijoille ja muille ryhmille[27]. Sääntelyriskin välittöminä syinä voivat olla sääntelyn epätarkoituksenmukainen systematiikka ja tekninen muoto, sisältö taikka sääntelijän harkitsematon tai muuten oikeudenmukaisuuden vajeisiin johtava passiivisuus nopeasti muuttuvassa yhteiskunnassa[28].

---

[23] Magnusson Sjöberg 2018: 22.
[24] Pöysti 1997: 11.
[25] Myös Pöysti on tunnistanut erääksi riskiksi oikeudellisen riskin, jolla viitataan vaatimusten noudattamatta jättämiseen (*”non-compliance”*) sekä sopimusten tai lakisääteisten määräysten nojalla annettuihin oikeudellisiin seuraamuksiin, joita sovelletaan lakisääteisten vaatimusten noudattamatta jättämiseen (ks. Pöysti 2023: 46–47).
[26] Esimerkiksi tietosuoja-asetuksen vaatimuksien täytäntöönpanoa tehostettiin tuntuvilla sanktioilla, jotka voivat olla jopa 20 milj. euroa taikka 4 % organisaation globaalista liikevaihdosta. Suuruus määräytyy rikkomuksen luonteen perusteella. Sanktiot voivat koskea sekä rekisterinpitäjiä että henkilötietojen käsittelijöitä. Ks. VAHTI 1/2016, s. 18 & 30. Esimerkkinä suurista sakoista on Ranskan tietosuojaviranomaisen (CNIL) Google LLC:lle langettama 50 miljoonan euron sakko tietosuoja-asetuksen velvoitteiden rikkomisesta. Sanktio liittyi muun muassa siihen, että Google ei ole kertonut riittävän selkeästi ja läpinäkyvästi asiakkailleen tietojen säilytysajoista ja käyttötarkoituksesta ja näitä tietoja on ollut vaikea löytää. Lisäksi käyttäjien suostumusta mainonnan kohdentamiseen ei voida pitää tapauksessa yksiselitteisenä. Ks. CNIL 2019.
[27] Alavesa 2016: 255; Pöysti 1997: 45.
[28] Korja 2016b: 445.

Digitalisaation ja tietoturvan sääntelyyn liittyvää noudattamishaastetta vaikeuttaa monimutkaisen sääntelyn lisäksi niiden globaali luonne. Vaikkakin verkkoyhteiskunnassamme maantieteellisten fyysisten rajojen vaikutus on pienentynyt, maantieteellisten rajojen oikeudellinen ylittäminen eri toiminnoissa on haasteellista, etenkin ylittäessä Euroopan unionin rajat[29]. Siinä missä kansalliset rajat toimivat ihmisten, hyödykkeiden sekä kansallisen lainsäädännön ja viranomaisten toiminnan rajana, internet on globaali ja ylikansallinen[30]. Näin ollen virtuaaliset ja fyysiset rajat ovat yksi suurimpia käytännön ja lainsäädännöllisten pulmien aiheuttajia.[31] Organisaatioiden pitäisi pystyä hallitsemaan itselleen relevanttien maiden lainsäädäntöä sekä suojaamaan luottamukselliset tietonsa jokaisessa maassa, missä organisaatiolla on toimintaa. Tähän liittyy globaalisti toimivilla organisaatioilla kolme keskeistä huomioitavaa seikkaa: 1) minkä maiden lainsäädäntöä on huomioitava, 2) vieraan maan lakien ja asetuksien saatavuus ja 3) vieraan maan säädöksien ymmärtäminen[32]. Esimerkiksi, jos suomalaisella organisaatiolla on toimintaa USA:ssa, tulee ottaa huomioon myös kansallisen ja EU-lainsäädännön lisäksi USA:n lainsäädäntö. Tietosuojalainsäädännön näkökulmasta organisaation itse ei tarvitse edes olla globaali toimija, sillä myös esimerkiksi kansallisten organisaatioiden käyttämissä globaaleissa pilvipalveluissa tapahtuvissa henkilötietojen tiedonsiirroissa EU/ETA-alueen ulkopuolelle on huomioitava kohdemaan tietosuojalainsäädäntö sekä henkilötietojen käsittelyn turvallisuus.

Voidaan todeta, että yhteiskuntamme muutokset luovat haasteita niin organisaatioille kuin lainsäätäjille. Tietoturvallisuuden merkitys on kasvanut teknologian kehittymisen, digitalisoitumisen ja globalisaation myötä, ja se heijastuu nykyisessä verkkoyhteiskunnassamme organisaatioiden toimintaan, yhteiskunnan toimivuuteen sekä yksilöiden oikeuksiin. Hyvä tietoturvan lopputulos saavutetaan asiakokonaisuuksien ymmärtämisellä sekä riskienhallinnalla[33]. Tämä ei kuitenkaan yksistään riitä, sillä lainsäädännön tulisi asettaa vähimmäistaso organisaatioiden tietoturvalle yhdessä hyvien tietoturvakäytänteiden kanssa. Yhteiskuntamme muutokset aiheuttavat täysin uudenlaisia tietoturvariskejä, joihin organisaatioiden ja lainsäätäjien tulisi reagoida ajoissa ja mieluiten proaktiivisesti riskien pienentämiseksi. Näin ollen tarvitaan kattava ja yhtenäinen organisaatioiden tietoturvan sääntelyjärjestelmä, joka samalla mahdollistaisi turvallisen digitalisoitumisen. Hyvä organisaatioiden tietoturvan sääntelyjärjestelmä olisi tällöin myös yksi työkalu niin organisaatioiden kuin yksilöiden tietoturvan parantamiseksi, joka mahdollistaisi paremman tietoturvauhkiin varautumisen sekä tietoturvaloukkauksiin

[29] Saarenpää 2016a: 78–79.
[30] Myös kyberrikoksille ominaista on niiden globaali luonne, jonka myötä kansainvälisen yhteistyön tarve korostuu. Ks. Ayanso & Herath 2012, s. 64.
[31] Riekkinen 2016a: 76.
[32] Svantesson 2018: 29–30.
[33] Andreasson & Koivisto 2013: 16–17; Alavesa 2016: 242.

reagoimisen. Tällöin hyvien tietoturvallisten käytänteiden omaksuminen on olennaista sekä organisaatioissa että lainsäädännön tasolla.

1.2 Tutkimustehtävä ja tavoitteet

Tietoturvayritykset, viranomaisohjeistukset, hyvät käytännöt sekä jatkuvaan tietoturvaosaamiseen ja sen ylläpitämiseen liittyvä koulutus ja tutkimus luovat organisaatioille työkaluja oman tietoturvatasonsa vahvistamiseen sekä keinoja tehostaa omaa riskienhallintaansa. Yhtä lailla lainsäätäjän luoman lain tulisi asettaa organisaatioiden tietoturvalle velvoittava vähimmäistaso, jolloin myös laista muodostuisi eräänlainen työkalu organisaatioille tietoturvan parantamiseksi ja uusien, yhteiskunnan kehityksen myötä syntyvien tietoturvariskien hallitsemiseksi. Tällöin edellytyksenä on se, että voimassa oleva lainsäädäntö on ajan tasalla verrattuna kehittyvään yhteiskuntaan ja muuttuvaan riskiympäristöön. Lisäksi lainsäädännön tulisi vastata hyviä alalla olevia käytänteitä.

Nykyinen tietoturvaa koskeva sääntely on hajaantunut kansallisella tasolla useaan eri säädökseen. Selkeimmät tietoturvavaatimukset kohdistuvat julkishallintoon, mutta muiden organisaatioiden osalta sääntely on ollut hyvinkin toimiala- tai sektorikohtaista ja tasoltaan vaihtelevaa. On huomioitava, että tietosuojalainsäädännössä on henkilötietojen suojaa parantavia tietoturvavaatimuksia, jotka koskevat kaikkia organisaatioita. Yhtä lailla perustuslaissa on tunnistettavissa tietoturvaan linkittyviä perusoikeuksia. Lainsäädännön ohella organisaatioiden tietoturvaa ohjaavat hyvät tietoturvakäytänteet ja käytännesäännöt, jotka ikään kuin täydentävät lainsäädännöstä tulevia tietoturvavelvoitteita. Käytänteiden on myös nähty pitävän teknologianeutraalisti säädeltyä lainsäädäntöä ajankohtaisena. Viimeisten vuosien aikana erinäisiä ohjeistuksia ja lakimuutoksia on julkaistu tietoturvaan liittyen jatkuvasti ja nopealla tahdilla. Lainsäädännön tavoitettavuuden ja ymmärrettävyyden lisäämiseksi tässä tutkimuksessa tehtävä tietoturvallisuuden sääntelyjärjestelmän kuvaaminen on tärkeää.

Tämän tutkimuksen päätehtävänä on muodostaa ja määritellä voimassa olevan lainsäädännön perusteella **organisaatioiden hyvä tietoturvan sääntelyjärjestelmä.** Tämä tapahtuu kokoamalla yhteen ja systematisoimalla organisaatioiden tietoturvaa käsittelevät lukuisat säännökset. Näin ollen tutkimuksessa tarkastellaan uusimpia tietoturvaan liittyviä säädöksiä sekä niiden mahdollisia vaikutuksia organisaatioiden tietoturvallisuuteen ja riskienhallintaan. Tämän lisäksi nykylainsäädäntöä peilataan jo olemassa oleviin suosituksiin, ohjeisiin ja tietoturvan viitekehyksiin. Täten pystytään muodostamaan ajantasainen käsitys nykyisestä

organisaation tietoturvan sääntelyjärjestelmästä sekä siihen liittyvistä ongelmista tai puutteista.

Tutkimuksen tavoitteena ei ole ainoastaan kuvata nykyistä tietoturvan sääntelyjärjestelmää vaan tehtävänä on määritellä hyvä sellainen. Näin ollen tutkimuksessa on välttämätöntä tunnistaa organisaatioiden hyvälle tietoturvan sääntelyjärjestelmälle elementtejä, joita käytetään apuna tutkimuskysymyksiin vastatessa. Nämä elementit toimivat samalla eräänlaisia kriteereinä sääntelyjärjestelmän hyvyydelle. Aivan kuten tietoturvallisuuden tavoitteena on suojata tietoja, organisaatioiden ja yhteiskunnan toimintaa ja jatkuvuutta sekä henkilöiden oikeuksia ja vapauksia, myös hyvä tietoturvalainsäädäntö edistää tätä suojaamistavoitetta. Sääntelyjärjestelmän hyvyyttä tarkastellaan tutkimuksessa normikeskeisesti tukeutuen tunnistettuihin hyvän sääntelyjärjestelmän elementteihin. Normikeskeinen tarkastelu mahdollistaa tasavertaisemman arvioinnin koko yhteiskunnan kannalta toisin kuin se, että tutkimuksessa arvioitaisiin hyvyyttä ainoastaan yrityksien, työntekijöiden, juristien tai kuluttajien näkökulmasta.

Muodostaessa hyvää organisaatioiden tietoturvan sääntelyjärjestelmää hyödynnetään samalla hyviä käytänteitä järjestelmän toteuttamisessa. Näin ollen tavoitteena on esittää **hyvän tietoturvatavan** muodostama kokonaisuus, joka tapahtuu arvioimalla organisaatioita velvoittavia tietoturvasäädöksiä sekä käytännesääntöjä. Samalla lainsäädännössä ilmenevää hyvää tietoturvatapaa vertaillaan organisaatioiden hyviin käytänteisiin ja toimintatapoihin. Täten pystytään muodostamaan käsitys siitä, vastaako lainsäädännön organisaatioilta edellyttämä tietoturvataso ja hyvä tietoturvatapa organisaatioiden hyviä käytänteitä sekä kuinka tehokkaasti se suojaa informaatiota. Lisäksi tarkoituksena on huomioida nykyaikaisen yhteiskunnan vaikutuksia organisaatioiden toimintaympäristöön. Koska nykyinen verkkoyhteiskuntamme on todettu olevan riskiyhteiskunta, tässä tutkimuksessa tarkastellaan hyvien tietoturvakäytänteiden ohella organisaatioiden hyviä riskienhallintakäytänteitä.

Tietoturvallisuuden merkitys nykyisessä oikeudellistuneessa verkkoyhteiskunnassamme on kiistattomasti kasvanut, joka ilmenee myös siten, että tietoturvaan liittyvää lainsäädäntöä on kehitetty reaktiivisesti heijastuen yhteiskunnan muutoksiin ja tarpeisiin. Näin ollen tässä tutkimuksessa tehtävä organisaatioiden hyvän tietoturvan sääntelyjärjestelmän määritteleminen on merkityksellistä. Tietoturvaa tulisi tarkastella suomalaisessa lainsäädännössä yleisen tietoturvaperiaatteen kautta, mikä ei ole toteutunut nykyisen lainsäätäjäriskin tuloksena [34]. Lisäksi meiltä puuttuu yleinen tietoturvalaki tietoturvan jakaantuessa erillissääntelyn alle. Tämän tutkimuksen päätehtävän, eli organisaatioiden tietoturvan

[34] Saarenpää 2016a: 272.

sääntelyjärjestelmän kuvaamisen lisäksi, onkin oleellista arvioida nykyisen tietoturvalainsäädännön tehokkuutta[35] ja toimivuutta sekä tämän arvion pohjalta yleisen tietoturvalain säätämistarvetta. Täten tutkimuksessa on kaksi olennaista tutkimuskysymystä:

1) **Onko nykyinen organisaatioiden tietoturvan sääntelyjärjestelmä hyvä?**

2) **Onko Suomessa tarpeen kansallinen tietoturvalaki?**

Tutkimus jakautuu 5 päälukuun. Ensimmäisen luvun eli tämän johdantoluvun tarkoituksena on tehdä katsaus muun muassa tutkimuksen tavoitteisiin, toteutukseen, aineistoon, menetelmiin sekä siihen, miten teknologian kehittyminen, digitalisoituminen ja globalisaatio ovat vaikuttaneet organisaatioiden toimintaympäristöön, tietoturvaan ja riskeihin. Täten johdantoluvun tavoitteena on toisin sanoen tehdä yleiskatsaus tutkimuksen lähtökohtiin ja määritellä tutkimustehtävä. Tutkimustehtävän eli organisaatioiden tietoturvan sääntelyjärjestelmän kuvaamisen toteutus tapahtuu siten, että tutkimuksen alussa käsitellään tietoturvan systematiikkaa sekä tietoturvan oikeudellista kehystä periaate- ja perusoikeustasolla. Tämän jälkeen kuvataan tiiviisti EU:n ja kansallisen lainsäädännön tietoturvasäädöksiä sekä tietoturvallisuuden käytännesääntöjä ja standardeja osana tietoturvallisuuden hyviä käytänteitä. Tällä tavoin luvussa 2 luodaan niin sanotusti kehys koko tutkimukselle. Tämän jälkeen tutkimuksessa luvuissa 3 ja 4 määritetään lainsäädännön organisaatioilta edellyttämä tietoturvan taso ja sisältö voimassa olevan oikeuden pohjalta. Määriteltäessä organisaatioiden tietoturvan sääntelyjärjestelmää, lainsäädännön hyvää tietoturvatapaa verrataan yhtäaikaisesti organisaatioissa toteutettaviin hyviin tietoturvallisiin käytänteisiin. Päälukujen 2–4 taustoista, sisällöstä ja tavoitteista on kerrottu kunkin luvun alussa ja lisäksi alla olevassa kuviossa on tiivistetysti esitetty päälukujen keskeiset aihealueet. Viimeinen pääluku on luonnollisesti havaintoja ja johtopäätöksiä käsittelevä luku.

[35] Suomen kyberturvallisuusstrategian 2013 (s. 8) strategisten linjausten 8. kohdassa on todettu tavoitteeksi se, että kansallisella lainsäädännöllä varmistetaan *tehokkaan* kyberturvallisuuden toteutumisen edellytykset. Tämä strateginen tavoite on toiminut myös innoittaja tämän tutkimuksen tutkimuskysymysten osalta.

Kuvio 1. Tutkimuksen rakenne ja tavoitteiden havainnollistaminen

1.3 Tutkimuksen rajaukset

Tutkimuksessa keskeinen tarkastelu kohdistuu kansalliseen voimassa olevaan tietoturvalainsäädäntöön sekä organisaatioiden hyviin, tietoturvallisiin käytänteisiin, jotka pohjautuvat erilaisiin viitekehyksiin, kuten käytännesääntöihin ja kansainvälisiin standardeihin.

Tutkimuksen vallitsevan organisaationäkökulman vuoksi yksi selkeä rajaus kohdistuu organisaatioiden ja kansallisen turvallisuuden välille: organisaatioita koskevat varautumisvaatimukset lainsäädännössä on rajattu pois tutkimuksesta. Näin ollen esimerkiksi CER-direktiivin kokonaisvaltainen ja yksityiskohtainen käsittely ei ole keskeistä tässä tutkimuksessa, sillä siinä painotetaan paljon toimijoiden häiriönsietokykyä ja varautumista. Koska käytettävyys on kuitenkin yksi tietoturvallisuuden osa-alue ja keskeinen osa organisaatioiden tietoturvaa,

järjestelmien varmuuskopiointi ja toipuminen on huomioitu tässä tutkimuksessa osana järjestelmien oikeudellista suunnittelua[36].

Toinen rajaus tutkimuksessa muodostuu organisaatioiden ja kuluttajien välille. Tutkimus käsittelee vain suppeasti sitä, miten esimerkiksi organisaatioiden toiminta ja tietoturva saattavat vaikuttaa kuluttajien eli asiakkaiden tietoturvallisuuteen ja luottamukseen menemättä kuitenkaan kovin syvälliselle tasolle näissä osa-alueissa. Koska kuitenkin tietosuoja on yksi osa-alue organisaatioiden tietoturvaa sekä yksityishenkilöt ovat yksi ryhmä organisaation sidosryhmistä, tässä tutkimuksessa huomioidaan yksityishenkilöt henkilötietojen suojaa ja yksityisyyttä käsiteltäessä.

Tietosuojaa käsittelevän kolmannen pääluvun tavoitteena on tunnistaa organisaatioiden hyvä tietoturvatapa tietosuojalainsäädännön sisäänrakennetun tietoturva- ja riskienhallintavaatimuksien kautta. Tarkoituksena ei kuitenkaan ole käsitellä kokonaisvaltaisesti kaikkia tietosuojavaatimuksia, sillä tutkimuksen näkökulma on tietoturvapainotteinen.

Lainsäädännön tietoturvavaatimuksia on kehitetty vuosien saatossa keskittyen etenkin viranomaisia velvoittaviin vaatimuksiin. Järjestelmäriippuvaisessa, linkittyneessä verkkoyhteiskunnassa myös muut toimijat tulisi huomioida kattavammin, jotta tietoturvan ja henkilöiden perusoikeuksien toteutuminen olisi tehokkaampaa. Näin ollen tämän tutkimuksen vallitseva näkökulma kohdistuu nimenomaan hyvään tietoturvatapaan ja lainsäädännön tietoturvavaatimuksiin huomioon ottaen organisaatiot yleensä, eikä ainoastaan viranomaisia. Tutkimuksesta on täten rajattu pois julkisen sektorin tietojen käsittelyn vaatimusten yksityiskohtainen tarkastelu ja keskitytty lähinnä yritystoimintaa harjoittavien organisaatioiden velvoittaviin tietoturvavaatimuksiin lainsäädännössä[37]. Esimerkiksi viranomaisen asiakirjojen suojaamisen yksityiskohtainen käsittely on rajattu tutkimuksen ulkopuolelle. Rajaus koskee myös digitaalisten palvelujen tarjoamisesta koskevan lain (306/2019, digipalvelulaki), EU:n datanhallinta-asetuksen (2022/868/EU) [38] sekä tiedonhallintalain (906/2019) yksityiskohtaista käsittelyä, sillä säädökset koskevat viranomaisen digitaalisia palveluita ja tiedonhallintaa. Rajaus on tehtävä tutkimuksen laajuuden hallitsemiseksi. Ottaen huomioon tutkimuksen tarkoitus käsitellä hyvää tietoturvatapaa ja organisaatioiden hyviä tietoturvakäytänteitä,

[36] Ks. luku 4.4.4 (”Varmuuskopioinnin ja toipumisen vaatimukset sääntelyjärjestelmässä”).
[37] Talousoikeudessa oikeudellisia kysymyksiä tarkastellaan usein yritystoiminnan näkökulmasta, ks. luku 1.4.3 (”Tutkimuksen sijoittuminen).
[38] Datanhallinta-asetuksen mukaisen datan uudelleenkäyttöä koskevat säännökset koskevat pitkälti julkista sektoria.

viranomaisen kattavia tietoturvan vähimmäisvaatimuksia[39] ja käsitteistöä on käsitelty esimerkinomaisesti tutkimuksessa. Nämä toimivat hyvänä esimerkkinä teknologianeutraalista vähimmäissääntelystä, jota voisi ulottaa laajemmin yksityiselle sektorille. Viranomaisen vähimmäistietoturvavaatimusten käsittelyä perustelee myös se, että viranomaisten tietoturvavaatimukset ulottuvat usein yksityiselle sektorille, esimerkiksi viranomaisen tietoja käsitteleviin tai järjestelmiä kehittäviin yrityksiin. Tämä on yksi syy, minkä vuoksi joitain viranomaisen hyviä tietoturvakäytänteitä ilmentäviä tietoturvavaatimuksia on välttämätöntä käsitellä asiayhteyksien mukaan tässä tutkimuksessa[40].

Tietoturvaan liittyviä ohjeistuksia, suosituksia ja viitekehyksiä on paljon. Tässä tutkimuksessa ei ole tavoitteena kirjoittaa kaikista tietoturvakäytänteistä, jotka vahvistaisivat organisaation tietoturvaa parhaimmaksi mahdolliseksi. Tässä tutkimuksessa on tavoitteena nostaa esiin tärkeimpiä ja yleisimpiä tietoturvakäytänteitä, joita hyvän tietoturvatason omaavat organisaatiot huomioivat toiminnassaan niin sanottuina minimikäytänteinä. Esimerkkikriteeristönä käytetään muun muassa Katakri 2020 -auditointikriteeristöä, koska se on hyvä esimerkki käytännesäännöistä, joissa suoraan viitataan velvoittavaan lainsäädäntöön.

Tutkimuksessa on yleisellä tasolla käsitelty organisaation johdon ja muiden työntekijöiden määriteltyjä ja dokumentoituja tietoturvavastuita sekä vastuuttamista osana hyviä tietoturvallisia käytänteitä ja sääntelyjärjestelmän vaatimuksia[41]. Tutkimuksen ulkopuolelle on kuitenkin rajattu yksittäisten roolien ja työtehtävien tarkastelu organisaation tietoturvaa lisäävinä tekijöinä. Organisaation tietoturvan ei kuuluisi olla henkilöityneenä ainoastaan yksittäisille henkilöille tai roolituksille. Lisäksi eri henkilöiden tietoturvaosaaminen voi rooleissaan vaihdella suuresti, minkä takia ei voi yleistää, että tietty rooli takaisi paremman tietoturvan organisaatiossa[42]. Esimerkiksi tietosuojavastaavan roolia ei ole käsitelty yksityiskohtai-

[39] Viranomaisten tietoturvan vähimmäisvaatimukset ovat lainsäädännössä määritelty tiedonhallintalain 4 luvussa. Ks. Valtiovarainministeriön julkaisuja 2024:19 (korvannut valtionvarainministeriön julkaisuja 2021:65), joka sisältää suosituksena yksityiskohtaisemmat ohjeet tiedonhallintalain tietoturvan vähimmäisvaatimuksien noudattamiseksi.
[40] On myös todettu, että sääntely-ympäristön kehittyessä, selkeää jakoa julkisoikeudellisen ja yksityisoikeudellisen tietoturvasääntelyn osalta on entistä vaikeampaa tehdä (Voutilainen 2023:23).
[41] Vastuuasioita on käsitelty luvussa 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).
[42] Esimerkiksi tietoturvaan liittyviä rooleja saatetaan joissain organisaatioissa organisoida pelkästään sisäisten resurssien puitteissa. Ei ole tavatonta, että pienemmän organisaation toimitusjohtaja toimii tietoturvavastaavana, vaikka hänellä ei välttämättä ole työtehtävään riittävää osaamista.

sesti tutkimuksessa, vaikkakin tietosuoja-asetuksen myötä vakiintunut roolitus organisaatioissa on ollut lähtökohtaisesti tietoturvallisuutta edistävä[43].

Tietoturva on moniulotteinen käsite, joka perinteisesti jakautuu vähintään kolmeen osa-alueeseen: hallinnollinen tietoturvallisuus, fyysinen tietoturvallisuus ja tekninen tietoturvallisuus. Tässä tutkimuksessa on riskienhallintanäkökulman ja hyvää tietoturvatapaa käsittelevän teeman vuoksi tehty rajauksia fyysisen ja teknisen tietoturvan yksityiskohtaisten ratkaisujen ja hyvien käytäntöjen osalta. Esimerkiksi hyviä käytänteitä tarkasteltaessa on huomioitu fyysinen ja tekninen tietoturvallisuus menemättä kuitenkaan yksityiskohtaisiin vaatimuksiin. Myös lainsäädännön teknologianeutraalisuuden periaatteen[44] takia yksityiskohtaiset tekniset toteuttamistavat on rajattu tutkimuksesta pois ja tutkimuksessa on keskitytty enemmän hallinnollisen tietoturvan vaatimuksiin.

Riskienhallinnan osalta tutkimus rajautuu ainoastaan tietoturvaan ja tietosuojaan liittyviin riskeihin. Tällöin sellaiset riskit rajautuvat pois, jotka eivät suoraan liity tietoturvaan tai tietosuojaan, vaan ennemminkin organisaation toimintaan yleisesti (esimerkiksi sopimus- ja markkinariskit). Tutkimuksessa ei ole myöskään nostettu ylös kaikkia toimialakohtaisia tietoturva- tai turvallisuusriskien hallintaan liittyviä säännöksiä niiden valtavan määrän vuoksi, koska ne ovat hyvin samantyyppisiä.

On tunnistettu, että rikoslaki on tärkeä organisaatioihin vaikuttava tietoturvarikoksia sanktioiva säädös[45]. Siitä huolimatta tutkimuksen laajuuden rajaamiseksi rikoslain yksityiskohtainen ja laaja käsittely on jätetty tutkimuksen ulkopuolelle, sillä tämä tutkimus keskittyy nimenomaan lainsäädännössä ilmenevään hyvään tietoturvatapaan, joka sisältää vaatimuksia tietoturvan vähimmäistason toteuttamiselle organisaatioissa.

---

[43] Huomioitava kyseisen roolituksen osalta on se, että tietosuojavastaavan tulisi olla riippumaton ja välttää tehtäviä, joissa tietosuojavastaavan tulisi määritellä rekisterinpitäjän tekemiä henkilötietojen käsittelyn keinoja. Tällöin ristiriita saattaa nousta tietoturvatoimenpiteiden määrittelyssä. Tietosuojavastaavien pääasiallisena tehtävänä on edistää organisaatioiden tietosuojaa tietosuojalainsäädännön erityisasiantuntijoina sekä valvoa rekisteröityjen oikeuksien suojaa henkilötietojensa osalta - ei niinkään taata tietoturvan toteutumista. Kuitenkin tietosuojavastaavan tehtävien myötä on luonnollisesti vaikutuksia myös organisaation tietoturvatasoon.

[44] Teknologianeutraalisuuden periaatetta on myöhemmin käsitelty tässä tutkimuksessa luvussa 2.4.2 (”Muut tietoturvalainsäädäntöön liittyvät keskeiset periaatteet”).

[45] Rikoslaki ulottuu myös olennaisesti tietosuojaan.
Tietosuojalainsäädäntö voidaan jakaa ennalta estävään ja jälkikäteiseen yksityisyyden suojaa turvaavaan lainsäädäntöön, jossa ennalta estävä lainsäädäntö asettaa vaatimuksia yksityisyyden suojan turvaamiseksi ja jälkimmäinen punnitsee rikosoikeudellisesti yksityisyyden suojaan kohdistunutta loukkausta. Ks. Voutilainen 2019, s. 78.

Tutkimus on painopisteeltään *de lege lata* -tutkimus eli fokuksena on voimassa olevan oikeuden tutkiminen[46]. Tästä syystä EU-lainsäädännön ehdotusluonnoksia on lähinnä käsitelty niiden oleellisten tietoturvavaatimusten ja hyviin käytänteisiin liittyvien vaatimusten osalta, mutta niiden kokonaisvaltainen läpikäyminen on rajattu tutkimuksen ulkopuolelle. Esimerkiksi tutkimuksessa tällainen ehdotusluonnos on kyberkestävyyssäädös (COM (2022) 454 final, CRA – Cyber Resilience Act).

Tässä tutkimuksessa säännöksiä ja oikeuskäytäntöä on seurattu **31.7.2024** saakka.

1.4 Tutkimusmenetelmä ja -aineisto sekä tutkimuksen sijoittuminen

1.4.1 Tutkimus- ja tulkintametodit

Oikeustieteelle on yhteiskuntatieteiden ja humanististen tieteiden tavoin tunnusomaista metodien[47] avoimuus: yleistä ja yhdenmukaista metodisäännöstöä ei ole. Aulis Aarnio on kuvannut oikeustieteen metodia ennemminkin näkökulmaksi oikeuteen kuin laskusäännöstöksi.[48] Metodi on sekä työkalu että kuvaus[49]. Oikeustieteen tutkimusmetodi määräytyykin tutkimuskohteen ja valitun tiedonintressin mukaan[50].

Tässä tutkimuksessa kohteena on organisaatioiden hyvä tietoturvan sääntelyjärjestelmä[51]. Tarkoituksena on tietoturvaa koskevien säännösten yhteen kokoaminen sekä oikeussäännösten sisällön selvittäminen. Tutkimusmenetelmä on oikeusdogmaattinen eli lainopillinen, jolloin tutkimuksessa **tulkitaan** ja

---

[46] Ks. seuraava luku 1.4 (”Tutkimusmenetelmä ja -aineisto sekä tutkimuksen sijoittuminen”)
[47] Hirvonen 2011: 4–5; Siltala 2003: 473–474; Siltala 2001:168, 86–87. Metodit ovat tieteellisiä tutkimusmenetelmiä, joilla tieteellistä tietoa hankitaan, muodostetaan ja perustellaan. Tutkimuksen keskeisiä tekijöitä on kaksi: 1) Oivaltamisen logiikka, joka on tutkijan omaa, luovaa ja intuitiivista toimintaa; sekä 2) perustelemisen logiikka, joka on toistettavissa, yleistettävissä, tiedeyhteisösidonnaista ja sen tutkimustulosten hyväksyntä on tärkeää ollakseen tieteellinen tulos. Metodi muodostuu näiden keskeisten tekijöiden eli oivaltamisen ja perustelemisen välisestä siirtymisestä syntyneistä päättelysäännöistä.
[48] Hirvonen 2011: 7, 9; Aarnio 2006: 237; Aarnio 1997: 35–36.
[49] Saarenpää 2016b: 54.
[50] Siltala 2003: 137.
[51] Osana organisaatioiden hyvää tietoturvan sääntelyjärjestelmää esitetään myös **hyvän tietoturvatavan** muodostama kokonaisuus, joka tapahtuu arvioimalla organisaatioita velvoittavia tietoturvasäädöksiä sekä käytännesääntöjä keskenään.

systematisoidaan[52] voimassa olevaa oikeutta, sekä punnitaan ja yhteensovitetaan oikeusperiaatteita (*de lege lata* -tutkimus).[53] Tutkimuksen toisessa luvussa keskeisessä tarkastelussa ovat tietoturvan sääntelyjärjestelmän eri säädökset, jonka jälkeen kolmannessa ja neljännessä luvussa tulkinta ja systematisointi suuntautuu enemmän säännöstasolle.

Yhteiskunnan ja organisaatioiden tietoturvaongelmat ovat muuttuneet ja lisääntyneet teknologian kehittymisen, digitalisoitumisen ja globalisoitumisen myötä. Tässä tutkimuksessa tarkastellaan organisaatioiden toimintaympäristön ja lainsäädännön muutoksia osana tietoturvan sääntelyjärjestelmää sekä sääntelyjärjestelmän riittävyyttä. Tutkimusongelma määritetään ja rajataan ennemminkin yhteiskunnasta eikä ainoastaan oikeusjärjestyksestä käsin ja siksi tutkimuksessa on ongelmakeskeisiä elementtejä[54]. Ongelmakeskeinen lainoppi analysoi, miten lainsäädännöllä ratkaistaan taikka jätetään ratkaisematta sosio-oikeudellisia ja yhteiskunnallisia ongelmia, jotka ovat olleet lainsäädäntöhankkeen takana[55].

Voimassa olevan oikeuden lisäksi tutkimuksessa on viittauksia tulevaan oikeussäännöstöön, mikä on *de lege ferenda* -tutkimusta[56]. Sen sisällöstä ei ole lainopin tavoin vakiintunutta määritelmää. *De lege ferenda* -kannanotot voivat keskittyä 1) nykyisten sääntöjen epäselvyyteen tai vanhentumiseen taikka 2) tulevaisuuden lainsäädännön merkityssisältöön. Molempien vaihtoehtojen osalta keskiössä on ongelma, jota pyritään ratkaisemaan. *De lege ferenda* -tutkimus edellyttää normatiivisia valintoja ja kannanotot vaativat enemmän perusteluja kuin perinteinen oikeusdogmatiikka.[57] Tutkimuksessa *de lege ferenda* -suositukset ja kannanotot kohdistuvat sekä nykyisen sääntelyjärjestelmän ongelmallisuuteen että tulevaan lainsäädäntöön, joka ratkaisisi voimassa olevan lainsäädännön epätäydellisyyttä. Säännöstutkimuksen ohella tutkimuksessa arvioidaan yleisen tietoturvalain säätämistarvetta, jolloin tutkimus on osaltaan myös lainsäädäntötutkimusta.

---

[52] Systematisoinnilla tarkoitetaan voimassa olevien oikeusnormien järjestämistä niin, että niiden merkityssisällön selvittäminen eli tulkinta käy päinsä. Ks. Tieteen termipankki 2016.
[53] Siltala 2001: 8–17; Hirvonen 2011: 21–26; Aarnio 1982: 23.
[54] Aarnio 1982, s. 62–63; Voutilainen 2009, s. 11; ja Kangas 1997, s. 94: Ongelmakeskeinen lainoppi on kyseessä, kun jokin kuviteltu tai konkreettinen oikeusongelma on tutkimuksen lähtökohtana. Oikeudellinen ongelma voi olla esimerkiksi tulkintaopillinen, juridistekninen tai systemaattinen. Oikeudellinen ongelma on lisäksi lähes aina yhteiskunnallinen. Oikeudenalat ylittävästä tutkimuksellisesta otteesta onkin käytetty usein tätä nimitystä.
[55] Lindqvist 2018: 10–11; Kangas 1997: 94, 106–107.
[56] *De lege ferenda* -tutkimuksessa uutta lainsäädäntöä koskeva ratkaisuehdotus syntyy tulkintaan ja systematisointiin pyrkivän lainopin sivutuotteena. Ks. Kolehmainen 2016, s. 108. Vrt. Leskinen 2022: 1159, 1162–1163: Koska *de lege ferenda* -tutkimus vaatii enemmän perusteluja, ratkaisuehdotukset eivät välttämättä ole ”vain” sivutuotteita.
[57] Leskinen 2022: 1159, 1162–1163.

Tutkimuksessa tarkastellaan muuttuvan toimintaympäristön ja tietoturvasääntelyn vaikutusta yritystoimintaa harjoittavissa organisaatioissa. Siksi lainopillisen metodin ohella tutkimuksessa hyödynnetään liiketaloudellista näkökulmaa keskittyen erityisesti organisaatioiden tietoturva- ja tietosuojariskien hallintaan ja toiminnan suunnitteluun. Samalla vertaillaan olemassa olevia hyviä tietoturvakäytänteitä ja -viitekehyksiä nykylainsäädäntöön, jotta tutkimuksessa pystytään arvioimaan kattavammin lainsäädännön hyvän tietoturvatavan ja nykyisen tietoturvan sääntelyjärjestelmän sisältöä. Liiketaloudellinen näkökulma muodostuu luontaisesti, sillä teknologisessa kehityksessä menestyminen edellyttää organisaatioiden tietoturvan kokonaisvaltaista suunnittelua sekä asiakkaiden tarpeiden huomioimista turvallisten tuotteiden ja palveluiden kehittämisessä ja tarjoamisessa[58]. Samalla tutkimuksessa annetaan organisaatioille talousoikeudelliseen tutkimukseen soveltuvia normikannanoton jälkeisiä toimintasuosituksia, jotka liittyvät tietoturvasäännösten soveltamiseen.

Tutkimuksessani on käytetty erilaisia tulkintametodeja tulkintakannanottoja muodostaessa. Tulkintakannanotot keskittyvät pääosin hyvään tietoturvatapaan ja tietoturvariskien hallintaan liittyvään kansalliseen, voimassa olevaan lainsäädäntöön. Tulkintametodina on käytetty sanamuodon mukaista ja lain kielelliseen ilmiasuun kohdistuvaa tulkintaa[59]. Sanamuodon mukaisessa tulkinnassa otetaan kirjaimellisesti huomioon säädöksessä käytetty terminologia ja sen epäyhtenäisyys, ja verrataan sitä käytännön tietoturva- ja riskienhallintasanastoon. Lainsäädännön ja käytännön käsitteistön semanttiset ja loogiset ongelmat johtavat helposti tulkintaongelmiin[60], joita tässä tutkimuksessa pyritään havainnollistamaan. Näin ollen sanamuodon mukainen tulkintametodi on relevantti arvioitaessa tietoturvan sääntelyjärjestelmän käsitteistön monimerkityksellisyyttä osana ongelmakeskeistä lainoppia sekä *de lege ferenda* -kannanottoja.

Lakitekstissä olevaa ilmaisua tulisi mahdollisuuksien mukaan käyttää eri yhteyksissä samalla tavalla. Ilmaisulle ei tule antaa yleisestä kielenkäytöstä poikkeavaa merkitystä, jollei ratkaisua pystytä riittävästi perustelemaan. Jos kuitenkin

---

[58] Talousoikeudellisen informaation tutkimusohjelmassa painotetaan nimenomaan yritystoimintaa harjoittavien organisaatioiden ilmiökeskeistä oikeustutkimuksen ja liiketoiminnan yhteyttä.

[59] Sanamuodon mukainen, semanttinen tulkinta tekee tutkimuksesta lakitekstikeskeistä. Aarnio 1982, s. 61–62: Tekstikeskeisen tutkimuksen lähtökohtana on tietty ilmaisu, jolloin tulkinnan aiheena voi olla esimerkiksi lakitekstin monimerkityksisyys tai epätäsmällisyys. Tekstikeskeisen ja ongelmakeskeisen tutkimusasetelman lähtökohdat ovat erilaiset, mutta ne eivät kuitenkaan eroa olennaisesti toisistaan. Molemmat tähtäävät lain sisällön selvittämiseen.

[60] Toisinaan tulkintaongelmien kohdalla laintulkitsija saattaa joutua valitsemaan kahden tai useamman soveltuvan normin joukosta oikeudellisin perustein haluamansa (ks. Husa & Jyränki 2012, s. 84). Myös esimerkiksi perusoikeuksien tulkinnanvaraisuus saattavat aiheuttaa tulkintaongelmia.

lakitekstin terminologia poikkeaa yleisestä kielenkäytöstä, erityisterminologialla on etusija yleiseen kielenkäyttöön nähden.[61] Sanamuodon mukaisen, semanttisen tulkintateorian mukaisesti käsitteiden merkityksiä voidaan määritellä viittaamalla sen käyttöön tavanomaisissa yhteyksissä ja yleiskielen mukaisessa merkityksessä. Toisaalta tietyn käsitteen merkitys voidaan liittää myös juridistekniseen erityismerkitykseen, jolloin kielenkäytön ja oikeudellisen tulkinnan arviointikriteerit liitetään muun lainsäädännön omaksumaan terminologiaan.[62] Tässä tutkimuksessa käytetään molempia tapoja: suurimmaksi osaksi käsitteitä määritellään yleiskielen kautta, mutta myös juridisteknisen erityismerkityksen eli lainsäädännössä omaksutun terminologian kautta.

Sanamuodon mukainen, semanttinen tulkinta ei ole kuitenkaan yksin riittävä metodi: säädöksiä on lähes välttämätöntä vertailla keskenään. Näin ollen tulkintametodi on myös osaltaan systematisoivaa eli muut oikeusnormit huomioon ottavaa tulkintaa.[63] Oikeusnormeja järjestelemällä pyritään tulkitsemaan niiden merkityssisältöä.

Tietoturvaan liittyvien käsitteiden ollessa ristiriitaisia ja monimerkityksellisiä, sanamuodon mukaisen tulkinnan ohessa on pohdittava lainsäätäjän tavoitteita ja tarkoitusta, sillä tutkimuksen tarkoituksena on esittää hyvän tietoturvatavan muodostama kokonaisuus osana organisaatioiden tietoturvan sääntelyjärjestelmää. Näin ollen tutkimuksessa on myös historiallisen eli lainsäätäjän tarkoituksen huomioon ottavan tulkinnan vivahteita.

Historiallisessa tulkinnassa[64] huomioidaan lainsäätäjän tarkoitus ja sääntelytavoitteet sekä säännöksen syntyhistoria. Lainsäätäjän tarkoitus tulee lähtökohtaisesti ilmi itse säädöksessä tai lain esitöissä. Tulkintaongelmia saattaa syntyä erityisesti silloin, kun lainsäätäjä ei ole pystynyt ennakoimaan oikeudellista pulmatilannetta, joka johtuu esimerkiksi teknologian kehittymisestä ja muuttuneesta toimintaympäristöstä. Lainvalmisteluaineisto vanhenee yhteiskunnan teknisen kehityksen ja muiden muutosten takia, jolloin jo muutaman vuoden vanhat esityöt voivat olla vanhentuneita tietyillä aloilla.[65] Lainvalmistelutöiden sisältöä rasittaa yhtä lailla tulkinnanvaraisuus kuin lakitekstejäkin[66]. Lisäksi on huomioitava se, että lainsäätäjän tarkoitusta arvioitaessa joko säädöksestä tai lain esitöistä, lain esityöt sijoittuvat oikeuslähdeopissa heikosti velvoittaviin oikeuslähteisiin. Täten lainsäätäjän tarkoitus sijoittuu usein heikosti velvoittaviin oikeuslähteisiin, ellei tarkoitus

[61] Aarnio 1982: 103.
[62] Siltala 2001: 110–113.
[63] Hirvonen 2011: 36–40.
[64] Käytetään myös nimeä alkuperäisen tarkoituksen mukainen tulkinta.
[65] Siltala 2001: 113–114; Siltala 2003: 339–340; Hirvonen 2011: 36–40.
[66] Aarnio 1982: 126.

tule selkeästi ilmi itse säädöksestä, joka on vahvasti velvoittava oikeuslähde.[67] Koska tietoturvasäännöksien taustalla vaikuttaa teknologianeutraalisuuden periaate, lain tulkinnassa on usein tukeuduttava esitöihin lainsäätäjän tarkoituksen selvittämiseksi. Tutkimuksessa tehtävän organisaatioiden hyvän tietoturvan sääntelyjärjestelmän määrittelyn osalta on oleellista vertailla lainsäätäjän tarkoitusta hyviin käytänteisiin, koska nopean yhteiskunnan ja teknologian kehittymisen takia tietoturvaan liittyvä lainvalmisteluaineisto voi olla varsin vanhentunutta. Historiallinen tulkinta tukee organisaatioiden hyvän tietoturvan sääntelyjärjestelmän määrittämistä, mutta myös korostaa nykyisen sääntelyjärjestelmän ongelmia ja siten edesauttaa *de lege ferenda* -kannanottojen muodostamista.

Lainopilliselle metodille keskeistä on tulkinta, jolla pyritään selvittämään, selventämään ja ilmaisemaan oikeusnormin antamaa informaatiota oikeusnormin merkityssisällöstä. Osana lainoppia on otettava huomioon oikeuslähdeoppi, josta tulkinnan on lähdettävä liikkeelle.[68] Aarnion mallin mukaisesti ensiksi sovellettavia oikeuslähteitä ovat vahvasti velvoittavat oikeuslähteet. Etusijajärjestykseltään näiden jälkeen sovelletaan heikosti velvoittavia oikeuslähteitä sekä viimeisenä sallittuja oikeuslähteitä.[69] Tässäkin tutkimuksessa tulkinta lähtee pääsääntöisesti ensiksi liikkeelle säännöksistä, joiden ohella yksityiskohtaisempaa merkityssisältöä etsitään esimerkiksi lain esitöistä ja prejudikaateista heikommin velvoittavina oikeuslähteinä.

Lain tulkinnassa tulee huomioida myös normien etusijajärjestys[70]. Käytettävät eri tulkintamenetelmät saattavat johtaa erilaisiin tulkintakannanottoihin. Esimerkiksi perus- ja ihmisoikeusmyönteisessä tulkinnassa on korostettu arvoperusteista tulkintaa, rikosoikeudessa sananmukaista tulkintaa ja EU-oikeudessa tarkoitusperäopillista tulkintaa.[71] Lisäksi on huomioitava EU-oikeuden etusijaperiaate, jolloin ristiriitatilanteissa EU-oikeus syrjäyttää jäsenmaan kansallisen normin[72]. Tässä

[67] Aarnio 2011: 68–72.
[68] Hirvonen 2011: 36–43.
[69] Aarnio 2006: 293–306. Vahvasti velvoittavia oikeuslähteitä ovat kansainvälisen ja kansallisen oikeuden normistot sekä maantapa. Heikosti velvoittavia oikeuslähteitä ovat esimerkiksi tuomioistuinten ennakkoratkaisut eli prejudikaatit ja lain esityöt. Sallittuja oikeuslähteitä ovat oikeustiede, oikeusperiaatteet, eettiset ja moraaliset perusteet sekä hyväksyttävät argumentit.
[70] Jos oikeusnormit ovat aidossa normiristiriidassa keskenään, käytetään seuraavanlaisia ratkaisunormeja: 1) Ylempitasoinen normi syrjäyttää alempitasoisen (*Lex superior derogat legi inferiori*); 2) uudempi normi syrjäyttää aiemmin säädetyn normin (*Lex posterior derogat legi priori)*; 3) erityisnormi syrjäyttää yleisnormin (*Lex specialis derogat legi generali*); ja 4) uudempi yleisnormi ei syrjäytä aiempaa erityisnormia, ellei toisin säädetty (*Lex posterior generalis non derogat legi priori speciali*). Ks. Hirvonen 2011, s. 40–41.
[71] Hirvonen 2011, s. 40–41.
[72] EU-tuomioistuimen mukaan suoraan sovellettavat eurooppaoikeudelliset normit syrjäyttävät minkä tahansa kansallisen säädöksen ristiriitatilanteessa, jopa perustuslain.

tutkimuksessa normien etusijaa tulee punnita etenkin tietosuoja- ja tietoturvalainsäädännön välillä. Monet EU-tasolta tulleet tietoturvasäädökset ovat direktiivejä, jolloin näiden direktiivien velvoitteet on saatettu osaksi kansallista lainsäädäntöä. Tällöin suoraan sovellettavan EU:n yleisen tietosuoja-asetuksen velvoitteet syrjäyttävät alempitasoiset direktiivit ja kansalliset normit, jotka tyypillisesti sisältävät tietoturvaan liittyviä normeja.

Yhteenvetona voidaan todeta, että oikeustieteelle ominaista on metodien moninaisuus, avoimuus ja hajaantuneisuus. Tästä syystä myös tutkijan työkalupakki on laaja. Tutkijan suuressa työkalupakissa olevien metodien soveltuvuus oikeudellisen analyysin työvälineenä tulee arvioida kussakin oikeudellisessa analyysitilanteessa erikseen[73]. Oikeustieteen tutkimusmetodi määräytyy tutkimuskohteen mukaan ja tutkimusongelma rajataan yhteiskunnasta käsin. Tässä tutkimuksessa on tarkastelu yhteiskunnan teknologisen kehityksen, digitalisoitumisen ja globalisoitumisen aiheuttamia muutoksia tietoturvalainsäädäntöön sekä organisaatioiden tietoturvan toimintaympäristöön. Tämän myötä tutkimuskohteena on organisaatioiden hyvä tietoturvan sääntelyjärjestelmä. Tutkimusmetodi on oikeusdogmaattinen, mutta siinä on myös ongelmakeskeisen lainopin ja *de lege ferenda* -tutkimuksen piirteitä. *De lege ferenda* -kannanotot kohdistuvat sekä nykyisen sääntelyjärjestelmän ongelmallisuuteen että tulevaan lainsäädäntöön. Tutkimus on pääpainotukseltaan säännöstutkimusta. Lisäksi se on lainsäädäntötutkimusta, sillä valittujen tutkimusmenetelmien myötä on välttämätöntä arvioida tietoturvan yleislain tarvetta. Lainopillisten kannanottojen lisäksi tutkimuksessa tehdään talousoikeudelliseen tutkimukseen tyypillisiä normikannanoton jälkeisiä toimintasuosituksia, jotka liittyvät tietoturvasäännösten soveltamiseen hyvien tietoturvakäytänteiden mukaisesti. Täten tutkimuksessa hyödynnetään myös liiketaloudellista näkökulmaa. Tulkintametodien osalta korostuvat erityisesti sekä sanamuodon mukainen että historiallinen tulkinta, jotka tukevat ongelmakeskeisen lainopin ja *de lege ferenda* -kannanottojen muodostamista sekä organisaatioiden tietoturvan sääntelyjärjestelmän määrittämistä ja arviointia.

EU-oikeuden etusijaperiaatteeseen liittyy näkemyseroja unionin tuomioistuimen ja jäsenmaiden tuomioistuinten välillä, sillä jäsenmaiden tuomioistuimissa on noussut vastustusta tällaiselle tulkinnalle. Ks. Tieteen termipankki 2018.
EU-oikeuden tulkintavaikutus kohdistuu kansallisen oikeuden tulkintaan, jolloin vaikutuksienn huomioon ottaminen on kansallisten tuomioistuimien harteilla eli kansallista lakia tulisi tulkita niin, että se on yhteensopiva EU-säädösten merkityssisällön kanssa. EU-tuomioistuimen vakiintuneen linjauksen mukaisesti kansallista normistoa tulisi soveltaa EU-oikeus-myönteisesti riippumatta kansallisen lainsäädännön antamisen ajankohdasta. Kansallisia säännöksiä ei voida asettaa etusijalle EU-oikeuteen nähden normiristiriitatilanteessa. Ks. Lohse 2012, s. 52–53, 58.

[73] Siltala 2003: 466.

1.4.2 Tutkimusaineisto

Lainopillinen tutkimusmetodi huomioon ottaen, tämän tutkimuksen tärkein tutkimusaineisto muodostuu voimassa olevasta kansallisesta tietoturva- ja tietosuojalainsäädännöstä.

Keskeisenä aineistona ovat tietoturvallisuusnormeiksi katsottavat normit, jotka koskevat informaation, tietojenkäsittelyn ja tietoliikenteen luottamuksellisuuden, eheyden sekä käytettävyyden suojaamista, ylläpitämistä ja edistämistä. Nämä normit asettavat usein välittömiä ja välillisiä velvoitteita ryhtyä hallinnollisiin, fyysisiin ja teknisiin tietoturvatoimenpiteisiin. Tietoturvallisuusnormeihin on myös luettavissa tietoturvallisuusorganisaatioita sääntelevät normit sekä normit, jotka sääntelevät tietoturvallisuustuotteita ja -palveluita, edistävät tietoturvallisuutta tai tehostavat tietoturvallisuusvelvoitteita sekä ylläpitävät hyvää tietoturvallisuustapaa.[74] Tämän tutkimuksen rajauksien vuoksi tarkoituksena ei ole kuitenkaan käydä läpi kaikkia mahdollisia tietoturvallisuusnormeja. On myös huomioitava se, että eurooppaoikeudellinen sääntely vaikuttaa keskeisesti informaatio-oikeudellisen sääntelyn aineelliseen sisältöön[75], joten luonnollisesti tässä tutkimuksessa käytetty lähdeaineisto muodostuu EU-lainsäädännöstä. Keskeisiä, tässä tutkimuksessa tarkasteltavia, kansallisten organisaatioiden tietoturvatoimintaan vaikuttavia säädöksiä ovat EU:n yleinen tietosuoja-asetus (GDPR), verkko- ja tietoturvadirektiivi (NIS 1 -direktiivi) sekä NIS 1 -direktiivin kumonnut kyberturvallisuusdirektiivi (NIS 2 -direktiivi). EU:n ja kansallisen tason tietoturvalainsäädäntöä osana tietoturvan oikeudellista kehystä on tarkasteltu jäljempänä[76]. Lisäksi lähdeluettelon lopussa on erikseen listattu tutkimuksen keskeiset säädökset sekä EU-asetukset ja -direktiivit.

Maantapa[77], jolla tarkoitetaan tietyllä oikeudenalalla tai sananmukaisesti maassa vakiintunutta, tapaa tai käytäntöä, on tutkimukseni oikeuslähteistä vähiten käytetyin. Tämä johtuu siitä, että maantapa syrjäytyy kirjoitetun lain ollessa olemassa. Maantavasta tulee erottaa tavanomainen oikeus, mikä tarkoittaa tapaa, joka on saanut tuomioistuimen vahvistuksen osana tuomioistuimen ratkaisun perustelua[78]. Myös jäljempänä on todettu hyvää tapaa käsiteltäessä, että tavanomaiseksi oikeudeksi voidaan katsoa vakiintuneet käyttäytymismallit, joihin tietyllä toimialalla toimivat ovat sitoutuneet, vaikka ne eivät kirjoitettuun lakiin

[74] Pöysti 1999: 454.
[75] Voutilainen 2019: 16.
[76] Ks. luku 2.6 (”Tietoturvan sääntelyjärjestelmän keskeiset säädökset”)
[77] Maantavan merkitys korostuu aloilla, joilla teknisen kehittymisen nopeuden takia oikeudellinen sääntely ei pysy muuttuvan toimiympäristön perässä. Ks. Siltala 2001, s. 99.
[78] Aarnio 2011: 70–71.

sisällykään[79]. Hyvät käytänteet ovat näin osa tavanomaista oikeutta. Esimerkiksi lainsäädännön tietoturvavaatimukset jättävät teknologianeutraalisuuden periaatteen mukaisesti tulkinnanvaraa lain soveltajalle, jolloin lain ollessa epäselvä turvaudutaan tulkinnassa hyviin tietoturvallisiin käytänteisiin. Nämä puolestaan pohjautuvat pitkälti ohjeistuksien ja standardien soveltamiseen, jotka ovat usein varsin universaaleja ja kansainvälisesti tunnistettuja. Hyvät, tietoturvalliset käytänteet ovat tässä tutkimuksessa keskiössä vertaillessa lainsäädännössä ilmenevää hyvää tietoturvatapaa käytänteisiin[80].

Oikeuslähteistä lain esityöt ovat myös keskeisiä oikeuslähteitä tutkimuksessani. Tämä johtuu tutkimuksessa käytettävästä historiallisesta tulkintametodista, jolla pyritään selvittämään säännöksen taustalla oleva lainsäätäjän tarkoitus ja sääntelytavoite. Kuten aikaisemmin edellisessä alaluvussa on todettu, lain tulkinnassa (ja tutkimustyössä) on usein tukeuduttava esitöihin lainsäätäjän tarkoituksen selvittämiseksi, koska itse tietoturvasäännökset ovat varsin teknologianeutraaleja.

Edellä mainittujen oikeuslähteiden lisäksi tutkimuksessa käytetään sallittuna oikeuslähteenä tietoturvallisuuteen liittyvää oikeudellista kirjallisuutta[81] ja muuta oikeudellista informaatiota, esimerkiksi tietosuojavaltuutetun toimiston ohjeita sekä julkishallinnon ja elinkeinoelämän yhteisiä ohjeita.

Liiketaloudellisen näkökulman vuoksi tutkimuksessa hyödynnetään tietoturvallisuuteen sekä tietoturva- ja tietosuojariskien hallintaan liittyviä tutkimuksia, artikkeleita sekä muuta kirjallisuutta tutkimusaineistona. Keskeisiä lähteitä ovat myös tietoturvallisuuteen liittyvät viitekehykset ja strategiat.

1.4.3 Tutkimuksen sijoittuminen

Tämä tutkimus sijoittuu osaksi informaatio-oikeuden oikeudenalaa, johon myös tietoturvaan ja tietosuojaan liittyvä sääntely katsotaan kuuluvan. Oikeudenalana informaatio-oikeus sijoittuu julkisoikeuden ja yksityisoikeuden välimaastoon. Oikeudenalajaottelun[82] tarkoituksena on jäsentää oikeusnormien muodostamaa

[79] Huhtamäki 1992: 19–23. Kaikki tavanomainen oikeus ei kuulu vahvasti velvoittaviin oikeuslähteisiin vaan se voi kuulua osiltaan myös heikosti velvoittaviin ja sallittuihin oikeuslähteisiin.
[80] Käytänteistä, käytännesäännöistä ja standardeista lisää ks. luku 2.7 (”Tietoturvan sääntelyjärjestelmä ja hyvät käytänteet”).
[81] Oikeustieteen perustellut kannanotot, jotka ovat saaneet oikeusyhteisön hyväksynnän, ovat sallittuja oikeuslähteitä. Ks. Lohse & Viitanen 2019, s. 26.
[82] Oikeudenalajaotus on perinteisesti nojannut ajatukseen siitä, että jokaisella normistolla on paikkansa aloihin jäsennetyssä oikeuden kentässä. Yhteiskuntamme muutokset ovat kuitenkin johtaneet oikeuden fragmentoitumiseen, jolloin uusien ilmiöiden myötä joudutaan usein pohtimaan voimassa olevan oikeuden soveltamista uusiin tilanteisiin. Ks. Lohse & Viitanen 2019, s. 240–241.

oikeusjärjestystä osiin oikeusjärjestelmäksi. Informaatio-oikeus on tietojen käsittelyn ja tiedonhallinnan oikeutta ja se tutkii tiivistetysti muun muassa informaation tuottamisen, välittämisen, käsittelyn, *suojaamisen*, säilyttämisen ja markkinoinnin oikeudellista sääntelyä.[83] Omana oikeudenalanaan informaatio-oikeudesta on tullut uuden infrastruktuurin verkkoyhteiskunnassa poikkeuksellisen tärkeä ja ajankohtainen eurooppalainen oikeudenala, jonka lainsäädännöllisessä kehityksessä EU:n rooli on ollut huomattava[84].

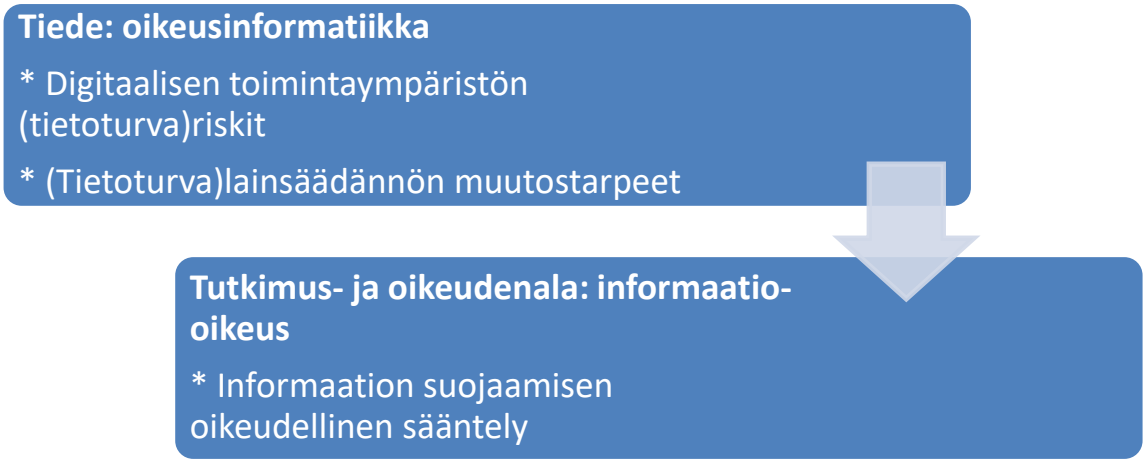
Informaatio-oikeus on oikeudenala, joka saa vaikutteita oikeusinformatiikan tutkimuksesta. Tomi Voutilaisen mukaan oikeusinformatiikka ei ole oikeudenala, koska siltä puuttuu oikeudellinen identiteetti sääntelyrakenteesta ja oikeudenaloille tyypilliset elementit toisin kuin esimerkiksi informaatio-oikeudessa. Oikeusinformatiikka on opetus- ja tutkimusala, jolloin informaatio-oikeus ei myöskään kuulu itsenäisenä oikeudenalana oikeusinformatiikan alle. Oikeusinformatiikan tutkimuksen tutkimusasetelma ei ole oikeuden sisäinen ja säännöskeskeinen, vaan siinä tutkitaan tietoteknologian hyödyntämistä oikeudellisissa toiminnoissa tai oikeudellisen tiedon hallintaa.[85] Esimerkiksi Saarenpään ja Riekkisen uusimmassa teoksessa tätä ajatusta haastetaan: informaatio-oikeus on ollut selväpiirteisenä kokonaisuutenaan oikeusinformatiikan sisällä jo 1990-luvulta ja näin on ollut kansainvälisessä katsannossakin. Teoksessa on mainittu, että suomalaisessa oikeustieteessä informaatio-oikeus mielletään nykyään myös oikeusinformatiikasta erilliseksi oikeudenalaksi. Tällöin puuttuva yhteys saattaa kuitenkin aiheuttaa uudenlaisia ymmärtämisen ongelmia. Kysymys ei pitäisi olla erillisten asioiden ongelmakeskeisestä metodisesta tarkastelusta, vaan yhteiskunnalliselta merkitykseltään tärkeästä ja pysyvämmästä oikeudenalasta osana oikeusinformatiikkaa.[86]

Koottuna näkökantana Voutilainen ei näe oikeusinformatiikkaa oikeudenalana informaatio-oikeuden tavoin vaan tutkimus- ja opetusalana, jonka alle informaatio-oikeus ei kuulu. Saarenpään ja Riekkisen mukaan oikeusinformatiikka on puolestaan tiede, jonka erityinen osa voidaan jakaa neljään toisistaan poikkeavaan tutkimus- ja opetusalaan: oikeudellinen tietojenkäsittely, oikeudellisen informaation tutkimus, informaatio-oikeus ja tietotekniikkaoikeus[87]. Ajan saatossa informaatio-oikeudesta on muotoutunut tutkimus- ja opetusalasta oma oikeudenalansa, joka on tärkeä ja erittäin ajankohtainen. Siitä kaikki ovat yhtä mieltä. Voutilaisen edellä esitetty näkökulma on kovin kapea-alainen, kun taas Saarenpään näkökulma on

[83] Voutilainen 2012: 27, 29; Saarenpää 2016a: 211; Voutilainen 2019: 15; Saarenpää & Riekkinen 2023: 170.
[84] Saarenpää & Riekkinen 2023: 28, 165.
[85] Voutilainen 2009: 17; Voutilainen 2012: 45; Voutilainen 2019: 53–54.
[86] Saarenpää & Riekkinen 2023: 33, 165, 170
[87] Saarenpää & Riekkinen 2023: 36–37.

laaja-alaisempi sekä kansainvälisesti ja laajasti hyväksytty erityisesti Pohjoismaissa.

Saarenpään mukaan oikeusinformatiikka on yksi digitaalisen toimintaympäristön riskejä tutkivista tieteistä, mutta sillä on muitakin tutkimusaiheita, kuten informaation yhteiskunnallisen merkityksen, lainsäädännön muutostarpeen, tietovarantojen käytön sekä tietojärjestelmien ja verkkojen käyttömahdollisuuksien tutkimus.[88] Tämä tutkimus yhtä lailla tutkii tietoturvaan liittyvän lainsäädännön muutostarpeita sekä pyrkii tunnistamaan digitaalisen ympäristön tietoturvariskejä. Näin ollen tutkimukseni on yhtä lailla oikeusinformatiikan tutkimus. Lisäksi tietoturva- ja tietosuojanäkökulman vuoksi tutkimukseni sijoittuu osaksi informaatio-oikeuden tutkimus- ja oikeudenalaa, sillä informaatio-oikeuden puitteissa tutkitaan informaation suojaamisen oikeudellista sääntelyä. Täten tutkimukseni sijoittuu oikeusinformatiikan tutkimuksen alle osaksi informaatio-oikeuden tutkimus- ja oikeudenalaa. Näkökantani mukaan informaatio-oikeutta ei voi, eikä pysty erottamaan oikeusinformatiikasta erilliseksi.



Kuvio 2. Tämän tutkimuksen sijoittuminen

Informaatio-oikeuden yksi keskeinen tehtävä on tunnistaa tietoon ja tietojen käsittelyyn liittyviä ristiriitoja suhteessa perusoikeuksiin sekä ratkaista niitä[89]. Perusoikeuksien sekä tietoturvan ja tietosuojan suhdetta käsittelevän näkökulman vuoksi tämä tutkimus kiinnittyy oikeudenalajaottelussa osittain myös valtiosääntöoikeuteen.

[88] Saarenpää 2016a: 82, 95; Saarenpää & Riekkinen 2023: 35.
[89] Voutilainen 2019: 18.

Yhteiskuntamme muuttuminen ja sen myötä syntyneet uudet ilmiöt merkitsevät uusia oikeudellisia ongelmia, jotka eivät ole usein sovitettavissa vallitsevan oikeudenalajaottelun mukaisiin siiloihin[90]. Tietoturvalainsäädäntö on informaatio-oikeuden lisäksi osa tietotekniikkaoikeutta, jonka puitteissa tutkitaan tietotekniikan sekä sen tuotteiden ja palveluiden kehittämiseen, käyttöönottoon ja käyttämiseen liittyvää oikeudellista sääntelyä ja tulkintaongelmia. Tietotekniikkaoikeuden keskeisiä painopistealueita ovat muun muassa tietotekniikkarikokset ja tietoturvallisuus, tietosuojalainsäädäntö ja julkisuus, tietotekniikan vastuukysymykset, sähköisen viestinnän palvelut, IT-sopimukset, internet-oikeus, sähköinen asiointi viranomaistoiminnassa ja sähköiset todisteet.[91] Näiden näkökulmien myötä tutkimus sijoittuu osittain myös tietotekniikkaoikeuden alle.

Informaatio- ja tietotekniikkaoikeuden välinen rajanveto on vaikeaa, sillä niiden historia on lähes samanmittainen ja niitä käsitellään samankaltaisen asiantuntemuksen puitteissa. Lisäksi niillä on lainopin tasolla yhtäläisyyksiä. Tietotekniikkaoikeuden piiriin katsotaan kuuluvan ensisijaisesti sellaiset oikeudelliset kysymykset, joiden ratkaiseminen tai käsittely vaatii niihin liittyvien tietoteknisten seikkojen ja erityissääntelyn ymmärtämistä.[92]

Tutkimuksessani korostuu myös talousoikeudellisen informaation tärkeys ja sen vaikuttavuus organisaatioiden toimintaan. Talousoikeudessa oikeudellisia kysymyksiä tarkastellaan yritystoiminnan näkökulmasta ja keskipisteenä on usein yritystoiminnan suunnittelu juridiikkaa hyödyntämällä[93]. Tietoturvaan liittyvät oikeudelliset kysymykset omaavat keskeisen liittymäkohdan talousoikeuteen, koska lain edellyttämien vähimmäistietoturvavaatimusten tulisi olla yritystoimintaa harjoittavien organisaatioiden toiminnan perussuunnittelua. Näin ollen tutkimukseni tukee organisaatioiden toiminnan kehittämistä tietoturvan ja riskienhallinnan saralla.

Liiketaloudellisia tietoturvaan liittyviä tutkimuksia löytyy kiitettävästi. Myös EU:n yleisen tietosuoja-asetuksen myötä tietosuojaan liittyvien tutkimusten määrä on lisääntynyt viime vuosien aikana. Sen sijaan ajankohtaisia, tietoturvalainsäädäntöön keskittyviä tutkimuksia löytyy vähemmän, mikä lisää tutkimukseni merkityksellisyyttä. Tässä tutkimuksessa hyödynnettyjä ajankohtaisia tietoturvaan liittyviä väitöstutkimuksia ovat olleet muun muassa Korjan väitöskirja *”Biometrinen tunnistaminen ja henkilötietojen suoja – tutkimus biometristen tietojen lainsäädännöllisestä asemasta”* vuodelta 2016, Hildénin väitöskirja *”The politics of datafication: The influence of lobbyist on the EU’s data protection reform and its*

[90] Lohse & Viitanen 2019: 241.
[91] Ks. Vaasan yliopiston opinto-opas 2023–2024: Informaatio- ja tietotekniikkaoikeus.
[92] Saarenpää 2016a: 131, 211, 247–250; Voutilainen 2012: 28, 35.
[93] Vaasan yliopiston opinto-opas 2023–2024: Informaatio- ja tietotekniikkaoikeus.

consequences for the legitimacy of the general data protection regulation" vuodelta 2019, Riekkisen väitöskirja *"Sähköiset todisteet rikosprosessissa – Tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaareen"* vuodelta 2019, Taluksen väitöskirja "*From simply sharing the cage to living together: reconciling the right of public access to documents with the protection of personal data in the European legal framework"* vuodelta 2019, Laurikkalan väitöskirja *Virkasalaisuusrikokset - Tutkimus rikoslain 40 luvun 5 §:n virkasalaisuusrikostunnusmerkistöjen sisällöstä ja muutostarpeista* vuodelta 2020 sekä Salmisen väitöskirja "*Et nää on näitä meiän kyberhyökkäyksiä nämä – The government of one and all in everyday digital security in Finnish Lapland"* vuodelta 2022.

1.5 Hyvä tapa tietoturvan sääntelyjärjestelmän elementtinä

Koska tässä tutkimuksessa on tarkoituksena esittää hyvän tietoturvatavan muodostama kokonaisuus osana hyvää tietoturvan sääntelyjärjestelmää, on syytä täsmentää, mitä hyvällä tavalla yleisesti ottaen on tarkoitettu lainsäädännössä sekä miten hyvä tietoturvatapa on ilmennyt aikaisemmin lainsäädännössä. Tässä tutkimuksessa hyvä tapa tukee hyvän tietoturvatavan määrittämistä sekä yhtä lailla hyvien käytänteiden arviointia.

Hyvä tapa -käsitettä on käytetty lisämääreenä säädännäisessä oikeudessa siten, että varsinaisen hyvän tavan säännöksien sisältö on tarkoitettu muodostuvaksi ajan, tilanteen ja niiden asettamien vaatimusten mukaisesti. Hyvä tapa voi olla myös ilmentymä oikeusperiaatteista. Hyvän tavan säännösten ja niiden johdosta annettujen tarkentavien soft law -tyyppisten normien ja suositusten kokonaisuudet muodostavat säädännäisestä oikeudesta ja tapaoikeudesta koostuvia elementtejä.[94] Hyvä tapa voidaan ymmärtää sekä moraaliseksi että oikeudelliseksi normiksi. Tästä moraalisen normin noudattaminen perustuu yleiseen käsitykseen yhteiskunnassa oikeanlaisesta käytöksestä, kun taas oikeudellisen normin noudattaminen perustuu velvollisuuteen noudattaa lakia.[95] Osa hyvistä tavoista perustuu lainsäädäntöön ja osa on voimassa puhtaasti eettisin perustein, josta seuraa se, että tapanormien sitovuuden aste vaihtelee sääntelyn mukaan. Näin ollen on olemassa lakisääteisiä hyviä tapoja ja on lakiin perustumattomia hyviä tapoja, jotka liittyvät enemmän ammattikuntien tapaohjeisiin.[96] Lakiin perustumattomien

[94] Voutilainen 2006a: 26–27; Pöysti 1997: 548.
[95] Streng 2007: 145; Huhtamäki 1992: 17.
[96] Sarja 2011: 134. Lakisääteisiä hyviä tapoja ovat esimerkiksi hyvä hallintotapa. Lakiin perustumattomia, ammattikunnille tyypillisiä hyviä tapoja ovat esimerkiksi hyvä asianajajatapa, hyvä isännöintitapa ja hyvä journalistitapa.

tapa- tai ammattieettisten ohjeiden oikeuslähdeopillinen asema on usein kiistanalainen, sillä ne eivät ole lainsäätäjän hyväksymiä, mutta ammattiryhmän keskuudessa niitä saatetaan pitää velvoittavuudeltaan lähes lakiin rinnastuvina. Toisinaan ammattieettiset ohjeet ovat toimineet mallina lainsäädännölle.[97]

Hyvät tavat ovat arvosidonnaisia ja täten esimerkiksi ammattiryhmien hyvän tavan määrittelytyö tulisi tapahtua ammattikunnan omassa keskuudessa eikä ulkopuolisen tahon toimesta.[98] Hyvän tavan määrittelemisen apuna voi myös käyttää perustuslain perusoikeussäännöksiä, sillä ne ilmentävät suomalaisen yhteiskunnan perustuvanlaatuisia arvoja. Perusoikeuksien merkitys korostuu etenkin sellaisissa tilanteissa, joihin ei liity laintasoista sääntelyä.[99] Hyvästä tietoturvatavasta tulisi heijastua perusoikeussäännösten perimmäiset arvot, kuten oikeus yksityisyyteen ja henkilötietojen suojaan sekä oikeus turvallisuuteen ja omaisuuden suojaan[100].

Hyvillä tavoilla voidaan täyttää lainsäädännön aukkoja ja selkeyttää toimintatapoja tilanteissa, joista ei ylipäätään ole mahdollista säätää kattavasti[101]. Hyvä tapa on ollut eri säädöksien tulkinnoissa mukana mittapuuna ja yleisenä tulkinnallisena tekijänä, jolloin esimerkiksi täsmällisten sääntöjen puuttuessa on pyrittävä toimimaan hyvän tavan mukaan[102]. Lisäksi hyvät käytännöt tietyllä toimialalla vaikuttavat päätöksentekoon tuomioistuinratkaisuissa[103]. Hyvää tapaa tulee hyödyntää erityisesti teknologianeutraalisti säädetyn tietoturva- ja tietosuojalainsäädännön tulkinnassa. Esimerkiksi tietosuojavaltuutetun ratkaisuissa ilmenee hyvä tietoturvatapa käytännön tasolla, kuten **ratkaisussa TSV 15.11.2022**, jossa todettiin, ettei vahva salasanasuojaus ollut riittävä keino erityisten henkilötietojen suojaamiseksi[104]. Näin ollen hyvä tapa tulee ilmi täsmällisten sääntöjen puuttuessa hyvinä käytänteinä tietyllä alalla eli osana tavanomaista oikeutta.

---

[97] Nieminen 2020: 1083–1084.
[98] Sarja 2011: 161.
Ammattiryhmien eettiset ohjeistukset ovat aikaan ja olosuhteisiin sovitettua moraalia. Luontainen moraalikoodi on korvautunut oikeusnormeilla. Sääntely on sitä monimutkaisempaa, mitä ohuemmaksi ihmisten luontainen moraalikoodi käy. Ks. Aarnio 2010, s. 541–542, 547.
[99] Meri 2023: 67, 73–74.
[100] Näitä oikeuksia on käsitelty yksityiskohtaisemmin luvussa 2.5 (”Tietoturva perusoikeutena osana tietoturvan sääntelyjärjestelmää”).
[101] Sarja 2011: 162.
[102] Saarenpää 2015: 349.
[103] Streng 2007: 147–148.
[104] TSV 15.11.2022, dnro 4022/171/22. Ks. lisää myös luvusta 4.4.3 (”Pääsynhallintavaatimukset tietoturvan sääntelyjärjestelmässä”).

Tavanomaiseksi oikeudeksi voidaan maantavan[105] lailla katsoa vakiintuneet käyttäytymismallit, joihin tietyllä toimialalla toimivat ovat sitoutuneet, vaikka ne eivät kirjoitettuun lakiin sisällykään. Maan tapa on katsottu oikeuslähdeopissa kirjoitetun lain jälkeen vahvasti velvoittavaksi, toissijaiseksi oikeuslähteeksi ollessaan kohtuullinen. Kaikki tavanomainen oikeus ei kuitenkaan välttämättä kuulu vahvasti velvoittaviin oikeuslähteisiin, vaan se voi kuulua osiltaan myös heikosti velvoittaviin ja sallittuihin oikeuslähteisiin. Liiketapa on pidettävä erillään maantavasta ja tavanomaisesta oikeudesta, sillä sitä ei pidetä samalla tapaa puolueettomana oikeutena eikä itsenäisenä oikeuslähteenä. Näin ollen tiettyä alaa koskevan tapaoikeuden asemaa on soveltamistilanteissa tarkoin harkittava oikeuslähdeopin kannalta.[106]

Hyvää tapaa koskevat normit ovat sääntelyn instrumentteina lisääntymässä[107]. Hyvää tapaa on säädelty eri laeissa yleensä velvoittaen joko toimimaan hyvän tavan mukaisesti taikka mitä tapahtuu hyvän tavan noudattamatta jättämisestä[108]. Käsitteen *”hyvä”* osalta onkin todettu sen viittaavan juridisesti esimerkiksi hyvään tapaan, jolloin myös hyvän rikkomiseen liittyy juridisia seurauksia, esimerkiksi vahingonkorvausvelvollisuus[109].

Hyvän tavan vastaisuudesta on annettu useita erityissäännöksiä, jotka viittaavat tietyn oikeudenalan tai sopimustyypin mukaisesta hyvän tavan vastaisuudesta.

> Esimerkkinä hyvän liiketavan vastaisuus. Hyvästä liiketavasta voidaan käyttää monenlaisia ilmaisuja eikä niillä tarkoiteta aina samanlaista hyvää tapaa. Toisinaan hyvä liiketapa voi merkitä esimerkiksi kyseisellä alalla toimivien kesken noudatettavaa hyvää tapaa. Huomioitava kuitenkin on, että kaikki määrätyllä alalla noudatettavat vakiintuneet tavat eivät välttämättä ole hyviä, mutta ne saattavat olla sekä oikeudenmukaisia että kohtuullisia ja sitä kautta hyviä.[110] Hyvän liiketavan vastaisuudesta on säädetty laissa sopimattomasta menettelystä elinkeinotoiminnassa (SopMenL. 1§), jonka mukaan elinkeinotoiminnassa ei saa käyttää hyvän liiketavan vastaista tai muutoin toisen elinkeinonharjoittajan kannalta sopimatonta menettelyä. Menettelyiden erotteleminen hyvän liiketavan mukaisiin ja vastaisiin ei käytännössä ole aina helppoa. Lain esitöiden mukaan säännöksen tulkinta on tehtävä ensi sijassa elinkeinotoimintaa harjoittavien henkilöiden sekä yritysten välisten yleisten menettelytapojen ja arvostusten perusteella.

[105] Alueellisen maantavan sijaan voidaan pitää nykyaikaan paremmin soveltuvana oikeuslähteenä käsitteellisesti laajempaa tavanomaista oikeutta.
[106] Huhtamäki 1992: 19–23.
[107] Pöysti 1997: 548.
[108] Saarnilehto 1992: 15; ks. myös Saarnilehto 1993: 173.
[109] Salo 2015: 3–4.
[110] Ämmälä 1993: 10, 17, 19.

> Lisäksi säännöstä sovelletaan myös sellaiseen menettelyyn, joka voidaan katsoa muilla perusteilla sopimattomaksi olematta kuitenkaan hyvän liiketavan vastaista.[111] Hyvän tavan lisämäärittelyllä erityisalan mukaan ei ole kuitenkaan kovin suurta merkitystä säännöksen tulkinnassa. Arvioitaessa tointa tai menettelyä joudutaan kiinnittämään huomiota toimen tai menettelyn tekohetken olosuhteisiin sekä tekijään huomioon ottaen myös eri toimialojen omat käsitykset kunnian vaatimuksista.[112]

Hyvän tavan vastaiset toimet liittyvät usein vääränlaisten tietojen antamiseen tai oikeanlaisten tietojen antamatta jättämiseen. Hyvän tavan vastaisuus saattaa ilmetä myös kohtuuttomuutena, ja näitä kahta erillisinä periaatteina voikin olla vaikea erottaa toisistaan. Hyvän tavan vastaisuuden kieltäminen ei täysin kerro siitä, mikä on hyvän tavan vastaista. Näin ollen tilanteen mukaan voidaan todeta, että hyvän tavan vastaista sekä hyvän tavan mukaista menettelyä voi olla monenlaista.[113] Hyvän tavan vastaisuus on hyvin elävä, vaihteleva ja tulkinnallinen käsite, jolloin sen määrittäminen yleispätevästi ei ole mahdollista. Hyvän tavan vastaisuus onkin kiinni usein arvo- ja moraalikäsityksistä.[114]

Kuten edellä todettiin, hyvän tavan vastaisuuden kieltävät normit liittyvät usein tietojen antamiseen: esimerkiksi tietojen antamatta jättäminen saattaa olla hyvän tavan vastaista. Harhaanjohtavien tietojen antaminen on yleensä myös kielletty erikseen lainsäädännössä.[115] Tietoturvalla usein suojataan tietoja ja myös annettavien tietojen tulee olla eheitä ja saatavilla. Tietojen antamatta jättäminen tai harhaanjohtavien tietojen antaminen ovat hyvän tavan vastaista menettelyä. Laajassa merkityksessä tällainen toiminta on myös hyvän tietoturvatavan vastaista, mikäli esimerkiksi toiminta toteutuisi laiminlyömällä tahallaan tietojärjestelmässä olevien tietojen tietoturvaa. Tällaista voisi olla muun muassa tietojen vääränlainen luokittelu, jos esimerkiksi salassa pidettävät tiedot luokiteltaisiinkin julkisiksi. Täten hyvän tietoturvatavan vastaista tulisi olla muun muassa sellainen toiminta, jossa tietojen eheyteen tai saatavuuteen vaikutetaan tahallisesti.

Käytännössä informaatiota suojaavat suoraan tietoturvaan liittyvät säännökset, liikesalaisuuksia ja immateriaalioikeuksia suojaavat säännökset sekä organisaatioiden väliset sopimukset ja siihen liittyvä tapaoikeus. Näin ollen huomioitava on, että informaation suoja ei liity ainoastaan hyvään tietoturvatapaan, vaan siihen voi liittyä myös muita aspekteja.

---

[111] Pohjonen 1993: 138, 160.
[112] Saarnilehto 1993: 179.
[113] Saarnilehto 1992: 8–10, 13–14.
[114] Ämmälä 1993: 5, 7.
[115] Saarnilehto 1992: 10.

> Esimerkiksi välillisesti neuvotteluissa luovutettavaa informaatiota voi suojata hyvän liiketavan vaatimus, hyvä tapa oikeusperiaatteena sekä sopimussuhteisiin liittyvä lojaliteettiperiaate. Täten hyvä (liike)tapa voi myös välillisesti suojata informaatiota.[116]

Täsmällistä ja yleistä säännöstä hyvän tavan vastaisuudesta ei ole Suomen lainsäädännössä. Näin ollen hyvää tapaa säännellään yleisen oikeusperiaatteen sekä toisaalta erityisnormien kautta. Elinkeinotoimintaa suojaavat säännökset ovat usein väljiä ja siten myös tulkinnanvaraisia. Hyvän tavan tarkan sisällön määrittelyn puuttuminen johtuu siitä, että hyvä tapa on tapaoikeutta, jolle on ominaista sen sisällön kirjoittamattomuus lakiin. Tapaoikeutta ei voi kirjoittaa lakiin, koska se muuttuu käytäntöjen muuttuessa.[117] On myös määrittelykysymys jääkö hyvän ja pahan tavan väliin neutraalialue, jossa ei ole kysymys hyvästä eikä pahasta tavasta[118]. Säännösten esitöissä ja oikeuskirjallisuudessa on usein pyritty löytämään esimerkkejä hyvästä tavasta säännöksiä tulkittaessa, mutta kuitenkin vasta oikeuskäytännössä hyvän tavan periaate saa lopullisen sisältönsä[119].

Hyvän tavan käsite on avoin, arvostusta edellyttävä ilmaisu ja tunnusmerkki. Tälle käsitteelle on soveltamistilanteessa annettava merkityssisältö asianomaisen säännöksen soveltajan toimesta.[120] Hyvän tavan mukainen toiminta on usein se tapa toimia, mikä katsotaan normaaliksi eli vakiintuneeksi tavaksi tai käytännöksi toimia. Useimmiten vakiintuneet tavat ovat alalla kohtuullisia ja oikeudenmukaisia. Hyvän tavan oikeusperiaatteelle on ominaista, että se tarkoittaa kaikille samaa. Yleinen hyvä tapa voi kuitenkin myös muuttua, koska käytäntö muuttaa sitä. Lisäksi hyvän tavan periaatteen tarkkarajaista sisältöä on vaikea muodostaa sekä erottaa muista periaatteista kuten kohtuullisuuden periaatteesta.[121]

Hyvästä tietoturvatavasta ei ole säädetty suoraan lainsäädännössä eikä sillä ole siten samanlaista oikeudellista velvoittavuutta kuin esimerkiksi lainsäädäntöön perustuvalla hyvällä hallintotavalla (PL 21 § ja hallintolain 434/2003 2 luku) tai hyvällä liiketavalla (laki sopimattomasta menettelystä elinkeinotoiminnassa 1061/1978, 1§). Toisaalta hyvä tietoturvatapa ei myöskään ilmene suoraan lakiin perustumattomista, ammattikuntakohtaisista hyvistä tavoista. Oikeuskirjallisuudessa on täsmennetty, että ammattikunnille tyypillisiä piirteitä ovat ainakin 1) tietty koulutus ja käytännön kokemus, 2) sitoutuminen ammattikunnan olemassaolon kannalta elintärkeän yhteiskunnallisen funktion toteuttamiseen, 3)

---

[116] Kaasalainen 2008: 14, 43.
[117] Kaasalainen 2008: 51; Ämmälä 1993: 5.
[118] Saarnilehto 1993: 174.
[119] Pohjonen 1993: 138.
[120] Aarnio 1989: 168–169.
[121] Kaasalainen 2008: 79, 84; Ämmälä 1993: 19; Saarnilehto 1992: 15–16.

itsesääntely, 4) rajoitettu jäsenyys ja 5) lainsäädännössä tunnustettu asema[122]. Tietoturva-alan ammattilaisten koulutustaustat vaihtelevat: osa on itseoppineita ja nuoremmat alan osaajat ovat saattaneet valmistua esimerkiksi Jyväskylän yliopistosta kyberturvallisuuden maisteriohjelmasta tai Laureasta kybertradenomiksi. Tietoturvalainsäädännössä ei siis ole suoraan kelpoisuusvaatimuksia tietoturva-alan ammattilaisille, mutta voidaan todeta, että heidän työnsä on merkityksellistä yhteiskunnan toimivuuden sekä yksilöiden ja organisaatioiden luottamuksellisten tietojen suojaamisen kannalta. Tietoturvatoimenpiteet perustuvat pitkälti lainsäädännön velvoitteisiin ja alan hyviin käytänteisiin. Toisaalta tietoturva-alan ammattilaisilla, esimerkiksi asiantuntijoilla ja tietoturvapäälliköillä, ei ole ammattikuntaan liittyvää rajoitettua jäsenyyttä eikä lainsäädännössä tunnustettua asemaa. Näillä perustein hyvä tietoturvatapa ei suoraan linkity ammattikuntakohtaisiin tapaohjeisiin, koska varsinaista ammattikuntaa ei ole tunnistettavissa oikeuskirjallisuuden kriteereistä tulkittuna[123]. Etiikkaan perustuvia tietoturvaohjeita huomioidaan käytännön työssä itseasiassa valitettavan vähän[124]. Organisaatioissa tietoturvatyötä rakennetaan pitkälti erilaisten standardien, käytännesääntöjen ja ohjeistuksien pohjalta, joissa kaikissa, esimerkiksi hallinnollisen tietoturvan näkökulmasta, toistuvat samat vähimmäismenettelyt. Toisessa organisaatiossa saatetaan ottaa käyttöön Kybermittari[125] tietoturvan kehittämisen työkaluksi, kun taas toisessa organisaatiossa hyödynnetään ISO/IEC 27001-standardin vaatimuksia taikka Katakri 2020-auditointikriteeristöä[126]. Kuitenkaan yhtä sellaista

[122] Sarja 2011: 144.

[123] Ammattikuntakohtaisilla tapaohjeilla määritetään ammattikunnan hyvän edustajan ihannetyyppi ja ammatillisille tapaohjeille voidaan löytää yhteisten tavoitteiden ohella myös yhteisiä sisällöllisiä piirteitä. Niissä otetaan huomioon ammatin edellyttämä tieto, taito ja kokemus. Toiseksi niissä määritellään ammattikunnan edustajan oikeudet ja velvollisuudet. Ks. Sarja 2011, s. 144.
Tapaohjeilla pyritään ohjeistamaan sitä, kuinka ammattia harjoitettaessa toimitaan oikein ja vältetään sellaiset väärät toimintatavat, jotka eivät välttämättä ole lainvastaisia, mutta jotka saattavat heikentää kansalaisten luottamusta kyseisen ammattikunnan toimintaan. Tapaohjeilla voidaan myös välittää informaatiota mm. ammattikunnan jäsenille tietoa lain sisällöstä ja lainvalmisteluasiakirjoissa ilmaistuista tavoitteista. Ks. Sarja 2011, s. 136.

[124] Esimerkiksi OEDC:n digitaalisen turvallisuuden riskienhallinnan ohjeessa (ks. OECD 2022, *Recommendation of the Council on Digital Security Risk Management*, OECD/LEGAL/0479, s. 8) korostetaan ihmisoikeuksia ja fundamentaalisia arvoja: Kaikkien sidosryhmien tulee hallita digitaalisen turvallisuuden riskejä läpinäkyvällä tavalla ja johdonmukaisesti ihmisoikeuksien ja perusarvojen kanssa. Sidosryhmien tulisi toteuttaa digitaalista turvallisuutta ihmisoikeuksia ja fundamentaalisia arvoja kunnioittavasti ja tukevasti, ml. sananvapaus, vapaa tiedonkulku, tiedon ja viestinnän luottamuksellisuus, yksityisyyden ja henkilötietojen suoja, yhdistymisvapaus, syrjimättömyys, avoimuus ja oikeudenmukaisuus. Lisäksi sidosryhmien digitaalisen turvallisuuden tulisi perustua eettiseen toimintaan.

[125] Kybermittaria käytetään organisaatioissa kyberturvallisuuden arviointiin ja kehittämiseen. Se mahdollistaa myös toimialakohtaisen vertailun. Lisätietoja Kybermittarista, ks. Traficom, kyberturvallisuuskeskus 2024b.

[126] Ks. lisää käytännesäännöistä ja standardeista luvusta 2.7 (”Tietoturvan sääntelyjärjestelmä ja hyvät käytänteet”).

ammattikuntakohtaista ohjetta ei ole niin kuin journalisteilla on journalistin ohjeet ja asianajajilla hyvän asianajajatavan ohjeet.

Tämä ei kuitenkaan tarkoita, etteikö hyvää tietoturvatapaa tulisi tunnistaa lakisääteisenä hyvänä tapana osana tietoturvan sääntelyjärjestelmää. Hyvä tietoturvatapa voisi olla joustava normi, jota sisällöllisesti määrittelisi sekä lainsäädännössä tietoturvan vähimmäisvaatimukset että tuomioistuinten ratkaisut, tietoturva-alan hyvät käytännöt, käytännesäännöt sekä valvovan viranomaisen, kuten tietosuojavaltuutetun päätökset ja linjaukset.

Organisaatioita velvoittavat tietoturvasäännökset ovat hajanaisia, minkä vuoksi on vaikea muodostaa selkeää kuvaa lainsäädännön vähimmäisvaatimuksista ja nykyisestä hyvästä tietoturvatavasta. Tietoturvan näkökulmasta on kuitenkin löydettävissä tietoturvahenkisiä, hyvä tapa -vaatimuksia, joista keskeisimpiä ovat esimerkiksi **hyvän hallinnon ja hyvän sähköisen hallinnon vaatimus, hyvä tiedonhallintatapa** sekä **hyvä tietojenkäsittelytapa tai henkilötietojenkäsittelytapa.**

Hyvän hallinnon (hyvän hallintotavan) ja oikeusturvan perusteiden yleissäännökset on säädetty hallintolaissa (434/2003), jonka tarkoituksena on toteuttaa ja edistää hyvää hallintoa[127]. Hyvää hallintoa määrittäviä säännöksiä löytyy muualtakin kuin hallintolaista[128] ja lisäksi keskeinen merkitys hyvän hallinnon käsitteen määrittelemisessä on ollut valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen ratkaisuilla. Hyvä hallintotapa on ollut oikeuslähde jo ennen sen kirjaamista lainsäädäntöön. Lakiin kirjattuna se on oikeudellisesti velvoittava.[129] Hyvä ja tietoturva tulevat ilmi osana hyvän hallinnon vaatimusta[130]. Muun muassa eduskunnan oikeusasiamies on korostanut tietoturvallisuuden merkitystä osana hyvää hallintoa. Hyvän hallinnon periaatteisiin voidaan katsoa kuuluvan muun muassa Suomen perustuslaissa (731/1999) kirjattu vaatimus julkisen vallan tietojärjestelmien häiriöttömästä ja laadukkaasta toiminnasta.[131] Myös julkisuusperiaate on osa hyvän hallinnon perusoikeudellisia vaatimuksia[132], mihin liittyy osaltaan sisäänrakennettu vaatimus viranomaiselle huolehtia tietoturvallisuudesta, jotta asiakirjat olisivat saatavilla oikea-aikaisesti ja oikeutetuille henkilöille.

---

[127] Voutilainen 2006a: 23.
[128] Esimerkiksi tiedonhallintalain 1 §:ssä on määritelty hyvän hallinnon oheen palvelujen tarjoaminen tuloksellisesti ja laadukkaasti.
[129] Sarja 2011: 133–134, 140.
[130] Ks. myös luku 2.5.6 (”Perusoikeuksien turvaaminen oikeusvaltiossa ja hyvä hallinto”).
[131] Saarenpää 2016a: 82, 136.
[132] Ks. Voutilainen 2006a: 46–47.

Nykyisessä järjestelmäriippuvaisessa yhteiskunnassa hyvän hallintotavan yhtenä ulottuvuutena on hyvä sähköinen hallinto. Hyvän sähköisen hallinnon vaatimus ei kuitenkaan ole sellaisenaan lakisääteinen hyvä tapa niin kuin hyvä hallintotapa on.

> Tietoturvallisuus on yksi tärkeimmistä *hyvän sähköisen hallinnon*[133] elementeistä. Sähköisen hallinnon tietoturvallisuusvaatimuksia voidaan tarkastella perusoikeuksien näkökulmasta. Esimerkiksi perustuslain 10 § turvaa kansalaisen oikeuden henkilötietojensa suojaan sekä asettaa viranomaiselle velvollisuuden huolehtia, että jokaisen yksityiselämä, kunnia ja kotirauha turvataan. Perustuslain 7 §:ssä on säädetty oikeudesta turvallisuuteen ja 10.2 §:ssä oikeudesta luottamukselliseen viestintään. Tietoturvallisuusvaatimukset nousevat esiin myös perustuslain 12.2 §:n julkisuuden turvaamisesta eli oikeudesta saada tieto viranomaisen asiakirjasta. Perusoikeuksien turvaamissäännöksen eli perustuslain 22 § velvoittaa viranomaista ottamaan huomioon toiminnassaan tietoturvallisuuden.[134] On todettu, että hyvä sähköinen hallinto huomioi myös suhteellisuusperiaatteen eli tietoturvatoimet tulisi ratkaista tarkoituksenmukaisella tavalla toimintakohtaisesti ja perusteellisesti[135]. Toimintakohtaisuus on ”vanhentunutta” ajattelua ottaen huomioon nykyinen teknologinen ympäristö, lainsäädännön kehitys ja hyvät käytänteet. Suhteellisuusperiaatteen tulisi heijastaa riskiperustaista lähestymistapaa, jolloin riittävät tietoturvatoimenpiteet määriteltäisiin riskien hallitsemiseksi. Yhtä lailla lainsäädännössä toimintakohtaiset tai toimialakohtaiset tietoturvavaatimukset eivät ole riittäviä suojaamaan tietoa ja yksilöiden perusoikeuksia nykyisessä verkkoyhteiskunnassa, jossa palvelut ja toimijat ovat linkittyneet toisiinsa. Myös nykyinen oikeuskanslerimme Tuomas Pöysti on korostanut yhdeksi sähköisen hallinnon haasteeksi ja oikeudelliseksi vaaraksi lainsäädännön

---

[133] Sähköinen hallinto tarkoittaa teknisesti sitä, että se koostuu sähköisistä asiointipalveluista, sähköisestä asianhallintajärjestelmästä, perus- ja taustajärjestelmistä sekä niitä yhdistävistä tietoverkoista ja palveluita käyttävistä toimijoista, kuten viranomaisista ja viranomaisten asiakkaita. Ks. Voutilainen 2006a, s. 2.
Vrt. Pöysti 2010, s. 93–94, 100: Sähköisellä hallinnolla (*eGovernment, electronic Government*) tarkoitetaan yleensä tieto- ja viestintätekniikan käyttöä julkishallinnossa ja julkisten palvelujen tuottamisessa. Tästä myös astetta pidemmälle kehittynyt verkkoyhteiskunnassa toimiva ”tietohallinto” (*iGovernment, information Government*) mahdollistaa laajemman julkisen hallinnon ja palvelutuotannon toiminnan, jonka ensisijaisia muotoja ovat tiedon tuottaminen ja käsittely.

[134] Ks. Saraviita 2011, s. 153–159 (PL 7 §), 178–191 (PL 10 §), 198–209 (PL 12 §) sekä 292–297 (PL 22 §). Lisäksi: Pellonpää 2011: 281–301 (PL 7 §), Viljanen 2011: 389–411 (PL 10 §), Manninen 2011: 459–491 (PL 12 §) sekä Lavapuro & Tuori 2011: 809–820 (PL 22 §).

[135] Voutilainen 2006a: 115–118.

> sirpaloitumisen moniin säädöksiin, jotka eivät muodosta johdonmukaista kokonaisuutta[136].

Hyvän hallintotavan sisältämien tietoturvavaatimusten ohella viranomaisen toiminnan julkisuudesta säädetyn lain eli julkisuuslain (621/1999) keskeinen periaate tietoturvan osalta oli sen 18 §:ssä säädetty *hyvä tiedonhallintatapa*, johon tietoturvallisuus voitiin katsoa systemaattisesti osaksi[137]. Julkisuuslaissa säädetty hyvä tiedonhallintatapa koostui erityisesti tietoturvaperiaatteesta, mutta myös asianhallinnan perusperiaatteista, tietojärjestelmien avoimuusperiaatteista sekä tietojärjestelmien, hallinnollisten ja lainsäädännöllisten uudistusten määrittely- ja suunnitteluperiaatteista. Näin ollen viranomaisen oli huolehdittava toimintansa järjestämisestä sekä hyvän tiedonhallintatavan noudattamisen valvonnasta hallinnollisesti ja teknisesti. Hyvän tiedonhallintatavan tarkoituksena oli tällöin varmistaa, että viranomaisen tietojärjestelmien ja asiakirjojen tietojen saatavuudesta, eheydestä, käytettävyydestä ja suojaamisesta sekä muista tietojen laatuun vaikuttavista tekijöistä huolehditaan. Näin ollen kaikista tietoon liittyvistä laatuominaisuuksista oli huolehdittava tarpeellisin keinoin.[138] Hyvän tiedonhallintatavan tavoitteena oli turvata julkisuusperiaatteen toteutumisen lisäksi yksilön tiedonsaantioikeudet. Hyvä tiedonhallintatapa oli nimensä mukaisesti toimintatapa, jolloin sen toteutuminen vaati ohjeistuksen lisäksi vähintään prosessien tuntemusta ja suunnittelua, koulutusta, varmistus- ja suojausjärjestelmiä, resursointia sekä vastuiden selkeyttämistä ja jakamista.[139]

Hyvää tiedonhallintatapaa ilmentävä julkisuuslain 18 § kumottiin viranomaisen tiedonhallintalailla (906/2019), jolla tarkennettiin hyvää tiedonhallintatapaa koskevaa sääntelyä[140]. Myös asetus tietoturvallisuudesta valtionhallinnossa (tietoturvallisuusasetus, 681/2010) kumottiin tiedonhallintalain myötä. Tietoturvallisuusasetuksessa tietoturvallisuus nähtiin osana hyvää tiedonhallintatapaa, mutta kyseisen säädöksen pääfokus oli lähinnä asiakirjojen luokittelussa[141]. Näin ollen hyvän tiedonhallinnan sääntely siirtyi kauttaaltaan tiedonhallintalakiin. Tiedonhallintalakia on kuitenkin kritisoitu hyvän tiedonhallintatavan systeemisen periaatteen puuttumisesta, koska siitä saattaa aiheutua ongelmia teknologian ja sen soveltamisen kehittyessä eteenpäin[142]. Hyvä tiedonhallintatapa ei tule tiedonhallintalaista suoraan ilmi eli se ei ole samalla tavalla lakisääteinen hyvä tapa kuin

---

[136] Pöysti 2010: 98. Heikko tietoturva ja huono tiedonhallinta ovat erityisiä oikeudellisia riskejä yksityiselämän suojalle sekä oikeudelle saada tietoja (Pöysti 2010: 116–117).
[137] Pöysti 1999: 446–447, 452–453; Saarenpää 2016a: 142.
[138] Voutilainen 2006a: 47, 112; HE 30/1998 vp: 47, 79.
[139] Kiviniemi 2002: 16–18.
[140] HE 284/2018 vp: 32, 34, 121–122.
[141] Pöysti 1999: 446–447, 452–453; Saarenpää 2016a: 142.
[142] Pöysti 2023: 44.

ennen[143]. Huomioitava kuitenkin on se, että tiedonhallintalain myötä hyvän tiedonhallinnan ja tietoturvallisuuden vaatimukset ovat täsmentyneet ja parantuneet entisestään. Erityisesti tiedonhallintalain 4 luvun tietoturvavaatimukset ovat vähimmäiskriteereitä tietoturvan toteuttamiselle julkishallinnossa. Nämä kyseiset vähimmäiskriteerit ikään kuin ilmentävät hyvän tietoturvatavan vähimmäistasoa julkishallinnon osalta, mutta vaatimukset koskevat lähinnä säädöksen alaan luettuja viranomaisia. Hyvä tietoturvatapa on siis jo lähtökohtaisesti olemassa, mutta se ei ulotu velvoittavana kaikkiin organisaatioihin eikä sitä ole tiedonhallintalaissakaan säädetty suoraan lakisääteisenä hyvänä tapana. Viranomaisen hyvää tietoturvatapaa ilmentävät vähimmäisvaatimukset ovat kuitenkin hyvä esimerkki riittävästä teknologianeutraalista sääntelystä.

> Hyvän tiedonhallinnan toteuttamisesta on annettu paljon ohjeistuksia ja suosituksia muun muassa valtion tietoturvallisuuden johtoryhmän toimesta. Tietohallintotoiminnan ympärille on muodostunut tapaoikeustyyppinen sääntelymalli, joka pohjautuu osittain erilaisten standardien ja suositusten soveltamiseen ja noudattamiseen. Tällaisten normien yhteydessä puhutaan soft law -sääntelystä, joka muodostuu epäitsenäisistä oikeuslähteistä. Viranomaisen näkökulmasta tällainen sääntely on tarkoitettu ohjaamaan viranomaisen toimintaa. Soft law -normit eivät ole sinällään sitovia, mutta niiden taustalta on usein löydettävissä jokin laintasoinen velvoite.[144] Hyvä esimerkki tällaisesta soft law -tyyppisestä käytännesäännöstöstä on valtiovarainministeriön *Suositus tietoturvallisuuden vähimmäisvaatimuksista*[145]. Suosituksessa on kuvattu tietoturvallisuuden vähimmäisvaatimukset, joilla tarkoitetaan yleisiä tai yksityiskohtaisia tietoturvallisuustoimenpiteitä, jotka viranomaisten ja tiedonhallintayksiköiden tulee tiedonhallintalain perusteella toteuttaa tietoturvallisuuden varmistamiseksi[146].

Vastaavanlaisia hyvää tietoturvatapaa ilmentäviä tietoturvan vähimmäisvaatimuksia ei ole esitetty yhtä selkeästi muiden organisaatioiden osalta. Hyvän tavan vaatimuksien tulisi olla kohtuullisia ja oikeudenmukaisia sekä, niin kuin

---

[143] Toisaalta esimerkiksi hallituksen esityksessä 284/2018 (s. 127) on mm. täsmennetty, että tiedonhallintalaissa säädettäisiin hyvään tiedonhallintatapaan kuuluvista seikoista.
[144] Voutilainen 2006b: 6.
[145] Valtiovarainministeriön julkaisuja 2024:19. Suositus on korvannut valtiovarainministeriön toimesta julkaistun suosituskokoelman tiettyjen tietoturvallisuussäännösten soveltamisesta, joka koski lähinnä tiedonhallintalain 4 luvun tietoturvan vähimmäisvaatimusten soveltamista käytännössä. Tässä julkaisussa korostettiin, että kyseistä suositusta ei ole tarkoitettu käytettäväksi arviointikriteeristönä eivätkä suositukset ole velvoittavia lainsäädännön tavoin vaan ne kuvaavat parhaita käytäntöjä (ks. Valtiovarainministeriön julkaisuja 2021:65, s. 9.)
[146] Valtiovarainministeriön julkaisuja 2024:19: 8.

aikaisemmin on mainittu, hyvän tavan tulisi kaikille tarkoittaa samaa. Mikäli lainsäädännön tietoturvavaatimukset koskevat vain rajattua joukkoa organisaatioita, tietoturvan sääntelyjärjestelmä näyttäytyy kovin häilyvänä eikä välttämättä siten niinkään oikeudenmukaisena. Näin ollen lakisääteinen hyvä tietoturvatapa ei tulisi muotoutua yksistään viranomaisia koskevista tietoturvavaatimuksista.

Hyvä tiedonhallintatapa oli kytköksissä myös hyvään (henkilö)tietojenkäsittelytapaan[147]. Yhtä lailla hyvä tietojenkäsittelytapa on yksi hyvän hallinnon elementeistä[148]. Tietosuojan osalta *hyvä tietojenkäsittelytapa* ilmeni suoraan kumotussa henkilötietolaissa (523/1999), jossa säädettiin hyvän tietojenkäsittelytavan kehittämisestä ja noudattamisesta luonnollista henkilöä koskevien henkilötietojen käsittelyn näkökulmasta[149]. Tosin on huomioitava se, että käsitteenä hyvä tietojenkäsittelytapa voisi sisältää muunkin hyvän tavan mukaisen tietojenkäsittelyn kuin henkilötietojen käsittelyn. Esimerkiksi ATK-sanakirjan mukaan se sisältää tietojenkäsittelyä koskevan lainsäädännön ja sen soveltamisohjeiden noudattamista koskevat menettelyt.[150] Jo ennen henkilötietolakia henkilörekisterilain (471/1987) aikaan puhuttiin myös hyvästä rekisteritavasta. Hyvällä rekisteritavalla tarkoitettiin tällöin sellaisten menettelytapojen luomista, jolla edistettiin ja toteutettiin henkilörekisterilain tarkoittamien arvojen suojaa. Esimerkiksi hyvään rekisteritapaan katsottiin kuuluvaksi teknisen kehityksen ja sen tuomien mahdollisuuksien seuraamisen tietosuojan tehostamiseksi. Lisäksi toisena esimerkkinä henkilörekisterilain 3 §:n huolellisuusvelvoitteen mukaisesti rekisteröidyn yksityisyyden suojaa ei saanut perusteettomasti loukata eikä toiminnassa vaarantaa valtion turvallisuutta.[151] Hyvä rekisteritapa ja hyvä tietojenkäsittelytapa olivat käsitteinä (ja sisällöltään) varsin laveita.

> *Hyvä henkilötietojenkäsittelytapa* on käsitteenä osuvampi ja kuvastaa selkeämmin tietosuojan merkitystä nimenomaan henkilötietojen suojaamisessa. Hyvällä henkilötietojenkäsittelytavalla tarkoitetaan lainmukaista henkilötietojen käsittelyä[152]. Nyttemmin hyvä henkilötietojenkäsittelytapa liittyy EU:n yleiseen tietosuoja-asetukseen sekä kansalliseen tietosuojalainsäädäntöön. Tosin tietosuoja-asetuksessa ja esimerkiksi kansallisessa

[147] Henkilötietolain mukaisen henkilörekisterinpitäjän on noudatettava lain vaatimaa hyvää tiedonhallintatapaa, eli huolehdittava arkaluontoisia tietoja sisältävän rekisterin asianmukaisesta teknisestä tietoturvasta, rekisteriin käyttöoikeudet ovat tarkkaan määrätty ja rekisteriin vietävät tiedot ovat virheettömiä. Ks. Lehtonen 2001, s. 348.
[148] Talus 2019: 225.
[149] Ks. henkilötietolain 1 §, jonka mukaisesti kyseisen lain tarkoituksena oli toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.
[150] Voutilainen 2006a: 50; ATK-sanakirja 1 2008: 78.
[151] Wallin & Nurmi 1991: 23, 51–52.
[152] Voutilainen 2006a: 127.

> tietosuojalaissa (1050/2018) ei ole säädetty hyvästä henkilötietojenkäsittelytavasta niin kuin kumotussa henkilötietolaissa, jolloin siihen mahdollisesti liittyvät standardit, ohjeistukset ja suositukset eivät välttämättä ole oikeuslähdehierarkiassa vahvasti velvoittavia eikä se kategorisoidu lakisääteiseksi hyväksi tavaksi.

Hyvän tietoturvatavan kannalta tietosuoja on oleellinen ulottuvuus. Henkilötietojen suojaamiseen liittyy tietosuoja-asetuksen 5 artiklan henkilötietojen käsittelyä koskevia yleisiä periaatteita eli *tietosuojaperiaatteita*, jotka organisaatioiden tulee huomioida toiminnassaan ja lisäksi osoittaa niiden toteutuminen käytännössä (osoitusvelvollisuus[153]). Tällaisia periaatteita ovat muun muassa lainmukaisuusperiaate, kohtuullisuuden ja läpinäkyvyyden periaate, käyttötarkoitussidonnaisuuden periaate, tietojen minimoinnin periaate (tarpeellisuusvaatimus), täsmällisyyden periaate, säilytyksen rajoittamisen periaate sekä luottamuksellisuuden ja turvallisuuden periaate. Nämä tietosuoja-asetuksen tietosuojaperiaatteet kertovat paljonkin hyvän henkilötietojenkäsittelytavan sisällöstä ja sen vaatimuksista. Tietosuojaperiaatteita on noudatettava tietoturvatoimenpiteitä suunniteltaessa ja toteuttaessa. Näin ollen ne myös kiinnittäytyvät hyvään tietoturvatapaan.

> Henkilötietojen käsittely on *lainmukaista*, jos sille löytyy sopiva laissa määritelty käsittelyperuste[154]. Esimerkiksi henkilötietojen käsittely on tietosuoja-asetuksen 6 artiklan mukaan lainmukaista, jos käsittely on tarpeen toteuttaakseen rekisterinpitäjän oikeutettua etua. Tällainen oikeutettu etu voi tietosuoja-asetuksen johdannon 49 kappaleen mukaan liittyä tietoturvaloukkauksiin ja onnettomuuksiin varautumiseen sekä verkko- ja tietojärjestelmien suojautumiskyvyn takaamiseen, kun se on oikeasuhtaista ja rajoittuu ehdottoman välttämättömään käsittelyyn[155]. Tällainen oikeutettu

[153] Osoitusvelvollisuutta käsitelty yksityiskohtaisemmin myös luvussa 3.2.4 (”Osoitusvelvollisuus”).

[154] Henkilötietojen käsittely on 6 artiklan mukaan lainmukaista, jos
a) se perustuu rekisteröidyn spesifioituun käsittelytarkoitukseen kohdennettuun suostumukseen;
b) käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jonka osapuolena rekisteröity on, tai ennen sopimuksen tekemistä olevien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;
d) käsittely on tarpeen rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai yleistä etua koskevan tehtävän suorittamiseksi;
e) käsittely on tarpeen luonnollisen henkilön elintärkeiden etujen suojelemiseksi; taikka
f) käsittely on tarpeen kolmannen osapuolen tai rekisterinpitäjän oikeutettujen etujen toteuttamiseksi pois lukien rekisteröidyn perusoikeudet ja henkilötietojen suojaa vaativat edut, jotka syrjäyttävät nämä.

Käsittelyn lainmukaisuudesta on myös yksityiskohtaisemmin säädetty kansallisen tietosuojalain 4 §:ssä.

[155] Korpisaari & Toikkanen 2020: 472.

etu voi tulla kyseeseen esimerkiksi kameravalvonnassa tai lokitietojen käsittelyssä[156]. Tietosuojadirektiivin osalta tietosuojatyöryhmä on määritellyt, että oikeutetun edun tulee olla lainmukainen, riittävän täsmällinen ja sen on ennustettava todellista ja välitöntä intressiä eli se ei saa olla spekulatiivinen. Oikeutettua etua käytettäessä käsittelyperusteena tulee käsittelyä tarkastella tasapainotestin eli rekisteröidyn etuja koskevan punninnan avulla. Jos rekisteröidyn edut ja oikeudet eivät ole painavampia kuin rekisterinpitäjän intressi henkilötietojen käsittelyyn, henkilötietoja saa käsitellä. Tasapainotesti perustuu kokonaisarvioon. Näin ollen mitä huomattavampi vaikutus käsittelyllä on rekisteröityyn, sitä enemmän rekisterinpitäjä on tarjottava asianmukaisia takeita tietosuojalle. Tällaisia takeita ovat esimerkiksi tekniset ja organisatoriset toimenpiteet, henkilötietojen salaus, anonymisointi[157] ja yksityisyyden suojaa parantavat toimenpiteet, kuten DPIA-arviointi.[158] Lainmukaisen käsittelyperusteen lisäksi tietojen käsittelyn tulee olla *kohtuullista ja läpinäkyvää* käsittelyn tarkoitukseen suhteutettuna, mikä korostaa käsittelyn informoimisvelvoitteita. *Käyttötarkoitussidonnaisuuden periaatteen* mukaisesti henkilötietojen käsittelyn tarkoitus on määriteltävä ja informoitava rekisteröidylle.

Tietojen minimoinnin periaatteen mukaan henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja ainoastaan suhteessa siihen tarpeeseen, johon tarkoitukseen niitä käsitellään. Tietojen minimoinnin periaatteesta käytetään myös tarpeellisuusvaatimuksen nimeä[159]. Periaatteen mukaan tietoja ei saa kerätä ”talteen” varmuuden vuoksi, vaan tietojen pitää olla tarpeellisia suhteessa käyttötarkoitukseen. Esimerkiksi toukokuussa 2018, eli pian tietosuoja-asetuksen voimaantulon jälkeen, Saksa antoi ensimmäisenä EU-valtiona langettavan päätöksen (**10 O 171/18**) liittyen tietojen minimoinnin periaatteeseen. Päätös koski domain-nimiä ostavien henkilöiden henkilötietoja ja niiden liiketoiminnan kannalta tarpeetonta keräämistä, jossa yhdysvaltalaisyritys ei pystynyt perustelemaan tiettyjen tietojen keräämistarkoitusta saksalaiselle tuomioistuimelle.[160] Tietojen minimoinnin periaate ja *tarpeellisuusvaatimus* tulevat ilmi muun muassa teknistä, tietoturvaa parantavaa valvontaa toteuttaessa työpaikalla, jolloin

[156] Järvinen 2022a: 141.
[157] Anonymisointi tarkoittaa henkilötiedon muuttamista sellaiseen muotoon, josta luonnollista henkilöä ei voi enää tunnistaa. Vastakohtaisesti pseudonymisoidut tiedot ovat vielä yhdistettävissä henkilöön ja ovat siten myös henkilötietoja.
[158] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 133–135. 139; Euroopan WP29-tietosuojatyöryhmä WP217: *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, s.* 25.
[159] Nyyssölä 2018: 66.
[160] 10 O 171/18; Keller & Heckman LLP 2018.

myös työelämän tietosuojalaki tulee sovellettavaksi[161]. Lisäksi on huomioitava se, että kunkin rekisterinpitäjän alaisuudessa toimivan henkilön osalta on arvioitava tarve päästä käsittelemään henkilötietoja, jolloin tarpeellisuusvaatimuksen toteuttaminen edellyttää käsittelyoikeuksien määrittelyä tehtäviin ja käsittelytarpeeseen nähden. Tarpeellisuusvaatimuksen toteuttaminen vaatii näin ollen henkilötietojen käsittelyn ja saatavuuden asianmukaista rajoittamista.[162] Tietojen minimointiin ja tarpeellisuuteen liittyy olennaisesti myös säilytyksen rajoittamisen periaate eli henkilötiedoille tulisi määritellä elinkaari ja niitä ei saa säilyttää tarpeettoman pitkään käyttötarkoitukseen nähden.

Henkilötietojen tulee olla myös *täsmällisyysperiaatteen* mukaisesti virheettömiä ja päivitettyjä, mikä korostaa tietoturvan ulottuvuuksista etenkin tiedon eheyttä. Tietosuoja-asetuksen *luottamuksellisuuden ja eheyden (eli turvallisuuden) periaatteet* painottavat, että henkilötietoja on käsiteltävä tavalla, jolla varmistetaan niiden asianmukainen, riskien arviointiin perustuva turvallisuus. Tietoturvallisuuden eli tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaamiseen kuuluu muun muassa tiedon suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta tuhoamiselta, hävittämiseltä tai vahingoittumiselta tiedon koko elinkaaren ajalta. Tästä voidaan johtaa, että tämän vaatimuksen toteutumiseksi tulee toteuttaa hallinnollisia, fyysisiä ja teknisiä tietoturvatoimenpiteitä, jolloin tietoturva tietosuojan toteuttajana korostuu.

Tietosuojalainsäädännön vaatimukset, jotka ilmentävät hyvää henkilötietojen käsittelytapaa, velvoittavat kaikkia organisaatioita. Vaatimukset linkittyvät oleellisesti hyvään tietoturvatapaan, sillä hyvällä tietoturvalla mahdollistetaan henkilötietojen tehokas suojaaminen sekä useiden edellä mainittujen tietosuojaperiaatteiden toteutuminen. Näin ollen hyvä henkilötietojenkäsittelytapa on luonnollinen osa tietoturvan sääntelyjärjestelmää.

Tässä tutkimuksessa hyvää tietoturvatapaa ilmentäviä vähimmäisvaatimuksia on pyritty muodostamaan voimassa olevan oikeuden tulkinnan ja systematisoinnin pohjalta sekä arvioimalla organisaatioiden tietoturvaa ohjaavia käytännesääntöjä ja muita viitekehyksiä. Siinä missä aikaisemmin esiintyneet hyvän hallinnon ja hyvän sähköisen hallinnon sekä hyvän tiedonhallinnan vaatimukset asettavat tietoturvavaatimuksia lähinnä viranomaisille, tämän tutkimuksen hyvän

[161] Työelämän tietosuojalain 3 §:n mukaan työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta *tarpeellisia* henkilötietoja.
[162] Voutilainen 2019: 132.

tietoturvatavan näkökulma ulottuu kaikkiin organisaatioihin. Hyvää tietoturvatapaa käsiteltäessä termi ”hyvä” kuvaa tässä tutkimuksessa hyviä lähtökohtia tietoturvan ja riskienhallinnan toteutukselle. Tällöin hyvä tietoturvatapa asettaa niin sanotusti vähimmäisvaatimukset organisaatioiden tietoturvalle[163]. Hyvä tietoturvatapa tulisi tunnistaa lakisääteisenä hyvänä tapana osana tietoturvan sääntelyjärjestelmää, eli sen noudattamisesta voisi säätää laissa. Lisäksi hyvän tietoturvatavan sisältöä voisi oikeuskäytännön, käytännesääntöjen, tietoturva-alan hyvien käytänteiden ja esimerkiksi viranomaispäätösten ja linjausten ohella täydentää tietoturvan vähimmäisvaatimuksilla, jotka velvoittaisivat kaikkia organisaatioita[164].

Tässä luvussa aikaisemmin mainitut hyvän tavan määritykset tukevat hyvän tietoturvatavan määrittämistä. Näin ollen hyvän tietoturvatavan tulee olla *kohtuullinen* ja *oikeudenmukainen* ollessaan vakiintunut tapa toimia. Lainsäädännön hyvän tietoturvatavan tulee *huomioida organisaatioita ohjaavat hyvät käytänteet*, mutta sen tulisi olla *teknologianeutraali*. On huomioitava, että hyvän tavan oikeusperiaatteelle on ominaista, että se tarkoittaa kaikille samaa[165]. Täten myös *tavoitettavuus* ja *ymmärrettävyys* ovat oleellisia elementtejä hyvän tietoturvatavan osalta.

Lisäksi hyvä tietoturvatapa *huomioi perusoikeudet*. Tällöin perusoikeuksia voisi käyttää arviointiperusteena hyvälle tavalle[166]. Perustuslain 2 luvussa on tällä hetkellä johdettavissa tietoturvan tärkeyttä korostavia oikeuksia vaikkakin suoranaisesti oikeutta tietoturvaan ei ole lakiin kirjattu[167]. Hyvän tietoturvatavan arviointiperusteena voisi käyttää esimerkiksi perustuslain 7 §:n oikeutta turvallisuuteen, 10 §:n oikeutta yksityiselämän suojaan, 12 §:n oikeutta saada tieto julkisesta asiakirjasta ja tallenteesta, 15 §:n oikeutta omaisuuden suojaan sekä 22 §:n julkisen vallan velvollisuutta turvata perus- ja ihmisoikeuksien toteutuminen[168]. Hyvät käytänteet, jotka ovat osa hyvää tietoturvatapaa, eivät luonnollisestikaan voi olla

---

[163] Tiedonhallintalaissa tällaiset vähimmäisvaatimukset esiintyvät tietoturvallisuuden osalta säädöksen luvussa 4. Hyvä tietoturvatapa on siis jo lähtökohtaisesti olemassa, mutta se koskee lähinnä säädöksen alaan luettuja viranomaisia.

[164] Laajan velvoittavuuden osalta tulee huomioida myös riittävä sanktiointi. Esimerkiksi Aarnio on kritisoinut hyvä tapa -ohjeiden sanktioiden puutetta, ks. Aarnio 2010, s. 543: Muotoillessa sanallisesti kaikki ryhmät kattava ohjeistus, muotoilu muodostuu väkisinkin hyvin yleiseksi, jolloin sen merkityssisältö ohenee. Tavoite on hyvä, mutta teho ei välttämättä. Osin tämä johtuu sanktioiden puutteesta.

[165] Kaasalainen 2008: 79, 84; Ämmälä 1993: 19; Saarnilehto 1992: 15–16.

[166] Meri 2023: 67, 74.

[167] Ks. yksityiskohtaisemmin luku 2.5 (”Tietoturva perusoikeutena osana tietoturvan sääntelyjärjestelmää”).

[168] Ks. Saraviita 2011, s. 153–159 (PL 7 §), 178–191 (PL 10 §), 198–209 (PL 12 §), 225–229 (15 §) sekä 292–297 (PL 22 §). Lisäksi: Pellonpää 2011: 281–301 (PL 7 §), Viljanen 2011: 389–411 (PL 10 §), Manninen 2011: 459–491 (PL 12 §), Länsineva 2011: 549–604 (PL 15 §) sekä Lavapuro & Tuori 2011: 809–820 (PL 22 §).

perusoikeuksien vastaisia tai aiheuttaa esimerkiksi sellaista henkilötietojen käsittelyä, joka olisi perusoikeuksien vastaista. Hyvän tavan vastaista olisikin perusoikeuksia loukkaava käyttäytyminen tai toiminta. On myös huomioitava se, että toisen oikeudet lisäävät toisen vastuita. Tämä tarkoittaa sitä, että hyvä tietoturvatapa huomio perusoikeuksien lisäksi *yksilöiden vastuuttamisen sekä yksilöt tietoturvan toteuttajana*.

Hyvän tietoturvatavan muodostama kokonaisuus osana tietoturvan sääntelyjärjestelmää asettaa kriteereitä myös itse sääntelyjärjestelmälle ja sen hyvyydelle. Näin ollen hyvän tietoturvan sääntelyjärjestelmän on oltava hyvän tietoturvatavan sisältämien elementtien mukaisesti kohtuullinen ja oikeudenmukainen, tavoitettava ja ymmärrettävä, hyvät käytänteet, yksilöt ja perusoikeudet huomioiva sekä teknologianeutraali. Hyvän tietoturvan sääntelyjärjestelmän hyvyyttä tarkastellaan näiden elementtien kannalta normikeskeisesti.

2 TIETOTURVAN SÄÄNTELYJÄRJESTELMÄN KEHYS

2.1 Luvun päämäärä

Tutkimuksen päätehtävänä on systematisoida voimassa olevan lainsäädännön perusteella organisaatioiden hyvä tietoturvan sääntelyjärjestelmä sekä esittää hyvän tietoturvatavan muodostama kokonaisuus. Tutkimuksen tavoitteet huomioon ottaen, tämä pääluku on tärkeä kokonaiskuvan muodostamisen kannalta. Tämän toisen pääluvun tarkoituksena on luoda yleiskäsitys tietoturvaan liittyvästä lainsäädännöstä sekä tietoturvalainsäädännön taustoista ja yleisistä periaatteista.

Aluksi käsitellään tietoturvaan liittyvää peruskäsitteistöä, jota esiintyy muun muassa tietoturvan viitekehyksissä, liiketaloudellisessa kirjallisuudessa, oikeuskirjallisuudessa ja lainsäädännössä osana tietoturvan sääntelyjärjestelmää. Tarkoituksena on havainnollistaa, mitä eroavaisuuksia esimerkiksi käytännön peruskäsitteillä on verrattuna lainsäädännön tietoturvakäsitteisiin sekä mitä käytännön haasteita käsite-erot mahdollisesti aiheuttavat.

Tutkimuksen ja tietoturvan sääntelyjärjestelmän keskeisten käsitteiden havainnollistamisen jälkeen tutkimuksessa siirrytään tarkastelemaan yhteiskuntamme kehitystä oikeudellistuneeksi verkkoyhteiskunnaksi, sillä yhteiskuntamme muutokset ovat myös myötävaikuttaneet nykyisen tietoturvan sääntelyjärjestelmän muodostumiseen sekä tietoturvasäännöksien että informaatio-oikeuden periaatteiden kehittymisen tasolla.

Näin ollen yhteiskunnan kehittymisen tarkastelun jälkeen tarkoituksena on syventää lainopillista näkökulmaa käsittelemällä erityisesti tietoturvaan liittyviä informaatio-oikeuden alan meta- ja oikeusperiaatteita, jotka ovat oikeusjärjestyksemme ydinarvoja sekä ihmis- ja perusoikeuksien taustalla olevia oikeuksia oikeuksista. Tämän tutkimuksen kannalta *oikeus tietoturvaan* on keskeinen tarkasteleva metaperiaate.

Meta- ja oikeusperiaatteiden käsittelyn jälkeen on luonnollista siirtyä käsittelemään tutkimuksessa keskeisiä perusoikeuksia, sillä ne muodostavat perustan organisaatioiden hyvälle tietoturvan sääntelyjärjestelmälle. Tarkastelussa ovat erityisesti ne kansalliset perusoikeudet, joista on mahdollista tulkita tietoturvaan liittyviä oikeuksia ja velvoitteita. Tässä luvussa tarkoituksena on tarkastella myös oikeutta kyberturvaan eräänlaisena tietoturvallisuuden alaulottuvuutena, sillä järjestelmistä riippuvaisessa nykyverkkoyhteiskunnassamme kyberturvallisuus on entistä keskeisemmässä roolissa: yksilöillä on oltava oikeus perinteisen turvallisuuden ulottuvuuden lisäksi kyberturvallisuuteen. Huomioitava kuitenkin on, että

kansallisessa perustuslaissamme ei ole säädetty oikeutta tieto- tai kyberturvaan omana perusoikeutenaan eikä siinä ole myöskään suoranaisesti viittauksia tieto- tai kyberturvallisuuteen.

Periaatteiden ja perusoikeuksien käsittelyn jälkeen tutkimuksessa siirrytään systematisoimaan organisaation tietoturvan sääntelyjärjestelmään kuuluvia tietoturvasäädöksiä. EU-lainsäädännöllä on ollut merkittävä vaikutus kotimaisen tietoturvasääntelyn kehittämiseen. Näin ollen luvussa käsitellään ensiksi EU-oikeuden keskeisiä tietoturvasäädöksiä, jonka jälkeen tarkoitus on käsitellä ylätasolla kansallisen lainsäädännön tietoturvasäädöksiä ennen 3 ja 4 luvuissa käsiteltävää yksityiskohtaisempaa säännöstason tarkastelua.

Viimeisempänä toisen pääluvun lopussa kuvataan vielä hyvien, tietoturvallisten käytänteiden taustalla olevia tietoturvaviitekehyksiä, koska tarkoituksena on muiden päälukujen säännöskohtaisessa tarkastelussa arvioida säännöksiä ja hyviä käytänteitä keskenään. Tällainen ylätason käsittely pohjustaa myös lainsäädännön hyvän tietoturvatavan arviointia.

Yhteenvetona todettakoon, että tämän pääluvun keskeisenä tarkoituksena on luoda ikään kuin kehys tietoturvan sääntelyjärjestelmälle koostamalla yhteen tietoturvan sääntelyjärjestelmän keskeisiä käsitteitä, periaatteita, perusoikeuksia sekä säädöksiä ja hyvien käytänteiden viitekehyksiä. Samalla tunnistetaan elementtejä sääntelyjärjestelmän hyvyydelle. Tarkoituksena on myös tarkastella tietoturvan sääntelyjärjestelmän kehittymisen taustalla vaikuttaneita seikkoja, kuten yhteiskunnan kehittymistä oikeudellistuneeksi verkkoyhteiskunnaksi sekä sen myötä tietoturvalainsäädännön muutoksia.

2.2 Tietoturvan sääntelyjärjestelmän systematiikkaa

2.2.1 Tietoturva

Tieto on yksi aikamme tärkeimmistä suojattavista hyödykkeistä. Sille voidaan myös määrittää erilaisia arvoja, esimerkiksi rahallinen, historiallinen ja todistuksellinen, ja se voi olla myös vallankäytön väline[169]. Tietoon kohdistuvat oikeudet ovat yleensä kielto-oikeuksia, jotka antavat oikeudenhaltijalle mahdollisuuden kieltää muita hyödyntämästä tietoa[170]. Myös tiedon turvaamisen tärkeys korostuu niin yksilöiden elämässä kuin organisaatioiden toiminnassa: tiedon tulee olla

[169] Voutilainen 2019: 22.
[170] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 26.

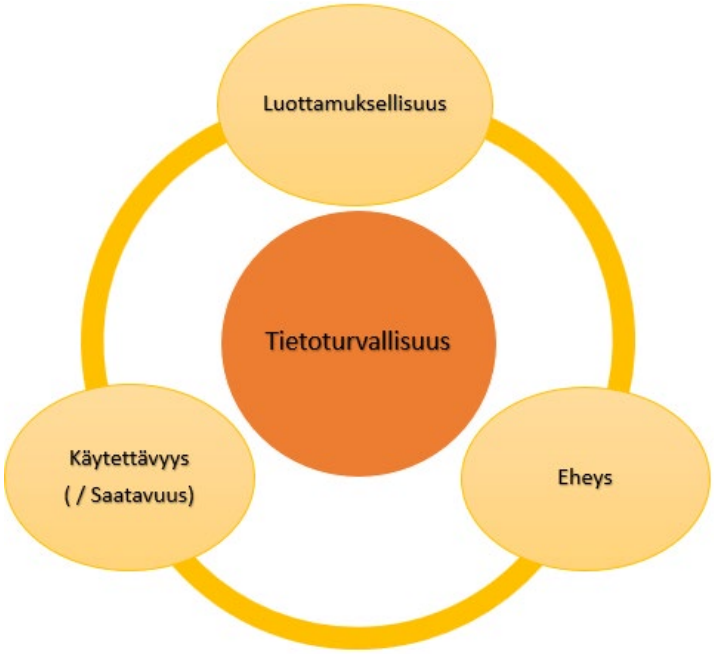
luottamuksellista, eheää ja käytettävissä. Nämä kolme ulottuvuutta ovat ominaisia tietoturvallisuuden määrittelyssä.

Tietoturva on yksi osa organisaation toiminnan laatua ja sillä turvataan organisaation lisäksi yksilöiden ja yhteiskunnan etuja. Tietoturvan toteuttamisen tavoitteena on taata järjestelmien, tietoaineistojen ja palveluiden asianmukainen suojaus niin, että **luottamuksellisuuteen (*confidentiality*), eheyteen (*integrity*) ja käytettävyyteen (*availability*)** liittyvät riskit on otettu huomioon. Tietoturvallisuudesta huolehtiminen on jokaisen velvoite ja tarkoituksena on taata tiedon luottamuksellisuus, eheys ja käytettävyys.[171] Verkottuneessa yhteiskunnassa tietoturvan huolehtimisvelvollisuus koskee kaikkia, sillä niin sanotut heikommat lenkit riskeeraavat myös muiden tietojen turvallisuutta. Näin ollen jo yksilötasolla on tärkeää pitää huolta omista tiedoistaan, jotta ei vaaranna toisten tietoja.

> Esimerkkinä sähköpostin tai sosiaalisen median (some) tietomurrot: Kun hyökkääjä pääsee tunnusvuodon seurauksena kiinni käyttäjän sähköposti- tai sometilille, hyökkääjä usein pyrkii levittämään haittaa eteenpäin. Tällöin ikään kuin lumipalloefektinä haitallista viestiä lähetetään eteenpäin murretuilta tileiltä, jolloin myös muut voivat helpommin erehtyä huijaukseen. Lisäksi muiden henkilöiden tietosuoja ja luottamuksellinen viestintä ovat uhattuina, kun hyökkääjä pääsee urkkimaan tietoja kaapatulla tilillä.

Yhtä lailla organisaatioissa tietoturvan maturiteettitaso on kiinni kaikista työntekijöistä eli ei ainoastaan niistä, jotka ovat suuntautuneet työssään tietoturvaan. Tämä näkökulma tulisi huomioida tietoturvaa koskevassa sääntelyssä, jolloin hyvä tietoturvan sääntelyjärjestelmä huomioi ja vastuuttaa myös yksilöitä.

[171] VAHTI 4/2013: 17–18.



Kuvio 3. Tietoturvallisuuden ulottuvuudet

Tietoturvallisuuden ulottuvuuksista *luottamuksellisuudella* tarkoitetaan sitä, että tieto on vain sille oikeutettujen yksilöiden saatavilla. Tiedon *eheydellä* tarkoitetaan puolestaan tietoa, joka on täydellistä ja johdonmukaista, eikä sitä ole muutettu tai tuhottu. *Käytettävyydellä* (toisinaan käytetään myös termiä *saatavuus*[172]) tarkoitetaan, että tieto ja palvelut ovat oikeutettujen yksilöiden käytettävissä oikeaan aikaan.[173]

Oikeudellisesta näkökulmasta luottamuksellisuus voi asiayhteytensä mukaan viitata myös salassapitosäännöksiin, liikesalaisuuksien sääntelyyn ja vaitiolovelvollisuussopimuksiin[174]. Luottamuksellisuudessa on kysymys informaation sekä sen esittämiseen ja rakenteeseen liittyvien oikeuksien suojaamisesta[175]. Esimerkiksi tietosuojalainsäädännössä henkilötietojen suojaamisessa luottamuksellisuus korostuu siten, että henkilötietoja tulisi käsitellä luottamuksellisesti ja henkilötietojen käsittely tulisi rajata käyttötarkoitussidonnaisuuden mukaisesti. Eheyden oikeudellisena ulottuvuutena puhutaan usein aitoudesta, jota voidaan todentaa esimerkiksi sähköisellä tunnistuksella. Oikeudellisesta näkökulmasta myös käytettävyys (saatavuus) on tärkeä ulottuvuus, sillä monilla tietoturvallisuusnormeilla pyritään tehostamaan ja takaamaan informaation ja tietojärjestelmien oikea-aikaista

[172] Käytännön työssä käytettävyyttä ja saatavuutta käytetään hyvinkin rinnakkain ja ne ovat synonyymit toisilleen.
[173] NIST Special Publication 800-12 1995: 5–7; NIST Special Publication 800-100 2006: 75.
[174] Andersson & Nordén 2018: 64.
[175] Pöysti 1999: 458–461.

hyödynnettävyyttä.[176] Tietojärjestelmien ja tiedon käytettävyys (saatavuus) liittyvät myös myöhemmin käsiteltyihin perusoikeuksiin, joiden myötä viranomaisen positiivisiin velvoitteisiin kuuluu muun muassa hyvän hallinnon mukaisesti varmistaa yksilöille edellytykset oikeuksiensa käyttämiselle. Uudehkona lakiuudistuksena tätä velvoitetta ajaa laki digitaalisten palvelujen tarjoamisesta (306/2019, digipalvelulaki), jolla on pantu täytäntöön Euroopan parlamentin ja neuvoston saavutettavuusdirektiivi (2016/2102/EU). Lain tarkoituksena on edistää muun muassa digitaalisten palveluiden *saatavuutta*, laatua ja *tietoturvallisuutta* sekä sisällön saavutettavuutta[177], ja siten parantaa jokaisen mahdollisuutta käyttää yhdenvertaisesti digitaalisia, julkisen sektorin palveluita. Saavutettavuus tulisi olla tasapainossa tietoturvan kanssa[178].

Kaikki edellä mainitut tietoturvallisuuden ulottuvuudet, luottamuksellisuus – eheys – käytettävyys, ovat tärkeitä. Jos yksi ominaisuus näistä kolmesta uupuu, tietoturvallisuus ei ole täydellistä eikä esimerkiksi toiminta tai palvelu ole tietoturvallinen.

Tietoturvallisuuden kolmen perusulottuvuuden lisäksi tietoturvan käsitteen alaa voidaan laajentaa ottamalla mukaan kiistämättömyys (non-repudiation) ja pääsynvalvonta (access control), jotka ottavat huomioon myös tiedon tuottajan identiteetin sekä laitteistojen ja järjestelmien arvon. Tässä kontekstissa kiistämättömyys tarkoittaa järjestelmän kykyä tunnistaa ja tallentaa järjestelmää käyttävän tiedot samalla varmistaen tiedon alkuperä, mikä mahdollistaa tiedon luvattoman käytön tunnistamisen. Pääsynvalvonnalla tarkoitetaan menetelmiä, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä. Tällainen tietojen pääsyn rajoittaminen on osa luottamuksellisuuden ylläpitoa. Tietoturvan ulottuvuudeksi voidaan liittää myös todentaminen (autenttisuus, authentication), jolla tarkoitetaan järjestelmien käyttäjien sekä laitteiden tunnistusta. Tämä ulottuvuus on perusedellytys luottamuksellisuudelle ja kiistämättömyydelle, vaikka se jätetään usein tietoturvan käsitteen alan ulkopuolelle.[179]

---

[176] Pöysti 1999: 458–461.
[177] Saavutettavuudella tarkoitetaan digitaalisten palvelujen tarjoamisesta annetun lain 2 §:n mukaisesti periaatteita ja tekniikoita, joita on noudatettava digitaalisten palvelujen suunnittelussa, kehittämisessä, ylläpidossa ja päivittämisessä, jotta ne olisivat paremmin käyttäjien, erityisesti vammaisten henkilöiden, saavutettavissa. Esimerkiksi digipalvelulain 4 §:n mukaisesti viranomaisen on varmistettava digitaalisten palvelujensa yhteensopivuus yleisesti käytettyjen ohjelmistojen ja tietoliikenneyhteyksien kanssa. Myös saatavuudesta on huolehdittava muulloinkin kuin varanomaisen asiointipisteiden aukioloaikoina, eli esimerkiksi käyttökatkot on suunniteltava vähäisen käytön ajankohtaan.
[178] Saavutettavuusongelmia ei tulisi eriyttää tietoturvaongelmista. Ks. Pöysti 2023, s. 50–51. Lakisääteiset saavutettavuuskriteerit ovat minimikriteereitä, jolloin niitä ei voi jättää toteuttamatta vetoamalla priorisointiin tai siihen, että ne eivät ole tärkeitä palvelun käyttäjälle. Ks. Valtiovarainministeriö 2022, s. 21.
[179] Alavesa 2016: 218–219; Hakala, Vainio & Vuorinen 2006: 5–6.

Tietoturvallisuutta on määritelty myös muilla tavoin kuin sen ulottuvuuksien kautta. Käytännössä tietoturvallisuudella tarkoitetaan tietojen ja palvelujen, tietoliikenteen ja järjestelmien suojaamista sekä niihin kohdistuvien riskien hallitsemista normaali- ja poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä[180]. Tietoturvalla ja tietoturvallisuudella voidaan myös tarkoittaa oloja, joissa tietoturvariskit ovat hallinnassa[181]. Tietoturvallisuuden tavoitteena on mahdollistaa liiketoiminnan jatkuvuus, luoda organisaatiolle kilpailuetua ja varmistaa toiminnan lainmukaisuus[182]. Sen päämääränä on myös estää tietojen ja tietojärjestelmien valtuudeton käyttö sekä tahallinen tai tahaton tiedon tuhoutuminen tai vääristyminen, turvata toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta sekä minimoida aiheutuvat vahingot[183].

Tietoturva jaetaan usein vielä pienempiin hallittaviin osa-alueisiin. Yksinkertaisin jaottelumuoto on jakaa tietoturva hallinnolliseen tietoturvaan, fyysiseen tietoturvaan ja tekniseen tietoturvaan. Tätä jaottelumuotoa käytetään myös tässä tutkimuksessa, koska jaottelu kuvaa olennaisella ja yksinkertaisella tavalla tietoturvan eri elementtejä.

Näistä hallinnollinen tietoturva kattaa tietoturvan kehittämisen ja johtamisen eli muun muassa tietoturvavastuiden määrittelyn ja organisoinnin, dokumentoinnin, riskienhallinnan, varautumisen ja turvallisuuspoikkeamien hallinnan, tietoturvan huomioimisen henkilöstön työsuhteen koko elinkaaren osalta ja tietoturvakouluttamisen[184] sekä tietojen elinkaaren, luokittelun ja salassapidon huomioimisen[185]. Fyysinen tietoturva kattaa rakennuksen tilojen ja niihin sijoitettujen laitteiden suojaamisen fyysisiltä uhkilta. Tekninen tietoturva sisältää tekniset kontrollit tietoliikenne-, ohjelmisto-, laitteisto- ja käyttöturvallisuuden osalta. Teknisen tietoturvallisuuden osa-alue voidaan jakaa tietoliikenneturvallisuuteen, tietojärjestelmäturvallisuuteen (sisältäen ohjelmistoturvallisuuden ja laitteistoturvallisuuden osa-alueet) ja käyttöturvallisuuteen.

Tietoturvan käsite on määritelty myös lainsäädännössä. Ensimmäistä kertaa se määriteltiin yksityisyyden suojasta televiestinnästä ja teletoiminnan tietoturvasta annetun lain (22.4.1999/565) 3 §:n käsitteissä. Tosin tässä tietoturva oli sidottu teletyrityksen teletoimintaan. Sanotun säännöksen mukaan teletoiminnan tietoturvalla tarkoitettiin televiestinnässä välitetyn tiedon luottamuksellisuutta,

[180] Andreasson & Koivisto 2013: 29; VAHTI 3/2007:13.
[181] Turvallisuuskomitea 2018: 15.
[182] Olson & Wu 2017: 145.
[183] Andreasson, Koivisto & Ylipartanen 2013: 14.
[184] Työsuhteen tietoturva- ja koulutusasiat usein kategorisoidaan myös henkilöstöturvallisuuden alle.
[185] Tietoaineiston käsittelyyn liittyvät asiat, kuten tietojen luokittelu ja salassapito, usein kategorisoidaan tietoaineistoturvallisuuden alle.

eheyttä ja käytettävyyttä, joka on varmistettu teleyrityksessä hallinnollisin ja teknisin toimenpitein.[186] Tämä laki myöhemmin kumottiin sähköisen viestinnän tietosuojalailla (16.6.2004/516). Tämä puolestaan kumottiin tietoyhteiskuntakaarella, joka tunnetaan nykyään nimellä laki sähköisen viestinnän palveluista (7.11.2014/917).

Laissa sähköisen viestinnän palveluista tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että a) tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, b) tietoja ei voi muuttaa muut kuin siihen oikeutetut; sekä c) tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Täten sähköisen viestinnän palveluista annettu laki viittaa myös edeltäjänsä tavoin tällä määritelmällä nimenomaan tietoturvallisuuden kolmeen ulottuvuuteen: luottamuksellisuuteen, eheyteen ja käytettävyyteen. Määritelmää on kritisoitu siitä, että se ei käsittele oikeudellista tietoturvallisuutta ja maininta hallinnollisista toimista viittaa ennemminkin tietoturvan avustavasta merkityksestä kertovaan ajattelutapaan[187]. Kritiikki on sinänsä aiheetonta, sillä määritelmässä kuvataan juuri tyypillistä tietoturvan osa-alueiden jaottelua: hallinnollisia tietoturvatoimenpiteitä sekä teknisiä tietoturvatoimenpiteitä. Määritelmä ei kuitenkaan ota huomioon osa-alueista fyysistä tietoturvallisuutta, eli se ei kattavasti määrittele tietoturvan osaksi fyysisiä tietoturvatoimia. Huomioitava kuitenkin on, että kyseisessä määritelmässä erotetaan toisistaan käsitteinä hallinnolliset ja tekniset toimenpiteet, mikä voidaan myös tulkita niin, ettei tietoturva ole ainoastaan teknisen IT-henkilöstön vastuulla. Tämän lisäksi määritelmän hallinnolliset ja tekniset toimenpiteet ovat rinnastettavissa alkuperäisessä NIS 1 -direktiivissä ja tietosuoja-asetuksessa käsiteltyihin teknisiin ja organisatorisiin toimenpiteisiin[188].

Vuoden 2020 alussa kumotussa tietoturvallisuusasetuksessa (681/2010) tietoturvallisuudella tarkoitetaan tietojen salassapitovelvollisuuden ja käyttörajoituksien noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä. Perinteinen luottamuksellisuuden ulottuvuus on tässä määritelmässä jätetty kokonaan pois, ellei sitä katsota sisältyvän määritelmän jälkiosioon, missä mainitaan salassapitovelvollisuudesta. Lisäksi määritelmässä käytetään samassa lauseessa saatavuutta ja käytettävyyttä, mikä yleensä mielletään saman kategorian sisälle tietoturvallisuuden kolmessa ulottuvuudessa (availability). On myös huomioitava se, että tämä määrittely on suppeampi verrattuna sähköisen viestinnän palveluista annetun lain määritelmään, sillä se rajaa näkökulman valtionhallintoon[189].

---

[186] Lehtonen 2016: 270.
[187] Saarenpää 2015: 348.
[188] Teknisiä ja organisatorisia toimenpiteitä käsitellään yksityiskohtaisemmin luvussa 3.4 (”Tietoturvan sääntelyjärjestelmän erilaiset tietoturvatoimenpiteet”).
[189] Lehtonen 2016: 270.

Tietoturvallisuusasetuksen kumonneessa viranomaisen tiedonhallintalaissa (906/2019) tietoturvallisuus määritellään tietoturvallisuustoimenpiteiden kautta. Tietoturvallisuustoimenpiteillä tarkoitetaan tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Tässä määritelmässä on mukana luottamuksellisuuden ulottuvuus. Määritelmään on myös otettu mukaan käsite ”toiminnalliset toimenpiteet”, jota ei ollut tietoturvallisuusasetuksessa. Lisäksi tietoturvallisuustoimenpiteillä tarkoitetaan tässä nimenomaan toiminnan turvallisuuden, fyysisen turvallisuuden, tietoaineistoturvallisuuden, tietoliikenneturvallisuuden[190] sekä laitteistoja ohjelmistoturvallisuuden varmistavia toimenpiteitä.[191] Uuden tiedonhallintalain määritelmä koskee tietoturvaan liittyviä toimenpiteitä ja se määrittelee tietoturvallisuuden kolme ulottuvuutta. Lisäksi se ottaa huomioon hallinnolliset, toiminnalliset ja tekniset toimenpiteet, mikä on laajempi määritelmä kuin EU:n yleisessä tietosuoja-asetuksessa ja NIS 1 -direktiivissä ilmi tuleva tekniset ja organisatoriset toimenpiteet. Tiedonhallintalaki on tosin suunnattu viranomaisille ja viranomaisen tietoaineistojen suojaamiselle, jolloin sama aikaisemmin esiin nostettu tietoturvallisuusasetuksen ongelma toistuu: näkökulma rajautuu valtionhallintoon.

Tietoturvan sääntelyjärjestelmässä tietoturvaa käsittelevä terminologia ei poikkea suuresti muiden lähteiden määritelmistä, mutta se on hajanaista ja osittain epäyhtenäistä. Käsitteenä tietoturva vaikuttaa olevan hyvin monelta kantilta määritelty, mikä vaikuttaa negatiivisesti käsitteen johdonmukaisuuteen ja ymmärrettävyyteen. Suositeltavaa olisi ottaa kattavammin huomioon hyvien käytänteiden mukaisesti myös fyysisen tietoturvallisuuden ulottuvuus, esimerkiksi huomioon ottaen *tietoturvatoimenpiteet, joilla tarkoitetaan tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamista hallinnollisin, fyysisin ja teknisin toimenpitein*. Kuitenkaan lainsäädännössä tietoturvatoimenpiteiden määritelmä ei ole ilmennyt näin yksinkertaisena, ja ottaen huomioon lainsäädännön nykyinen kehityskulku, käsitteistöä tuskin yksinkertaistetaan näin suoraviivaisesti[192]. Tämä huomioon ottaen voimassa olevassa kansallisessa lainsäädännössä kattavin tietoturvallisuuden määritelmä on tiedonhallintalaissa.

Yhteenvetona voidaan todeta, että tietoturvallisuuden avulla suojataan tiedon kolmea perusulottuvuutta: luottamuksellisuutta, eheyttä ja käytettävyyttä

---

[190] Hakala, Vainio & Vuorinen 2006: 12. Tietoliikenneturvallisuudessa huolehditaan tiedonsiirtoratkaisujen, kuten verkkoyhteyksien sekä muiden viestintäjärjestelmien turvallisuudesta.
[191] HE 284/2018 vp: 65–66.
[192] Ks. lisää tietoturvatoimenpiteiden määrittelyn kehittymisestä luvussa 3.4 (”Tietoturvan sääntelyjärjestelmän erilaiset tietoturvatoimenpiteet”) sekä pohdintaa tarkemmin luvussa 3.4.4 (” Tietoturvatoimenpiteiden käsitteistön yhdenmukaisuus”)

(saatavuutta). Nämä ulottuvuudet ovat oleellisia tietoturvallisuuden määrittelyssä, mutta kuitenkin ne ovat huomioitu hyvin vaihtelevalla tasolla nykyisessä sääntelyjärjestelmässä. Tietoturvallisuus on määritelty moninaisesti niin kirjallisuudessa kuin lainsäädännössä. Usein tietoturva jaetaan vielä osa-alueisiin, jotka kuvaavat eri tietoturvatoimenpiteiden elementtejä. Tällaisia ovat hallinnollisen, fyysisen ja teknisen tietoturvan osa-alueet. Näiden osa-alueiden osalta etenkin fyysisen tietoturvan huomiointi on jäänyt vähemmälle tietoturvan sääntelyjärjestelmässä ilmenevässä käsitteistön määrittelyssä. Edellä mainittuja tietoturvan ulottuvuuksia ja osa-alueita on myös käytetty tässä tutkimuksessa tietoturvan sääntelyjärjestelmän hyvän tietoturvatavan arvioinnissa. Hyvässä tietoturvan sääntelyjärjestelmässä käsitteistön tulisi olla yhtenäistä, johdonmukaista, helposti ymmärrettävää ja hyvät käytänteet huomioivaa. Epäyhtenäinen tietoturvan käsite, joka on määritelty tietoturvatoimenpiteiden osalta eri tavalla säädöksistä riippuen, johtunee siitä, että meillä ei ole ollut tietoturvan yleislakia. Tulevaisuuden säädöskehityksessä tietoturvan voisi hyvien käytänteiden pohjalta määritellä tarkoittavan *tiedon luottamuksellisuuden, eheyden ja käytettävyyden suojaamista hallinnollisilla, fyysisillä ja teknisillä tietoturvatoimenpiteillä.*

2.2.2 Tietosuoja

Tietosuojalla tarkoitetaan yksityisyyden suojaamista henkilötietoja käsiteltäessä[193]. Käsitteenä tietosuoja on varsin harhaanjohtava, sillä tietosuojassa ei ensisijaisesti pyritä tietojen salaamiseen vaan suojaamaan yksilön oikeuksia[194]. Tietosuojaa pyritään toteuttamaan muun muassa tietoturvalla[195], ja siksi se on olennainen osa myös tietoturvan sääntelyjärjestelmää. Tietosuojaan on perinteisesti katsottu kuuluvan henkilötietojen käsittelyä koskevien vaatimusten huomioiminen yksityisten henkilöiden yksityisyyden, oikeusturvan ja muiden etujen ja oikeuksien varmistamiseksi muun muassa ohjaamalla rekisterinpitäjiä hyviin henkilötietojen käsittelykäytäntöihin[196].

On huomioitava, että käsitteinä henkilötietojen suoja ja tietosuoja eroavat toisistaan, vaikka niitä on käytetty toisinaan toistensa synonyymeina. Henkilötietojen suoja on osa yksilön yksityisyyden suojaa, sitä toteutetaan tietosuojalainsäädännön avulla, ja se on osa yksilöiden perusoikeuksia[197]. Käsitteenä henkilötietojen suoja on täten oikeudellinen peruskäsite ja tietosuoja puolestaan kansainvälisesti vakiintunut käsite henkilötietojen suojan oikeudellisesta sääntelystä. Tietosuoja

[193] VAHTI 1/2016: 12.
[194] Pöysti 1999: 433.
[195] Turvallisuuskomitea 2018: 16.
[196] Andreasson, Koivisto & Ylipartanen 2013: 14.
[197] Ks. myös luku 2.5.3 (”Yksityisyys: yksityiselämän, henkilötietojen ja viestin suoja”).

on terminä itsessään ristiriitainen, sillä se kuvastaa kaikenlaisten tietojen suojaamista. Alun perin tavoitteena on kuitenkin ollut suojata luonnollisia henkilöitä eikä vain tietoja.[198] Tietosuojan vaatimukset voivat kuitenkin ulottua myös organisaatioiden muihin tietoihin, esimerkiksi liikesalaisuuksiin[199]. Käsitteenä tietosuoja on määritelty laajasti esimerkiksi EU:n yleisessä tietosuoja-asetuksessa, jonka johdanto-osan mukaan asetuksessa kunnioitetaan kaikkia perusoikeuksia ja otetaan huomioon perusoikeuskirjassa tunnustetut vapaudet ja periaatteet. Täten tietosuojan voidaan nähdä koostuvan vaatimuksista, joilla turvataan yksilön perusoikeuksien toteutuminen henkilötietojen käsittelyssä.[200]

Lainsäädännössä henkilötietojen suoja sijoittuu ensisijaisesti siviilioikeuteen kuuluvaan persoonallisuusoikeuteen, koska kysymys on lähtökohtaisesti identiteetistä ja sen suojaamisesta. Kuitenkin henkilötietojen suojaa edesauttava tietosuojalainsäädäntö on vakiintunut oikeusinformatiikan lainopillisiin tutkimusaiheisiin.[201]

Henkilötietoja suojataan pääsääntöisesti tietoturvatoimenpiteillä, jolloin puutteellinen tietoturva johtaa puutteelliseen tietosuojan tasoon sekä rekisteröityjen oikeuksien heikkenemiseen. Tällaisia oikeuksia voivat olla perusoikeudet, mutta myös esimerkiksi tietosuojaoikeudet[202]. Huomioitava on, että tietoturvatoimenpiteillä turvataan myös muita yksilöiden perusoikeuksia kuin oikeutta henkilötietojen suojaan.

Vaikka tietoturvatoimenpiteiden toteutuminen ja organisaation hyvä tietoturvataso ovat oleellisia yksilöiden tietosuojan ja muidenkin perusoikeuksien turvaamiseksi, tietoturvaa ei ole käsitelty lainsäädännössä samalla tavoin tärkeänä, luonnollisten henkilöiden perusoikeuksien toteuttajana kuin tietosuojaa on käsitelty lainsäädännössä[203]. Tämän epäsuhdan korjaamiseksi olisikin tärkeää tietoturvan sääntelyjärjestelmässä korostaa ja huomioida paremmin tietoturva yksilöiden perusoikeuksien toteuttajana vähintään samanarvoisesti kuin tietosuoja on huomioitu yksilöiden perusoikeuksien toteutumisen turvaajana henkilötietojen

[198] Saarenpää 2015: 324–325.
[199] Neuvonen 2014: 64.
[200] Voutilainen 2019: 68.
[201] Saarenpää 2016a: 75.
[202] Esimerkiksi oikeus saada pääsy tietoihin, oikeus saada informaatiota henkilötietojen käsittelystä sekä oikeus rajoittaa tietojen käsittelyä. Lisätietoja rekisteröityjen oikeuksista löytyy tietosuojavaltuutetun sivuilta, mutta myös organisaatioiden informointivelvoitteen täyttämiseksi tehdyissä tietosuojaselosteissa tai vastaavassa informaatiossa rekisteröityjen tietosuojaoikeudet tulisi olla kuvattuna.
[203] Esimerkiksi henkilötietojen suojasta on säädetty osana yksilöiden perusoikeuksia, jota turvataan muun muassa EU:n yleisen tietosuoja-asetuksen ja sitä täydentävän kansallisen tietosuojalainsäädännön avulla.

käsittelyä koskevassa sääntelyssä. Tämä olisi mahdollista esimerkiksi täydentämällä perustuslakia tietoturvasäännöksellä[204].

Yhteenvetona voidaan todeta, että tietosuojan fokus keskittyy yksityisyyden sekä muiden rekisteröityjen oikeuksien ja etujen suojaamiseen henkilötietoja käsiteltäessä. Käsitteinä henkilötietojen suojaa ja tietosuojaa käytetään usein synonyymeina. On myös huomioitava se, että käsitteenä tietosuoja on aavistuksen harhaanjohtava, sillä se ilmentää kaikkien tietojen suojaamista, vaikka tietosuojalainsäädännössä keskeistä on henkilötietojen sekä rekisteröityjen oikeuksien ja vapauksien suojaaminen. Lähtökohtaisesti tietoturvan fokuksena on muidenkin tietojen suojaaminen kuin henkilötietojen. Käsitteinä tietosuoja ja tietoturva on lähtökohtaisesti pidettävä erillään, mutta tietosuoja on huomioitava systemaattisena osana organisaatioiden tietoturvan sääntelyjärjestelmää: tietosuojalainsäädännöstä tulevat keskeiset tietoturvavaatimukset organisaatioille. Tietosuoja ja tietoturva ovat näin ollen linkittyneet toisiinsa. Tietoturvatoimenpiteillä suojataan sekä henkilötietoja että muita organisaation luottamuksellisia tietoja. Yhtä lailla tietoturvatoimenpiteillä suojataan yksilöiden perusoikeuksia, kuten oikeutta henkilötietojen suojaan. Näin ollen tietosuojan ja hyvän henkilötietojen käsittelytavan toteutuminen ovat pitkälti riippuvaisia tietoturvatoimenpiteistä. Siitä huolimatta lainsäädännössä ja erityisesti perusoikeuksien osalta tietosuoja on saanut enemmän painoarvoa kuin tietoturva, sillä oikeus henkilötietojen suojaan on lakiin kirjattu perusoikeus. Sinänsä tämä on ristiriitaista ottaen huomioon se, että tietoturvan toteutuminen on oleellista kaikenlaisten tietojen turvaamisen ja digitalisoituneen verkkoyhteiskunnan toimivuuden osalta – mikäli tietoturva on puutteellista, monet yksilöiden oikeudet ja vapaudet eivät toteudu.

2.2.3 Uhka ja riski sekä niiden keskeiset eroavaisuudet

Seuraavaksi tässä alaluvussa käsitellään uhkaa ja riskiä käsitteinä, koska ne omaavat merkittävän liitynnän tietoturvaan: yksinkertaistettuna tietoturvan päämääränä on turvata luottamuksellisia tietoja, jolloin tietoturvatoimenpiteitä tarvitaan tietojenkäsittely-ympäristössä havaittujen uhkien proaktiiviseen torjuntaan ja tietoturvariskien hallintaan.

Käytännön tasolla riskien arvioinnin prosessi alkaa uhkien tunnistamisella sekä niiden seurausten ja todennäköisyyksien arvioinnilla. *Uhkalla* tarkoitetaan epätoivottua vaikutusta organisaatioon, jossa ei ole positiivista mahdollisuutta[205]. Näin

[204] Saarenpää 2016a: 123, 218; Saarenpää & Riekkinen 2023: 177, 204. Enemmän pohdintaa myös luvussa 2.5 (”Tietoturva perusoikeutena osana tietoturvan sääntelyjärjestelmää”).
[205] Valtiovarainministeriön julkaisuja 22/2017b: 5.

ollen esimerkiksi tietoturvauhka on määritelty mahdollisesti toteutuvaksi haitalliseksi tapahtumaksi tai kehityskuluksi, joka kohdistuu tietoturvaan ja toteutuessaan vaarantaa sen[206]. Lainsäädännössä ei ole määritelty uhkaa käsitteenä sellaisenaan, mutta esimerkiksi käsite kyberuhka on määritelty[207]. Lain esitöissä on määritelty hyvinkin konkreettisella tasolla tietoturvauhka: tietoturvauhkalla tarkoitetaan 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[208]. Näkökulma on tässäkin varsin kyberpainotteinen. On myös huomioitava se, että kyseisen hallituksen esityksen esimerkeistä erityisesti viimeinen on varsin erikoinen ja epätodennäköinen. Harvemmin tietomurtoja tehdään suoramarkkinointiviestien lähettämiseksi, vaan ennemminkin tavoitteena on luottamuksellisten tietojen löytäminen ja hyödyntäminen sekä haitallisten kalasteluviestien edelleen lähetys kaapatuilta tileiltä.

Riskiä saatetaan käyttää usein uhka-käsitteen synonyymina. Huomioitava on kuitenkin se, että uhka on aina negatiivinen.[209] Siinä missä uhkalla tarkoitetaan mahdollista negatiivista tapahtumaa, riskillä tarkoitetaan tapahtuman arvioituja seuraamuksia, mutta myös todennäköisyyttä, jolla uhka toteutuu[210]. VAHTI 7/2003-ohjeessa on määritelty, että riskillä tarkoitetaan tietyn uhkan aiheuttamaa menetyksen tai vahingon todennäköisyyttä. Myöhemmin vuonna 2017 julkaistussa VAHTI 7/2003 -ohjeen korvaavassa valtiovarainministeriön riskienhallintaohjeessa riski on määritelty tarkoittavan epävarmuuden vaikutusta tavoitteisiin eli niin sanotusti poikkeamaa odotetusta. Tässä riskienhallintaohjeessa riski nähdään aikaisempiin määrittelyihin verrattuna osittain positiivissävytteisenä, sillä riskin vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.[211] Riskien positiivinen näkökulma tulee myös voimakkaasti esiin ISO 31000:2018 -riskienhallintastandardissa. Riski ilmaistaan riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyksien yhdistelmänä, mikä vaikuttaa yhtä lailla riskin myönteisyyteen tai kielteisyyteen[212]. Positiivisesta riskistä on kyse, kun onnistumisen kautta siitä voi saada hyötyä tai etua, kun riskistä aiheutuvat epävarmuustekijät pystytään välttämään tai minimoimaan.[213]

---

[206] Turvallisuuskomitea 2018: 25.
[207] Ks. lisää käsitteestä jäljempänä olevasta luvusta 2.2.4 (”Keskeinen kyberterminologia”).
[208] HE 48/2008 vp: 29.
[209] Valtiovarainministeriön julkaisuja 22/2017a: 11–12.
[210] Pöysti 1997: 21.
[211] Andersson 2018: 3; VAHTI 7/2003: 77; Valtiovarainministeriön julkaisuja 22/2017a: 11.
[212] Turvallisuuskomitea 2018: 12.
[213] Valtiovarainministeriön julkaisuja 22/2017a: 11–12.

Käsitteinä uhka ja riski on pidettävä erillään, koska ne kuvaavat eri asioita: uhka on mahdollinen negatiivinen tapahtuma ja riski kuvaa uhkan toteutumisen seurauksia (ja todennäköisyyksiä), jotka tyypillisesti ovat negatiivisia. Toki seuraukset voivat olla myös positiivisia, mikäli riskin toteutumisesta voisi aiheutua negatiivisten seurausten lisäksi jotain hyvää, esimerkiksi organisaation toimiessa poikkeuksellisen hyvin tai avoimesti uhkan toteutumisen hetkellä ja sen takia organisaatio saisikin myönteistä julkisuuskuvaa sosiaalisessa mediassa ja siten lisää asiakkaita. Lähtökohtaisesti kuitenkin riskien arvioinnin tavoite on aina tunnistaa uhkia ja näin ollen arvioida niistä aiheutuneita riskejä sekä toteuttaa riskienhallintakeinoja, joilla näiden riskien toteutumisen todennäköisyyksiä voitaisiin pienentää. Näin ollen positiivinen riski on käsitteenä erittäin huono, koska riskin toteutuminen ei tulisi olla tavoiteltava tila. Positiiviset seuraukset sen sijaan voivat lieventää negatiivisen riskin seuraamuksia, mutta nekin ovat tyypillisesti niin sanotusti positiivisia yllätyksiä eikä tällaisten positiivisten yllätysten pitäisi alentaa varsinaisessa riskiarvioinnissa riskin vakavuuden arviota. Etenkin tietoturva- ja tietosuojariskien osalta positiivisia seurauksia ei lähtökohtaisesti ole eikä niihin liittyviä hypoteettisia positiivisia yllätyksiä tule käyttää riskiluvun pienentämiseksi, koska tietojen menettäminen tai niiden päätyminen ulkopuoliselle ei lähtökohtaisesti ole hyvä asia[214]. Tutkimuksen kirjoittamisen aikana ei ole noussut konkreettisia havaintoja, joiden myötä esimerkiksi tietoturvariski voitaisiin nähdä positiivisena.

Tietoturvariskillä tarkoitetaan tässä tutkimuksessa sellaisia ei-toivottuja tilanteita, joissa tiedon luottamuksellisuus, eheys tai käytettävyys ovat uhattuina[215]. Tietoturvariski voi toteutua sekä tahallisesta, oikeudettomasta teosta että tahattomasta vahingosta. Yleensä vahingot ovat taloudellisia eli esimerkiksi sellaisia, jotka johtuvat omaisuuden vahingoittumisesta, liiketoiminnan keskeyttämisestä, aineettomien oikeuksien loukkaamisesta tai vahinkoon liittyvistä suojautumis- ja tutkintakuluista. Tahattomaan vahinkoon liittyvät tietoturvariskit johtuvat useimmiten sopimussuhdevirheistä, tekniikan suunnittelu- tai toimintavirheistä, liiketoiminnan aineettoman pääoman mainehaitoista taikka liiketoiminnasta sellaisessa maassa, jossa olosuhteet aiheuttavat riskin liiketoiminnalle.[216] Lainsäädännössä ei ole kuitenkaan suoranaisesti määritelty tietoturvariskiä.

Alkuperäisessä NIS 1 -direktiivissä riskin määriteltiin tarkoittavan mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattoi samanaikaisesti vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen. NIS 1 -direktiivin määritelmä rajautui ainoastaan verkko- ja tietojärjestelmiin kohdistuviin turvallisuusriskeihin eli sen näkökulmana olivat lähinnä kyberriskit.

[214] Tätä näkökulmaa käsitelty myös luvussa 2.2.2 (”Tietosuoja”).
[215] Andersson 2018: 2.
[216] Andersson 2018: 2–3; Suomen tietoturvallisuusstrategia 2016: 19.

Esimerkiksi tietoturvan osalta se ei ottanut huomioon paperisiin asiakirjoihin liittyviä riskejä. Päivitetyssä kyberturvallisuusdirektiivissä eli NIS 2 -direktiivissä on sen sijaan käsitelty riskiä laajemmin. NIS 2 -direktiivin 6 artiklan mukaan riskillä tarkoitetaan poikkeaman aiheuttaman menetyksen tai häiriön mahdollisuutta, joka ilmaistaan tällaisen menetyksen tai häiriön suuruuden ja kyseisen poikkeaman toteutumisen todennäköisyyden yhdistelmänä. Tämä määritelmä vastaa täsmälleen samaa riskin määritelmää kuin direktiivissä kriittisten toimijoiden häiriönsietokyvystä (2022/2557/EU) eli CER-direktiivissä, joka tuli voimaan joulukuussa 2022 NIS 2 -direktiivin tavoin[217]. Tuoreimmissa direktiiveissä riskin arviointi ei enää rajaudu ainoastaan verkko- ja tietojärjestelmiin, vaan se ulottuu myös esimerkiksi järjestelmien fyysiseen ympäristöön eli fyysisen tietoturvallisuuden osa-alueeseen. Kaikissa säädöksissä riski nähdään myös negatiivisena.

Aivan kuten aikaisemmin ilmaistussa tietoturvariskin määrittelyssä, tässä kohtaa voidaan todeta, että *tietosuojariskillä* tarkoitetaan sellaisia riskejä, joissa henkilötiedon luottamuksellisuus, eheys tai käytettävyys ovat uhattuina[218]. Riski voi täten kohdistua sekä elektronisessa muodossa olevaan henkilötietoon että fyysiseen dokumenttiin, joka sisältää henkilötietoja.

Tietosuoja-asetuksessa tietosuojariskiksi on määritelty henkilötietojen käsittelyyn liittyvät riskit, kuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai laiton hävittäminen, tuhoaminen, muuttaminen taikka luvaton luovuttaminen tai henkilötietoihin käsiksi pääseminen, mikä voi aiheuttaa aineellisia, aineettomia tai fyysisiä vahinkoja. Tietosuojariski nähdään myös negatiivisena sekä käytännössä että tietosuoja-asetuksessa. Esimerkiksi henkilötietojen käsittelystä aiheutuvia uhkia arvioidaan siltä pohjalta, aiheuttaako tietojen käsittely riskin henkilöiden oikeuksille ja vapauksille. Mikäli tällainen riski toteutuisi luonnollisen henkilön kannalta, seuraukset eivät olisi positiivisia sekä henkilön että organisaation kannalta. Organisaatioiden ei tule myöskään arvioida mahdollisia positiivisia seurauksia luonnollisiin henkilöihin kohdistuvien riskien toteutumisen kautta, sillä se ei olisi hyvän tavan mukaista – lähtökohtaisesti lain mukaan rekisteröityjen oikeuksia ja vapauksia tulee suojella ja sellaisia henkilötietojen käsittelytoimia ei tule harjoittaa, joihin liittyy korkea riski.

---

[217] CER-direktiivissä on myös määritelty, että riskinarvioinnilla tarkoitetaan kokonaisprosessia, jonka avulla määritetään riskin luonne ja laajuus tunnistamalla ja analysoimalla sellaiset mahdolliset asiaankuuluvat uhat, heikkoudet ja vaarat, jotka voivat johtaa poikkeamaan, ja arvioidaan mahdollinen kyseisen poikkeaman aiheuttama keskeisen palvelun tarjonnan menetys ja häiriytyminen. Vaikka CER-direktiivin keskiössä on etenkin jatkuvuudenhallinta, on riskinarvioinnin hyvän tavan avaaminen säädöstasolla edistyksellistä.

[218] Andersson 2018: 3.

Verrattuna tietoturvariskeihin edellä mainitut seikat tekevät tietosuojariskien arvioimisesta erilaista: metodi pysyy samana, mutta näkökulma on eri. Käytännön työssä tämä menee helposti sekaisin, jolloin tietosuojariskejä arvioidaan organisaationäkökulmasta. Tietoturvariskit ovat helposti synkronoitavissa osaksi organisaation kokonaisriskienhallintaa, sillä haitan vakavuudessa arvioidaan usein samoja asioita liiketoiminnan kannalta, kuten riskin toteutumisen vaikutusta maineeseen ja asiakasluottamukseen, tuloihin sekä toiminnan jatkuvuuteen. Tietosuojariskien osalta vakavuuden arvioinnissa näkökulmana on aina luonnollisen henkilön oikeudet ja vapaudet, kuten esimerkiksi riskin toteutumisen vaikutus henkilön terveyteen, ihmissuhteisiin sekä tietosuoja- ja perusoikeuksien toteutumiseen. Tämä on oleellinen ero, joka tulee ottaa huomioon. Hyvä tietoturvan sääntelyjärjestelmä huomioi myös perusoikeudet ja yksilöt ollakseen hyvä.

Loppupäätelmänä voidaan todeta, että tietoturvan sääntelyjärjestelmässä riskiä on käsitelty monitahoisesti joko tietoturvallisuuteen tai kyberturvallisuuteen liittyvinä riskeinä taikka tietosuojaan liittyvinä henkilötietojen käsittelyn riskeinä. Erityisesti tietoturva- ja tietosuojariskien arviointituloksissa on eroja tietosuoja-asetuksen velvoitteiden takia, sillä jälkimmäisessä arvioidaan tietosuoja-asetuksen vaatimusten mukaisesti uhkien seurauksia luonnollisille henkilöille. Tietoturvariskien arvioinnissa keskitytään seurausten vaikutuksiin organisaationäkökulmasta, kuten muun muassa seurauksia organisaation maineeseen, talouteen ja jatkuvuuteen. Tietosuojariskien arvioinnin tuloksia on mahdollista kuitenkin jatkojalostaa niin, että huomioitaisiin luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien riskien seurauksien vaikutukset myös organisaatiolle: esimerkiksi mikäli tietosuojariskistä aiheutuisi luonnolliselle henkilölle mahdollisesti luottamuksellisen viestinnän ja tietosuojaoikeuksien heikkenemistä, organisaationäkökulmasta tämä voisi aiheuttaa organisaatiolle mainehaittaa ja asiakaskatoa. Yhteistä sekä tietoturva- että tietosuojariskien arvioinnissa on se, että tietoturvaan ja tietosuojaan liittyvät uhat ja riskit on arvioitava negatiivisina. Esimerkiksi tietoturvauhka kuvaa mahdollista negatiivista tapahtumaa ja tietoturvariski kuvaa uhan toteutumisen negatiivisia seurauksia (ja todennäköisyyksiä). Riskien arviointiin liittyvissä ohjeistuksissa on kuvattu myös positiivinen riski, jonka osalta nähdään, että riskejä sisältävästä toiminnasta pidättäytyminen voi johtaa samalla positiivisten mahdollisuuksien menettämiseen ja että riskien arvioinnissa on mahdollista tunnistaa positiivisia mahdollisuuksia[219]. Tämä on kuitenkin huono malli erityisesti tietosuojariskien arvioinnin kannalta. Organisaatioiden ei tulisi arvioida organisaationäkökulmalla mahdollisia positiivisia seurauksia luonnollisiin henkilöihin kohdistuvien riskien toteutumisen kautta taikka ottaa riskejä luonnollisten henkilöiden oikeuksien ja vapauksien kustannuksella ”positiivisten

[219] Esimerkiksi Valtiovarainministeriön ohje riskienhallintaan, s. 11–12 ja 15–16 (Valtiovarainministeriön julkaisuja 22/2017).

mahdollisuuksien” tavoittamiseksi, koska se ei ole hyvän tavan mukaista. Hyvän henkilötietojen käsittelytavan ja lainsäädännön velvoitteiden kautta rekisteröityjen oikeuksia ja vapauksia tulee suojella eikä korkeariskisiä käsittelytoimia tule harjoittaa.

2.2.4 Keskeinen kyberterminologia

Tässä tutkimuksessa käsitellään tietoturvallisuuden yhtenä alaulottuvuutena kyberturvallisuutta, jolloin on tärkeää määritellä kyberturvallisuus käsitteenä, mutta myös muut siihen liittyvät keskeiset käsitteet, kuten digitaalinen turvallisuus, kyberuhka, kyberriski, verkko- ja tietojärjestelmä sekä tietoverkkorikollisuus. Kyseiset käsitteet ovat myös tärkeä osa tietoturvan sääntelyjärjestelmää.

Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristön toiminta on turvattu ja luotettava. Käytännössä kyberturvallisuudella viitataan organisaatioiden ja yhteiskunnan digitalisoitumiseen liittyviin turvallisuushaasteisiin. Kybertoimintaympäristöksi puolestaan kutsutaan sähköistä ja moninaista tietojenkäsittely-ympäristöä, joka on riippuvainen tietojärjestelmien ja -verkkojen toiminnasta. Kyber-sanan merkitys liittyy usein sähköisessä muodossa olevan tiedon käsittelyyn.[220] Kyberturvallisuus ei ole pelkästään ”teknistä tietoturvaa”, vaan käsitteenä se on todella moniulotteinen, ja kyberturvallisuuden merkitys vaikuttaa laajasti leikaten läpi yhteiskunnan organisaatioista kansalaisiin. Kyberturvallisuuden merkitys korostuu esimerkiksi *digitaalisen turvallisuuden* ulottuvuuden kautta, jonka pohjalta OECD on päivittänyt suosituksiaan[221]. Digitaalisella turvallisuudella OECD tarkoittaa kyberturvallisuuden taloudellista ja yhteiskunnallista ulottuvuutta[222]. OECD:n suositusten kehitys kertoo ymmärryksen laajenemisesta, jossa digitaalinen turvallisuus nähdään yhä enemmän yhteiskunnan infrastruktuurin ja palvelujen laadun perustekijänä: kyber- ja tietoturvallisuus ovat laatuelementtejä infrastruktuureille[223]. Tässä tutkimuksessa kyberturvallisuus on tietoturvallisuuden alaulottuvuus (tietoturvallisuuden osa-alue), sillä tietoturva käsittelee laajemmin tietojen turvaamista kyberturvallisuuden keskittyessä enemmän

[220] Suomen kyberturvallisuusstrategia 2013: 12–13; Traficomin julkaisuja 2/2020: 4.
[221] Tällaisia suosituksia ovat mm. 2022 päivitetyt: OECD 2022, *Recommendation of the Council on Digital Security Risk Management*, OECD/LEGAL/0479; OECD 2022, *Recommendation of the Council on National Digital Security Strategies*, OECD/LEGAL/0480; OECD 2022, *Recommendation of the Council on the Digital Security of Products and Services*, OECD/LEGAL/0481; OECD 2022, *Recommendation of the Council on the Treatment of Digital Security Vulnerabilities*, OECD/LEGAL/0482.
[222] OECD 2022, *OECD Policy Framework on Digital Security*: 11. Digitaalisen turvallisuuden riskillä OECD tarkoittaa poikkeamista aiheutuvia taloudellisia ja yhteiskunnallisia riskejä kuin teknisiä riskejä (ks. s. 13).
[223] Pöysti 2023: 41–42.

sähköisen tiedon turvaamiseen järjestelmissä sekä organisaatioiden ja yhteiskunnan toimivuuteen verkko- ja järjestelmäriippuvaisessa kybertoimintaympäristössä.

Suomen kyberturvallisuusstrategiassa 2013 kyberturvallisuus nähdään oikeudellisesti uutena ilmiönä ja strategiassa on korostettu, ettei kyberturvallisuutta ole tarkoitettu oikeudelliseksi käsitteeksi, joka perustaisi uusia toimivaltuuksia viranomaisille ja muille tahoille[224]. Kyberturvallisuusstrategia on valtioneuvoston periaatepäätöksenä oikeudellisesti heikosti velvoittavaa hallinnon virallislähteistöä, joka sitoo julkisoikeudellisia oikeushenkilöitä, hallintoelimiä ja niiden henkilöstöä[225]. Tosiasiassa kyberturvallisuus on kuitenkin nykyään oikeudellinen käsite, jolloin edellä mainittu linjaus on vanhentunut[226] eikä se ole linjassa EU:n viimeaikaisimman lainsäädännön suunnan kanssa. Esimerkiksi EU:n kyberturvallisuusasetuksessa (2019/881/EU) kyberturvallisuus määriteltiin ensimmäistä kertaa laissa, jolloin siitä tuli virallisesti oikeudellinen käsite. Asetuksen *mukaan kyberturvallisuudella tarkoitetaan toimia, joita tarvitaan verkko- ja tietojärjestelmien, tällaisten järjestelmien käyttäjien sekä muiden asianosaisten henkilöiden suojaamiseksi kyberuhilta*. Lisäksi on huomioitava, että jo nykyisin kumottua NIS 1 -direktiiviä tituleerattiin ensimmäiseksi kyberturvallisuutta käsitteleväksi, yleiseurooppalaiseksi oikeudelliseksi säädökseksi ja NIS 2 -direktiiviä eli kyberturvallisuusdirektiiviä rajatessa hakutoiminnolla käsitettä ”kyberturva” tulee peräti 263 hakutulosta. EU:n kyberturvallisuusasetuksen ja NIS 2 -direktiivin mukainen kyberturvallisuuden määritelmä implementoidaan sellaisenaan myös kansalliseen kyberturvallisuuslakiin sekä tiedonhallintalakiin[227].

Lainsäädännössä *kyberuhka* on käsitteenä määritelty kattavammin kuin esimerkiksi tietoturvauhka. Kyberturvallisuusasetuksen mukaan kyberuhkalla tarkoitetaan potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä verkko- ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä sekä muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti. Myös NIS 2 -direktiivissä viitataan kyberuhkalla kyberturvallisuusasetuksen käsitteeseen ja NIS 2 -direktiivissä on määritelty merkittäväksi kyberuhkaksi sellainen, jonka voidaan sen teknisten ominaisuuksien perusteella olettaa vaikuttavan mahdollisesti vakavasti toimijan verkko- ja tietojärjestelmiin tai toimijan palvelujen käyttäjiin

[224] Suomen kyberturvallisuusstrategia 2013: 2. Ks. myös Suomen kyberturvallisuusstrategia 2019, s. 4–10: Vuonna 2019 päivitetty kyberturvallisuusstrategia nojautuu edelleen vuoden 2013 kyberturvallisuusstrategian yleisiin periaatteisiin.
[225] Pöysti 1997: 418.
[226] Kyberturvallisuusstrategiaa tullaan päivittämään NIS 2 -direktiiviä vastaavaksi. Hallituksen esityksessä 57/2024 (s. 56) todetaan, että nykyistä kyberturvallisuusstrategiaa on tarpeen päivittää muuttuneen ympäristön ja uusien sääntelyvelvoitteiden vuoksi, sillä se ei esimerkiksi sisällöllisesti täytä NIS 2 -direktiivin vaatimuksia.
[227] HE 57/2024 vp: 274, 299.

aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. NIS 2 -direktiivin implementoinnin myötä Suomen kyberturvallisuusstrategian 2013 mukaista määritelmää tulisi päivittää ottamaan paremmin huomioon mahdolliset vahingot. Kyseisessä strategiassa kyberuhka tarkoittaa mahdollisuutta tekoon tai tapahtumaan, joka toteutuessaan vaarantaisi jonkin kybertoimintaympäristöstä riippuvaisen toiminnon. Kybertoimintaympäristöön kohdistuvat uhat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen toiminnan[228]. Näin ollen se ei huomioi henkilövaikutuksia, kuten kyberturvallisuusasetus huomioi.

Kyberriskillä tarkoitetaan kybertoimintaympäristöön kohdistuvaa vahinkomahdollisuutta tai haavoittuvuutta, joka toteutuessaan tai jota hyväksi käyttäen voi aiheuttaa vahinkoa, haittaa tai häiriötä kybertoimintaympäristön toiminnasta riippuvalle toiminnolle.[229] Kyberriskit ovat myös sidoksissa oikeudellisiin riskeihin, kuten lakisääteisiin vaatimuksiin tietojenkäsittelytavoista taikka sopimusvaatimuksiin liiketoimintakumppanien tietojen suojaamisesta[230]. Huomioitava on, että kyberturvallisuusasetuksessa, NIS 2 -direktiivissä ja CER-direktiivissä ei ole määritelty kyberriskiä käsitteenä. Kuitenkin ehdotuksessa kyberkestävyyssäädökseksi (COM (2022) 454 final, ”CRA”) on määritelty merkittäväksi kyberturvariskiksi sellainen, jonka voidaan teknisten ominaispiirteidensä perusteella suurella todennäköisyydellä olettaa aiheuttavan poikkeaman, jolla voisi olla vakavia kielteisiä vaikutuksia muun muassa aiheuttamalla huomattavia aineellisia tai aineettomia menetyksiä tai häiriöitä.

Kybertoimintaympäristö on riippuvainen verkko- ja tietojärjestelmien toiminnasta, johon myös keskeiset kyberuhat ja -riskit kohdistuvat. NIS 1 -direktiivin sekä NIS 2 -direktiivin määritelmien mukaan *verkko- ja tietojärjestelmäksi*[231] katsotaan:

a) sähköinen viestintäverkko;

b) yksi laite taikka useamman toisiinsa yhteydessä olevan laitteen ryhmä, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; tai

[228] Suomen kyberturvallisuusstrategia 2013: 13.
[229] Suomen kyberturvallisuusstrategia 2013: 12.
[230] Traficomin julkaisuja 2/2020: 22.
[231] Käsite tietojärjestelmä itsessään sisältää vähintään yhden yksittäisen tietoteknisen laitteen ohjelmistoineen, mutta se voi olla myös laajempi verkottuneiden laitteiden ja ohjelmistojen toiminnallinen kokonaisuus. Ks. Riekkinen 2019, s. 100.

c) digitaalisia tietoja, joita yllä mainituissa järjestelmissä säilytetään, käsitellään, siirretään tai haetaan käyttöä, suojausta, toimintaa tai ylläpitoa varten.

Huomioitava on, että kansallisessa lainsäädännössä, esimerkiksi sähköisen viestinnän palveluista annetussa laissa, on käytetty vakiintuneena käsitteenä *viestintäverkko- ja tietojärjestelmä* NIS 1 -direktiivin suomennoksessa esiintyvän verkko- ja tietojärjestelmän sijaan. Samaa vakiintunutta käsitettä käytetään jatkossakin ja siitä säädetään kyberturvallisuuslaissa vastaavasti kuin NIS 2 -direktiivistä säädetään verkko- ja tietojärjestelmän käsitteestä[232].

Euroopan neuvoston vuoden 2007 tietoverkkorikollisuutta koskevassa yleissopimuksessa (60/2007) tietojärjestelmä on laite tai toisiinsa liitettyjä tai kytkettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten. Huomioitava on se, että yleissopimuksen tietojärjestelmän käsite on omaksuttu kansalliseen rikoslakiin laajassa merkityksessään tarkoittaen ”kaikkia sellaisia järjestelmiä, joissa käsitellään datan muodossa olevia tietoja”[233]. Myöhemmin rikoslain 38 luvun 13 §:ään on lisätty tietoverkkorikosdirektiivin (2013/40/EU) vähimmäisvaatimusten täyttämiseksi tarkennettu tietojärjestelmän määritelmä. Direktiivissä tietojärjestelmällä tarkoitetaan myös tietojärjestelmässä olevaa dataa.[234] Kyseisen rikoslain 38:13 mukaan tietojärjestelmällä tarkoitetaan myös a) laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten sekä; b) dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään sen tai niiden toimintaa, käyttöä, suojausta tai huoltoa varten. Tämä määritelmä vastaa myös suurimmaksi osaksi edellä mainittua NIS 2 -direktiivin tietojärjestelmän määritelmää b ja c -kohdan osalta.

Tietoverkkorikollisuudella (cybercrime) tarkoitetaan rikoksia, jotka kohdistuvat sähköisiin viestintäverkkoihin ja tietojärjestelmiin tai rikokset tehdään niitä hyödyntäen. Tähän sisältyy perinteiset rikollisuuden muodot[235], laittoman sisällön julkaiseminen[236] sekä ainoastaan sähköisissä verkoissa esiintyvät rikokset, kuten palvelunestohyökkäykset ja hakkerointi.[237] Kaiken tyyppisen tietoverkkorikollisuuden suojautumisen osalta ei ole luotu universaaleja ohjeita tai ratkaisuja, vaan organisaatiot ja valtiot soveltavat suojautumiseen kolmeen kategoriaan luokiteltavia mekanismeja: teknologinen suojautuminen, organisaation politiikat ja

[232] HE 57/2024 vp: 144–145.
[233] HE 153/2006 vp: 60; Riekkinen 2019: 101.
[234] HE 232/2014 vp: 38.
[235] Esimerkiksi petokset ja väärennykset.
[236] Esimerkiksi lasten hyväksikäyttö ja rotuviha.
[237] KOM (2007) 267 lopullinen: 2.

lainsäädäntö[238]. Viimeaikaisten lakiuudistuksien myötä lainsäädäntö onkin toiminut yhä enemmän organisaatioiden toimintaa ohjaavana tekijänä tietoverkkorikollisuudelta suojautumisen suhteen.

Tietoverkkorikollisuutta kutsutaan usein myös *kyberrikollisuudeksi*. Muita mahdollisia käytettyjä termejä ovat tietotekniikkarikollisuus, tietokonerikollisuus sekä verkkorikollisuus, joilla viitataan pääosin samaan asiaan ja rikollisten tekomuotojen joukkoon[239]. Selkein ja käytetyin käsite näistä kolmesta on kuitenkin tietoverkkorikollisuus, sillä käsitettä käytetään esimerkiksi säädösaineistoista tietoverkkorikosdirektiivissä ja Euroopan neuvoston yleissopimuksessa tietoverkkorikollisuudesta. Tietoverkkorikollisuuden käsitteen käyttämistä yleiskäsitteenä on myös puollettu kotimaisessa oikeuskirjallisuudessa, kun taas ulkomaisessa oikeuskirjallisuudessa cybercrime-käsitteen käyttö on yleistä[240].

Yhteenvetona todettakoon, että voimassa olevan lainsäädännön kyberkäsitteiden pohjalta on helppo tehdä päätelmä: kyberturvallisuus ei ole enää ainoastaan muotisana. Kyberturvallisuudella tarkoitetaan verkko- ja tietojärjestelmien toiminnasta riippuvaisen kybertoimintaympäristön turvaamista. Kybertoimintaympäristössä tapahtuu sähköistä tiedonkäsittelyä, johon liittyviä kyberriskejä, esimerkiksi tietoverkkorikollisuutta, pyritään hallitsemaan *tietoturvatoimenpiteillä*. Myös viimeaikainen lainsäädännön kehitys ilmentää sitä, kuinka kyberriskien vaikutuksien mitigoimiseksi on asetettu EU:n jäsenvaltioiden laajuisesti riskienhallinnan vaatimuksia organisaatioiden verkko- ja tietojärjestelmien tietoturvan parantamiseksi. Usein lainsäädännössä ilmaistulla verkko- ja tietojärjestelmien tietoturvalla tarkoitetaan juuri kyberturvallisuutta. Kyberturvallisuudesta onkin muotoutunut moniulotteinen oikeudellinen käsite oikeudellistuneen verkkoyhteiskuntamme muuttuessa yhä enemmän riippuvaiseksi verkoista, järjestelmistä ja sähköisistä palveluista. Näillä perustein lainsäädännön kyberturvaan liittyvät vaatimukset ovat luonnollinen osa organisaatioiden tietoturvan sääntelyjärjestelmää. Kyberturvallisuus on yksi tietoturvallisuuden alaulottuvuuksista tietoturvan käsitellessä laajemmin tietojen turvaamista myös fyysisessä ympäristössä, kun taas kyberturvallisuus keskittyy erityisesti sähköisen tiedon suojaamiseen sekä organisaatioiden ja yhteiskunnan toimivuuteen sähköisessä tietojenkäsittely-ympäristössä eli järjestelmä- ja verkkoriippuvaisessa kybertoimintaympäristössä[241]. Tällaista ”hierarkkista” jaottelua ei kuitenkaan aina välttämättä tunnisteta, sillä kyberturvallisuuden käsitteeseen liittyy paljon vivahteita ja sen suhde tietoturvallisuuteen näyttäytyy moninaisena.

---

[238] Ayanso & Herath 2012: 64.
[239] Riekkinen 2019: 161.
[240] Melander & Rautio 2022: 1283; Riekkinen 2019: 161.
[241] Tietoturvatoimenpiteillä suojataan niin henkilötietoja kuin kybertoimintaympäristöä.

Esimerkiksi Tero Haukilehto on jaotellut turvallisuuteen liittyviä käsitteitä eri tasoille, joista ensimmäisellä tasolla on kokonaisturvallisuus, toisella kyberturvallisuus, kolmannella organisaatioturvallisuus, neljännellä tietoturvallisuus ja viidennellä tasolla tietosuoja. Jaottelu perustuu suojauskohteeseen, jolloin (1) kokonaisturvallisuus suojaa yhteiskuntaa, (2) kyberturvallisuus suojaa digitaalista ja verkottunutta yhteiskuntaa tai organisaatiota, (3) organisaatioturvallisuus suojaa organisaatiota (omaisuutta ja henkilökuntaa), (4) tietoturva suojaa tietoa ja (5) tietosuoja suojaa henkilötietoja.[242] Tällainen jaottelu on kuitenkin erittäin altis kritiikille, koska mallissa yritetään jaotella yleisluontoisesti kompleksista asiaa yhteen muottiin. Esimerkiksi henkilöiden suojaamisen ulottuvuus yltää myös tietoturvallisuuteen[243]. Mallissa ei lähestytä asiaa joko organisaationäkökulmasta tai yhteiskuntanäkökulmasta, vaan mallissa yritetään yhdistää molemmat näkökulmat. Ensinnäkin pelkästään organisaationäkökulmasta tarkasteltuna organisaatioturvallisuus ei voi olla luokittelussa kyberturvallisuuden alla, koska suojattavana kohteena työntekijöiden turvallisuus (mahdollisesti jopa henki) priorisoituu aina ensisijaiseksi verrattuna muuhun organisaation omaisuuteen, kuten tietoon ja laitteisiin. Esimerkiksi tulipalossa evakuoidaan aina ensiksi ihmiset, jolloin työt keskeytetään ja tietoa sisältävät laitteet ja paperit tulisi jättää työpisteille sellaisenaan[244]. Toinen kritiikki on se, että ilman onnistuneita hallinnollisia ja fyysisiä tietoturvatoimenpiteitä, ei kyberympäristö ole asianmukaisesti suojattu. Toimenpidenäkökulmasta tietoturva sijoittuu siitä syystä kyberturvallisuuden yläpuolelle, koska tietoturvatoimenpiteillä suojataan kybertoimintaympäristöä. Puhtaasti organisaationäkökulmasta jaottelu olisi seuraavanlainen: 1) kokonaisturvallisuus (eli organisaatioturvallisuus[245]), 2) tietoturvallisuus, 3) kyberturvallisuus ja 4) tietosuoja. Yhteiskunnallisesta näkökulmasta jaottelu olisi vastaavanlainen suojattavien kohteiden perusteella: 1) kokonaisturvallisuus 2) tietoturvallisuus 3) kyberturvallisuus ja 4) tietosuoja. Edellä esitetyn yhteiskuntanäkökulman kaikkiin käsitteisiin tulisi sisältyä organisaatioissa tehtävä kokonaisvaltainen tietoturvatyö. Huomioitava on, että lainsäädännön näkökulmasta painotus on erilainen, sillä lainsäädännössä korostuu erityisesti henkilötietojen ja yksilöiden oikeuksien suojaaminen: esimerkiksi kansallisessa perustuslaissa on perusoikeutena turvattu henkilötietojen suoja ja henkilötietoja suojataan myös kattavilla tietosuojasäädöksillä. Tietoturva ja kyberturvallisuus saavat lainsäädännön näkökulmasta

[242] Haukilehto 2024: 8–9.
[243] Kyberturvallisuuteen määritelmätasolla sisältyy henkilöiden suojaamisen ulottuvuus, joka toki seuraa myös tietoturvallisuuden toteuttamisesta. Ks. HE 57/2024 vp, s. 215–216.
[244] Tämä tulee huomioida myös jatkuvuussuunnitelmissa ja mahdollisessa tietoturvariskien arvioinnissa.
[245] Organisaatioissa organisaatioturvallisuudesta käytetään myös käsitettä kokonaisturvallisuus.

vähemmän "suoraa" painoarvoa kuin tietosuoja: tietoturvaan liittyvä lainsäädäntö on hajanaista, eikä meillä ole perustuslaissa tietoturva- tai kyberturvasäännöstä.

2.3 Kehitys informaatioyhteiskunnasta oikeudellistuneeksi verkkoyhteiskunnaksi

Tietoturvan sääntelyjärjestelmän muodostumisen taustalla on vaikuttanut suuresti teknologian kehittymisen mahdollistama digitalisaatio. Digitalisaatio on varsin uusi asia, sillä suurimmat kehitysharppaukset on otettu vasta 90-luvulta lähtien. Tällöin internetin yleistymisen ja www-selaimen luonnin myötä nykyinen palvelupohjainen malli lähti alun perin liikkeelle. Älypuhelimet, digitaaliset palveluekosysteemit ja muun muassa sosiaalisen median jakamiskulttuuri ovat vasta yli 10 vuotta vanhoja ilmiöitä. Internet-verkon yleistymisen myötä sen hyödyntämiseen on luotu enemmän palveluita ja toimintamalleja, joiden myötä myös erinäisten asiointipalveluiden tuottaminen on tullut kustannustehokkaammaksi ja helpommaksi.[246] Informaatioteknologia on muuttunut entistä enemmän viestintäteknologiaksi internetin ja sen mahdollisuuksien myötä. Viestintäteknologian vahvistajia ovat olleet muun muassa sähköposti ja sähköpostilistat, kotisivut, uutisryhmät sekä chat-yhteisöt, jotka kaikki ovat kytköksissä internettiin ja osaltaan vahvistavat kaikenlaisten tietojen digitalisointia.[247] Tietojenkäsittely, työtehtävien ja muiden asiointipalveluiden hoitaminen on ajasta ja paikasta riippumatonta. Viisi huomattavaa tekijää tälle muutokselle ovat olleet päätelaitteet, tietoliikenne, tapa tuottaa palveluita (esimerkiksi pilvipalvelut), sosiaalinen media ja jalostettava tieto (esimerkiksi kerättävä tieto ja tekoäly).[248] Informaation käyttö ja hallinta, niin arjessa kuin työelämässä, ovat mullistuneet kannettavien laitteiden käytön myötä. Kannettavat laitteet yhdistettyinä hakukoneiden ja hakuteoksien (esimerkiksi Wikipedia) käyttöön ovat mullistaneet tiedon hallinnan ja faktatiedon hankkimisen.[249] Tosin tässäkin on huomioitava asioiden kääntöpuoli. Koska tietoa on valtavasti tarjolla, on myös osattava erottaa relevantti ja totuudenmukainen tieto väärästä ja muunnellusta informaatiosta.

Digitalisaation myötä tietotekniikkaa hyödyntänyt *informaatioyhteiskunta* (käytetty myös nimitystä tietoyhteiskunta[250]) on muuttunut askeleen kehittyneemmäksi digitaalisen toimintaympäristön *verkkoyhteiskunnaksi*, joka on tietojärjestelmiin ja -verkkoihin sitoutunut sekä niiden varassa toimiva yhteiskunta. Verkkoyhteiskunnan keskeisiä tunnuspiirteitä ovat muun muassa tietoverkkojen käytön

[246] Valtiovarainministeriön julkaisu 10/2017: 15, 83–84
[247] Seipel 2001: 131.
[248] Järvinen & Rousku 2017: 20, 28–29.
[249] Kemppinen 2011: 16.
[250] Riekkinen 2019: 37–38.

määrän nopea kasvu sekä muuttuminen oletusarvoksi kansalaisten arkipäivän toiminnoissa, verkkoviestinnän monipuolistuminen, talouden lisääntyvä verkkosidonnaisuus, sähköinen kaupankäynti, sähköisen hallinnon muuttuminen informaatiohallinnoksi, tietojärjestelmien hyödyntäminen tuomioistuimissa sekä avoimien tietoverkkojen toimimisen globaaliset vaikutukset.[251] Olemme erittäin riippuvaisia tietoverkoista, mikä korostaa tietoturvallisuuden ja sen sääntelyn merkitystä. Tietoverkoista onkin oikeudellisen merkityksensä vuoksi tullut keskeinen kipupiste sääntelyssä[252].

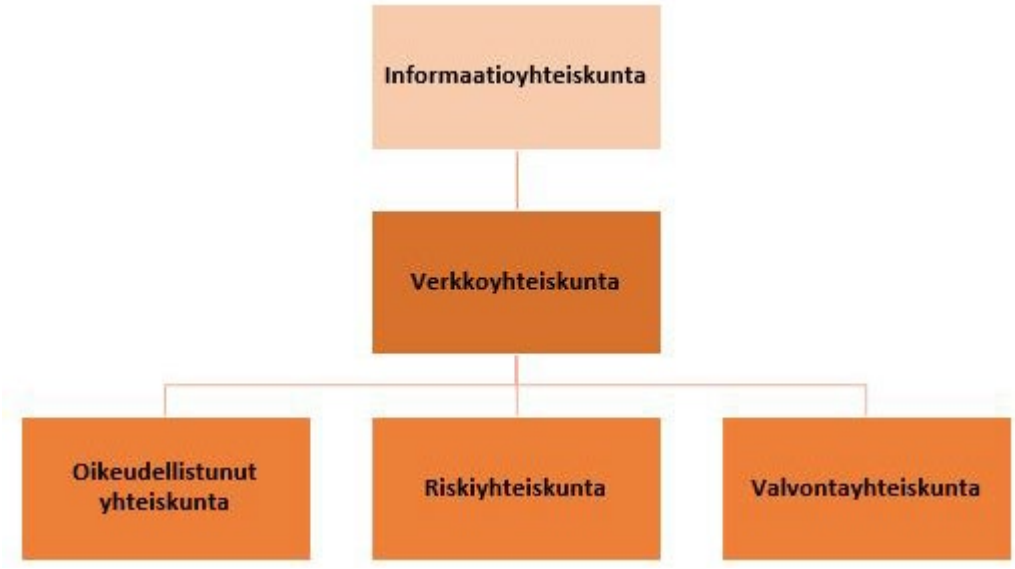
Järjestelmien, laitteiden ja tietoverkkojen merkityksen muuttuessa ilmenee myös lainsäädännöllisiä muutostarpeita sekä muutoksia oikeudellisissa kysymyksien asetteluissa. Toimiympäristömme muuttuessa oikeudellinen sääntely lisääntyy, oikeusperiaatteet muuttuvat ja oikeuskäsitteiden määrä lisääntyy. Puhutaan myös *oikeudellistuneesta yhteiskunnasta* taikka *oikeudellistuneesta verkkoyhteiskunnasta*, sillä suurin osa asioista tai ilmiöistä on jollain tapaa oikeudellisesti säänneltyä. Oikeudellistunut verkkoyhteiskunta ilmenee muun muassa uudenlaisena sääntelynä sekä ihmiskäsityksenä. Perusoikeudet ovat siirtyneet enemmän verkkoon, sähköiset palvelut ja asiointi ovat tulleet jäädäkseen, tieto- ja tietoverkkorikokset ovat lisääntyneet sekä infrastruktuurien merkitykset ovat muuttuneet. Myös informaatio ja sen käsittely oikeudelliselta asemaltaan ovat muuttuneet yhteiskunnassa. Tämän muutoksen yhteydessä ihmis- ja perusoikeuksien tärkeys ja suojaaminen järjestelmätasolta lähtien on kasvanut. Oikeudellistuminen saatetaan nähdä myös negatiivisena ilmiönä, joka ilmenee muun muassa säädösten ja säännösten lisääntymisenä. Keskeistä tässä muutoksessa on joka tapauksessa tietoturvallisuuden korostunut merkitys yhteiskunnan rakennetekijänä sekä yksilön oikeuksien toteutumisessa.[253] Yhtä lailla puhutaan nykyään digitaalisesta oikeusvaltiosta[254].

Informaatioinfrastruktuuri on digitalisoitumisen myötä entistä enemmän riippuvainen tietojärjestelmistä, tietoverkoista, informaatiotyökaluista, datan prosessoinnista ja tietomarkkinoista, minkä vuoksi toimiympäristössä ilmenee myös uudenlaisia riskejä. Näistä uudenlaisista riskeistä ovat esimerkkinä kyberriskit. Uudet riskit luovat myös uusia haasteita sääntelyn osalta. Näin ollen verkkoyhteiskuntamme on *riskiyhteiskunta*, jossa tietoturvallisuuden merkitys on entisestään kasvanut.[255]

---

[251] Saarenpää 2016a: 79, 103–106.
[252] Saarenpää & Riekkinen 2023: 68.
[253] Saarenpää 2016a: 79, 109; Saarenpää 2016b: 63–64; Saarenpää 2015: 203.
[254] Saarenpää & Riekkinen 2023: 1.
[255] Saarenpää 2016a: 81, 142; Saarenpää 2016b: 64–65; Saarenpää & Riekkinen 2023: 17.

Verkkoyhteiskuntamme on nykyään yhä enemmän myös *valvontayhteiskunta*.[256] Samaan aikaan olemme riippuvaisia teknologiasta, verkottuneesta yhteiskunnasta ja sen infrastruktuurista sekä muista mahdollisuuksista. Ikään kuin olisimme jumiutuneet verkkoon, joka on jatkuvan valvonnan alla. Valvonta tapahtuu rutiininomaisesti sekä lokaalisti että globaalisti, se on nyky-yhteiskunnassa jopa välttämätön ominaisuus eikä se ole ainoastaan valtion toteuttamaa. Monet suuret yritykset keräävät dataa asiakkaistaan luodakseen kuluttajaprofiileja. Vaikka valtiollinen seuranta on saanut suuren huomion uutisoinneissa, korporatiivinen seuranta on itseasiasta valtiollista yleisempää. Yhtäläisesti kasvaneella valvonnalla pyritään ylläpitämään ja luomaan turvallisuutta, esimerkiksi ehkäisemällä terrorismia ja takaamalla kansallinen turvallisuus, taikka toteuttamaan kohdistettua markkinointia. Samaan aikaan valvonta kuitenkin kajoaa perusoikeuksiimme. Keskeisenä elementtinä valvonnassa on luottamus.[257] Toisaalta voidaan todeta, että valvontaa toteutetaan luottamuksen puutteesta. Samaan aikaan kansalaiset sallivat heidän tekemistensä valvomisen, koska he luottavat ”isoveljeen”, joka valvoo. Joka tapauksessa kansalaisilla ei välttämättä ole mahdollisuuksia pysyä valvonnan ulkopuolella verkottuneessa, digitalisaation ja globalisaation myötä pienentyneessä nykyyhteiskunnassa. Kukaan ei pääse täysin pakoon hakukoneita ja sosiaalista mediaa, mutta paljon riippuu myös omasta toiminnasta, etenkin ei-julkisuuden henkilöiden kohdalla[258].



Kuvio 4. Informaatioyhteiskunnan kehittyminen verkkoyhteiskunnaksi

[256] Saarenpää 2016b: 65–66; Saarenpää & Riekkinen 2023: 18.
[257] Wiatrowski 2016: 109, 116; Korja 2016a: 197–198; Hildén 2019: 22.
[258] Järvinen 2022a: 322.

Edellä oleva kuvio havainnollistaa, kuinka informaatioyhteiskunta on muuttunut nykyajan verkkoyhteiskunnaksi, jota kuvataan myös oikeudellistuneeksi (verkko)yhteiskunnaksi, riskiyhteiskunnaksi sekä valvontayhteiskunnaksi sen ominaispiirteiden takia.

Tietoturvallisuuden tärkeys korostuu kaikissa edellä mainituissa yhteiskuntatyypeissä ja se heijastuu erityisesti erilaisista tarpeista. Riippuvuutemme tietoverkoista luo tarpeen tietoturvallisille ratkaisulle, tietoturvariskien hallinnalle sekä tietoturvallisuustason ylläpitämiselle valvonnan avulla. Ennen kaikkea muuttunut toimintaympäristö vaatii sellaista tietoturvan sääntelyjärjestelmää, joka olisi proaktiivinen ja huomioisi varhaisessa vaiheessa uudet riskit sekä samalla ohjaisi muuttuvaa teknologista toimintaympäristöä teknologianeutraalisti. Tällöin myös nykyinen lainsäätäjäriski pienenisi, jolloin lainsäädäntö olisi todennäköisemmin ajankohtaista toimintaympäristön muutoksista huolimatta. Tietoturvallisuuden yksi keskeisistä tavoitteista on proaktiivisesti varautua ympäristön uhkiin, koska reaktiivinen tietoturva tarkoittaa usein sitä, että uhkat ovat jo toteutuneet ja vahinkoja pyritään sillä hetkellä minimoimaan. Yhtä lailla sääntelyn tulisi olla proaktiivista eikä vastakohtaisesti reaktiivista, jolloin lainsäädäntö jälkikäteen reagoi jo tapahtuneisiin yhteiskunnan muutoksiin.

Yhteenvetona voidaan todeta, että teknologian kehitys ja sen mahdollistama digitalisaatio ovat suuresti vaikuttaneet nykyisen tietoturvan sääntelyjärjestelmän kehittymisen taustalla. Digitalisaatio on ilmiönä varsin tuore, ja siihen liittyvät ilmiöt ovat kehittyneet nopealla tahdilla. Tällaisia ilmiöitä ovat olleet internetin käytön yleistymisen jälkeen muun muassa digitaalisiin palveluihin ja älypuhelimella asiointiin siirtyminen, sosiaalisen median jakamiskulttuuri, kannettavat päätelaitteet ja älylaitteet, pilvipalvelut sekä nykyisin myös tekoälypohjaisten työkalujen käytön lisääntyminen. Tietojen käsittely on yhä enemmän ajasta, paikasta ja jopa laitteesta riippumatonta. Yhteiskuntamme on muuttunut informaatioyhteiskunnasta verkkoyhteiskunnaksi, jota voidaan kutsua myös oikeudellistuneeksi verkkoyhteiskunnaksi, riskiyhteiskunnaksi sekä valvontayhteiskunnaksi. Olemme erittäin riippuvaisia tietoverkoista ja järjestelmistä. Tämä lisää riskejä, sillä esimerkiksi perinteinen rikollisuus on siirtynyt yhä enemmän verkkoon ja kybertoimintaympäristömme tietoturva on päivittäin uhattuna. Olemme jo nyt huomanneet, kuinka datakaapelit ovat vaikeasti suojattavissa merenpohjassa tai kuinka tekoälypohjaisten sovellusten avulla tietojen kalastelukampanjat ovat muuttuneet entistä uskottavimmiksi. Digitaaliteknologioiden kasvava merkitys huomioon ottaen, nykyiseen oikeudelliseen kehykseen sisältyy tärkeitä kyberturvallisuuden osatekijöitä, kuten tuotteiden, palveluiden ja prosessien sisäänrakennettu turvallisuus ja

häiriönsietokyky[259]. Digitalisaation kehittyminen on riippuvainen luottamuksesta, kun taas kyberturvallisuuden avulla voidaan varmistaa luottamus digitaaliteknologiaan ja digitalisaatioon[260]. Tietoturvallisuuden sääntelyn merkitys on kasvanut ja siksi sekä perusoikeuksien että organisaatioiden luottamuksellisten tietojen turvaamiseksi tietoturvallisuuden sääntelyä on kehitettävä hyvien tietoturvallisten käytänteiden suuntaan sekä kohdistettava laajemmin kaikkiin organisaatioihin koosta riippumatta.

Ollakseen hyvä, tietoturvan sääntelyjärjestelmän on oltava sekä teknologianeutraali että proaktiivinen, jotta se pysyisi yhteiskunnan kehityksen mukana. Näin ollen nämä kaksi elementtiä ovat myös hyvän tietoturvan sääntelyjärjestelmän eräänlaisia kriteerejä. Nykyisessä verkkoyhteiskunnassamme muuttuvat riskit, valvonta ja näiden myötä oikeudellistuminen tulevat todennäköisesti olemaan pysyviä ominaispiirteitä osana kehitystä. Nämä asettavat myös reunaehtoja tietoturvallisuuden sääntelyjärjestelmälle. Lisäksi tulevaisuudessa tietoturvallisuuden sääntelyjärjestelmään tulee suuresti vaikuttamaan tekoälyn laaja käyttöönotto tietojen käsittelyssä.

2.4 Tietoturvaan liittyvät meta- ja oikeusperiaatteet informaatio-oikeuden alalla

2.4.1 Oikeus tietoturvaan periaatteena

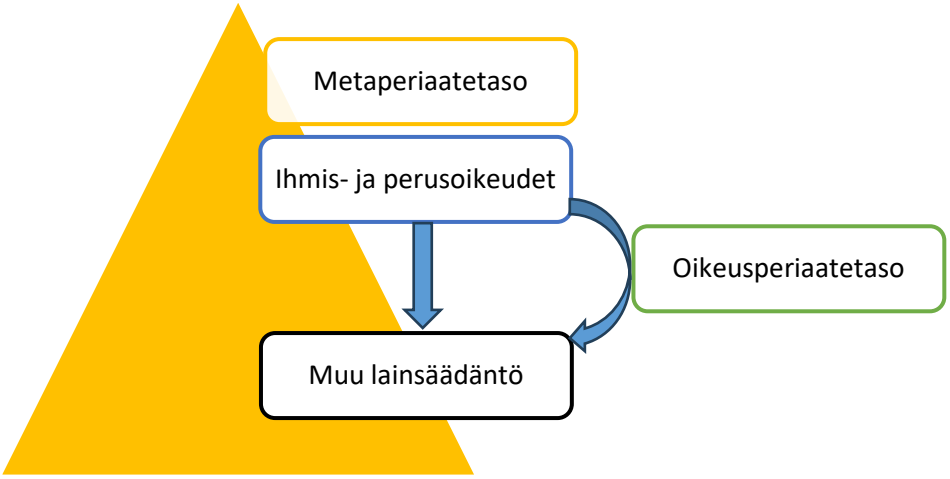
Yhteiskuntamme muutos ja datakeskeisyys sekä riippuvuutemme tietoverkoista kasvattavat tietoturvallisuuden merkitystä lainsäädännössä, minkä vuoksi on oleellista tarkastella tässä tutkimuksessa tietoturvaa periaatetasolta lähtien.

Ihmisoikeudet ja perusoikeudet, joita käsitellään jäljempänä, ovat itsemääräämisoikeuttamme turvaavia oikeuksia. Ne eivät kuitenkaan ole oikeusjärjestelmän ylimmän tason oikeuksia, vaan ihmis- ja perusoikeuksien yläpuolella ovat niistä

[259] Ks. Euroopan unionin neuvosto, EU:n digitaalipolitiikan tulevaisuus – Neuvoston päätelmät 21.5.2024: 6. Euroopan unionin neuvosto on myös ilmaissut huolensa siitä, kuinka digitaalisten palveluiden käyttäjät luovuttavat valtavan määrän dataansa vastineeksi pääsystä palveluun ymmärtämättä kuitenkaan täysin sitä, mihin heidän dataansa käytetään ja mitä seurauksia sillä on (ks. Ibid, s. 8). Huoli on aiheellinen, sillä nykyisessä yhteiskunnassa (henkilö)tieto on suojattavaa pääomaa, ja luonnolliset henkilöt eivät välttämättä ymmärrä tietojensa arvoa.

[260] Euroopan unionin neuvosto, Euroopan digitaalisen tulevaisuuden rakentaminen - Neuvoston päätelmät 9.6.2020: 11. Kyberturvallisuudella on ratkaiseva rooli menestyksekkään digitaalisen yhteiskunnan kulmakivenä, sillä se säilyttää kansalaisten luottamuksen järjestelmiin. Ks. Euroopan unionin neuvosto, Council Conclusions on the Future of Cybersecurity: implement and protect together 21.5.2024, s. 5.

kertovat metaoikeudet ja -periaatteet.[261] *Metaperiaatteet* ovat oikeusjärjestyksen ydinarvoja, jotka ovat ihmis- ja perusoikeuksien taustalla olevia oikeuksia oikeuksista[262]. Oikeustieteessä periaatteet ovat tulkintaa ohjaavia ja sääntelyä systematisoivia käsitteitä, jotka saavat tukea lainsäädännöstä, tuomioistuinratkaisuista tai oikeuskirjallisuudesta[263].



Kuvio 5. Oikeuden eri periaatetasot

Edellä olevassa kuviossa havainnollistetaan, että oikeuden periaatetasolla ylimpänä ovat metaperiaatteet, jotka heijastavat oikeusjärjestyksen ydinarvoja. Metaperiaatteet kertovat ihmis- ja perusoikeuksista, jotka ovat tästä syystä metaperiaatetason alapuolella. Sääntelyn lähtökohtina toimivien ihmis- ja perusoikeuksien pitäisi heijastua myös muusta lainsäädännöstä, minkä vuoksi lainsäädäntötaso on esitetty kuviossa alimpana. Metaperiaatteisiin liittyvät alisteiset oikeusperiaatteet luovat yhteyksiä säännösten välille.

Tomi Voutilaisen mukaan informaatio-oikeuden kantava, ylätason metaperiaate on ”oikeus tietoon”, joka kattaa yksilöä koskevan oikeuden saada tietoa ympäröivästä yhteiskunnasta ja oikeudesta omiin tietoihinsa.[264] Ahti Saarenpää puolestaan tunnistaa informaatio-oikeuden metaoikeuksiksi kahdeksan yleistä periaatetta: oikeus tietää, oikeus tietoon, informaation vapaus, informaation kulun vapaus, oikeus hyvään informaatiohallintoon, oikeus viestintään, tiedollinen itse-

[261] Saarenpää 2015: 221–222.
[262] Tämä näkökulma on yhteistä Saarenpään ja Voutilaisen kesken. Metaoikeudet ovat yhteiskuntasopimusten tasoisia tavoitteellisia, moraalisia päämääräoikeuksia, jotka ovat ihmis- ja perusoikeuksien sääntelyn selkeitä taustakertomuksia sekä myös niiden toteuttamisen keskeisiä edellytyksiä. Ks. Saarenpää & Riekkinen 2023, s. 172.
[263] Neuvonen 2019: 46.
[264] Voutilainen 2012: 33–35; Voutilainen 2019: 25–26.

määräämisoikeus sekä oikeus tietoturvaan[265]. Myöhemmin tähän listaan on myös lisätty oikeus avoimeen tietoon sekä oikeus hyvään informaatioinfrastruktuuriin[266]. Oikeus tietoturvaan on tässä tutkimuksessa erityistarkastelussa tutkimustehtävän takia, ja koska Saarenpään ja Riekkisen systematiikassa oikeus tietoturvaan kuuluu metaoikeuksiin. Huomioon on otettava, että Voutilaisen ja Saarenpään käsitteistössä on eroavaisuus: Voutilaisen käsitteistössä on käytössä metaperiaatteet ja Saarenpään käsitteistössä metaoikeudet. Tässä tutkimuksessa käytettävä käsite on metaperiaate, sillä näkemykseni mukaan myös metaoikeudet ovat ikään kuin periaatteita, koska niitä ei ole kirjoitettu suoraan lakiin, ja näin periaate on käsitteenä paremmin kuvaava.

Metaperiaatteista on erotettava *oikeusperiaatteet,* jotka ovat instrumentteja oikeudellisesti merkityksellisten ilmiöiden tunnistamiseen, ymmärtämiseen ja sääntelyyn. Ne auttavat tunnistamaan, mikä on oikeudellisesti olennaista[267]. Oikeusperiaatteet ovat metaperiaatteisiin liittyviä alisteisia periaatteita, joilla luodaan yhteyksiä eri säännösten välille. Oikeusperiaatteille ominaista on esimerkiksi niiden arvosidonnaisuus, säätämättömyys, ylipositiivisuus, universaalisuus sekä punnittavuus yksittäisen periaatteen painoarvon mukaan. Voutilaisen mukaan näillä perustein informaatio-oikeuden näkökulmasta oikeusperiaatteita ovat oikeus viestintään, julkisuusperiaate, tiedon omistusoikeus sekä tiedollinen itsemääräämisoikeus.[268]

Saarenpään mukaan informaatio-oikeuden metaoikeuksia täydentäviä erityisiä oikeusperiaatteita ovat yksityisyys, henkilötietojen suoja, avoimuus, sananvapaus, viestinnän vapaus, julkisen palvelun periaate, teknologianeutraalisuuden periaate sääntelyperiaatteena sekä monopolien kiellon periaate immateriaalioikeuksien osalta[269].

[265] Saarenpää 2016a: 213.
[266] Saarenpää & Riekkinen 2023: 172.
[267] Pöysti 1997: 556–557.
[268] Voutilainen 2009: 133; Voutilainen 2012: 33–35; Voutilainen 2019: 25–26.
[269] Saarenpää 2016a: 218–219.

Taulukko 1. Saarenpään ja Voutilaisen näkemykset meta- ja oikeusperiaatteista

	Saarenpää	**Voutilainen**
Metaperiaatteet	• Oikeus tietää • Oikeus tietoon • Informaation vapaus • Informaation kulun vapaus • Oikeus hyvään informaatiohallintoon • Oikeus viestintään • Tiedollinen itsemääräämisoikeus • **Oikeus tietoturvaan** • Oikeus avoimeen tietoon • Oikeus hyvään informaatioinfrastruktuuriin	• Oikeus tietoon
Oikeusperiaatteet	• Yksityisyys • Henkilötietojen suoja • Avoimuus • Sananvapaus • Viestinnän vapaus • Julkisen palvelun periaate • Teknologianeutraalisuus • Monopolien kiellon periaate	• Oikeus viestintään • Julkisuusperiaate • Tiedon omistusoikeus • Tiedollinen itsemääräämisoikeus

Näin ollen Voutilaisen ja Saarenpään näkemykset eroavat meta- ja oikeusperiaatteiden suhteen. Yhteistä molempien näkemyksille on se, että oikeus tietoon on metaperiaate. Voutilaisen mukaan oikeusperiaatteet ovat metaperiaatteisiin liittyviä alisteisia periaatteita, joille ominaista on muun muassa säätämättömyys[270]. Vastakohtaisesti Voutilaisen tulkinnalle Saarenpää luokittelee esimerkiksi henkilötietojen suojan metaoikeuksia täydentäväksi oikeusperiaatteeksi[271], vaikka henkilötietojen suojasta on säädetty sekä kansallisesti että kansainvälisesti. Tietoturvanäkökulmasta Saarenpään listaus on varsin kattava, ja Saarenpään luettelemat oikeusperiaatteet ovat selkeästi alisteisia esimerkiksi oikeus tietoturvaan -metaperiaatteelle. Näin ollen säätämättömyys ei ole Saarenpään tulkinnassa oikeusperiaatteiden ominaisuus, mikä on varsin paikallaan oleva tulkinta.

[270] Voutilainen 2009: 133; Voutilainen 2012: 33–35; Voutilainen 2019: 26–26.
[271] Saarenpää 2016a: 218–219.

Saarenpää perustelee tietoturvan kuuluvaksi metaoikeuksiin, koska yksilöillä tulee olla oikeus muun turvallisuuden lisäksi myös tietoturvaan sekä tietoturvalliseen informaatioinfrastruktuuriin, ja asianmukaisen tietoturvan avulla voidaan taata nykyisen verkkoyhteiskunnan informaatioinfrastruktuurin ja sen käytön toimivuus[272]. Voutilaisen mukaan Saarenpään osoittamat periaatteet (eli muun muassa oikeus tietoturvaan), eivät voi olla metatason periaatteita, sillä ne ovat toisiinsa nähden alisteisia. Voutilaisen mukaan nämä ovat informaatio-oikeudellisia tai siihen läheisesti liittyviä periaatteita, joista kuitenkin yksi nousee keskeisimmäksi: oikeus tietoon. Näin ollen muut periaatteet olisivat alisteisia tälle periaatteelle. Oikeus tietoon metaperiaatteena on myös perusteltavissa Voutilaisen mukaan monikansallisten sopimusten ja säädösten perusteella, sillä niiden sääntelyn kohteena on tietoon liittyvät oikeudet. Periaatteen ympäröivät kysymykset siitä kenellä on oikeus tietoon, missä tilanteissa tämä oikeus syntyy ja mihin tietoihin oikeus ulottuu. Esimerkiksi tietosuojasääntely kohdistuu kysymyksiin kenellä, missä tilanteessa ja milloin on oikeus käsitellä henkilötietoja. Oikeutta tietoon voidaan jakaa periaatetasolla sekä yksilön oikeuteen omiin tietoihinsa että oikeuteen saada tietoa ympäröivästä yhteiskunnasta.[273]

Saarenpään perustelu tietoturvan kuulumisesta metaoikeuksiin on hyvin perusteltu, ja se korostaa tietoturvan tärkeyttä, sillä ilman tietoturvaa ja toimivaa verkkoyhteiskunnan informaatioinfrastruktuuria moni muu meta- ja oikeusperiaate ei toteudu. Lisäksi huomioitava on, että Saarenpään ja Voutilaisen esittämät oikeusperiaatteet ovat selkeästi alisteisia oikeus tietoturvaan metaperiaatteelle, mikä myös puoltaa Saarenpään kantaa. Saarenpäällä on useampi metaperiaate ja näkökulmani mukaan nämä eivät välttämättä ole alisteisia toisiinsa nähden vaan toisiinsa linkittyneitä, yhtä tärkeitä, itsenäisiä metaperiaatteita. Saarenpään tulkinnan mukaisesti metaperiaatteilta ei vaadita itsenäisyyttä, vaan niillä voi olla riippuvuussuhteita tai kytköksiä toistensa välillä, esimerkiksi ilman tietoturvaa moni Saarenpään metaperiaatteista ei toteudu. Tämä ei kuitenkaan tarkoita, että ne olisivat suoraan alisteisia oikeus tietoturvaan -metaperiaatteelle. Näin kompleksisessa, verkottuneessa yhteiskunnassa ei ole mahdollista, että informaatio-oikeudessa olisi yksi metaperiaate, johon verrattuna kaikki muut periaatteet olisivat alisteisia.

Korostamalla oikeutta tietoon ainoana metaperiaatteena Voutilainen kaventaa tällä näkemyksellään tietoturvan tärkeyttä. Voutilaisen näkökulma on erittäin positiivisluontoinen, joka keskittyy ainoastaan oikeuteen saada tietoa, mutta samalla se asettaa vaatimuksen tiedon *käytettävyydelle* (saatavuudelle), joka on myös yksi tietoturvan kolmesta ulottuvuudesta. Käytettävyyden vaatimusten ohella henkilön

[272] Saarenpää 2016a: 123, 218; Saarenpää & Riekkinen 2023: 177.
[273] Voutilainen 2019: 26, 29, 32.

saaman tiedon tulisi olla eheää eli se ei saisi olla virheellistä tai manipuloitua, koska muutoin oikeudesta saada tietoa ei ole paljoa iloa.

Oikeus tietoturvaan sisältää automaattisesti velvoitteita ja toimenpiteitä, jotta tietoa ei saisi oikeudettomat henkilöt. Tämä on perustavanlaatuinen ja korostettava näkökulma tietomäärän kasvaessa muun muassa ydinalustapalveluissa, jota ei voi sivuuttaa. Näin ollen oikeus tietoturvaan painottaa myös suojavelvoitteita, tiedon *käytettävyyttä* ja *eheyttä*[274] sekä ”ei-oikeutta tietoon” -ulottuvuutta eli tiedon *luottamuksellisuutta*. Oikeus tietoon ainoana metaperiaatteena ei huomioi riittävällä tasolla tietoturvan eri ulottuvuuksien tärkeyttä ja erityisesti sitä, että kaikilla ei tulisi olla lähtökohtaisesti oikeutta tietoon. Täten oikeutta tietoturvaan ei tulisi hierarkisoida alisteiseksi oikeus tietoon -metaperiaatteeseen nähden. Metaperiaatetasolla tietoturva nähdään myös ensisijaisesti yhteiskunnan toimivuuden ja yksilön oikeuksien toteutumisen takeena, jolloin se toimii yhteiskunnallisena tavoitetilana ja kollektiivisena hyvänä[275]. Näin ollen sekä oikeus tietoturvaan että oikeus tietoon ovat periaatteina Saarenpään systematiikan mukaisesti vähintäänkin samantasoisia, itsenäisiä metaperiaatteita.

Voutilainen katsoo oikeuden tietoturvaan olevan perusoikeustason informaatiooikeudellinen periaate. Sen sisältönä on tiedon luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen lainsäädännöllisin keinoin. Tietoturvallisuus on myös ICT-oikeudellinen periaate, sillä se pohjautuu tietojenkäsittelyn, tietojärjestelmien ja -verkkojen sekä informaatio- ja viestintäteknologian turvaamiseen normaali- ja poikkeusoloissa. Periaatteena tietoturva on vaikeasti hallittava, koska se on myös käsite. [276] Voutilaisen näkemyksen mukaan oikeus tietoturvaan perusoikeustasoisena oikeutena linkittyy henkilötietojen suojan lisäksi myös luottamuksellisen viestinnän suojan oikeuteen sekä asiakirjajulkisuuteen[277]. Käytännössä tietoturvalla suojataan asiakirjojen ja muiden dokumenttien luottamuksellisuutta, eheyttä ja saatavuutta, luottamuksellista viestintää, henkilötietoja, tiedollisia tekijänoikeuksia ja liikesalaisuuksia. Linkitys tulisi kuitenkin myös kohdistua omaisuuden suojaan, sillä usein tietoturvaloukkauksissa saatetaan rikkoa samaan aikaan omaisuuden suojaan liittyviä oikeuksia[278].

Valtaosa tietojen käsittelystä on nykyään sähköisessä muodossa, mikä lisää vaatimuksia tietojärjestelmien ja -verkkojen turvaamiselle. Tästä näkökulmasta olisikin nykyaikaisempaa korostaa oikeutta kyberturvaan perusoikeustason

[274] Ks. luvusta 2.2.1 (”Tietoturva”) tietoturvallisuuden kolme ulottuvuutta: Luottamuksellisuus, eheys ja käytettävyys (saatavuus).
[275] Råman 2006a: 819.
[276] Voutilainen 2012: 37–38.
[277] Voutilainen 2019: 33.
[278] Ks. lisää luku 2.5.2 (”Oikeus turvallisuuteen ja omaisuuden suojaan”).

periaatteena tai jopa oikeusperiaatteena. Oikeutta kyberturvaan ei ole juurikaan nostettu vaihtoehdoksi oikeuskirjallisuudessa, mutta sitä on hyvä tarkastella yhtenä nykyajan vaihtoehtona digitalisoitumisen edetessä ja tiedon siirtyessä entistä enemmän verkkoihin. Tällöin tämä olisi selkeästi käsitteenä myös alisteinen ”taustakertomus” tietoturvalle, tietoturvan kattaessa laajemmin muun muassa fyysisen ympäristön turvallisuuden ja tietoturvalliset toimintatavat digitaalisen toimintaympäristön ulkopuolella[279]. Kyberturva keskittyisi nimenomaan verkottuneen ympäristön järjestelmiin ja sähköisiin palveluihin kohdistuviin kyberuhkiin[280], jotka muodostavat vakavammat ja todennäköisemmät riskit yksilöiden kannalta nyky-yhteiskunnassa[281].

Yhteenvetona voidaan todeta, että informaatio-oikeuden yksi keskeisistä metaperiaatteista on oikeus tietoturvaan, joka korostaa samalla oikeutta tietoon (käytettävyys) ja tämän tiedon eheyttä. Lisäksi oikeus tietoturvaan painottaa "ei-oikeutta tietoon" -ulottuvuutta eli tiedon luottamuksellisuutta. Oikeus tietoturvaan metaperiaatteena on oleellinen osa tietoturvan sääntelyjärjestelmää. Metaperiaatteet oikeusjärjestyksen ydinarvoina ovat ihmis- ja perusoikeuksien taustalla olevia oikeuksia oikeuksista ja ne voivat olla linkittyneitä muiden tärkeiden metaperiaatteiden kanssa. Oikeusperiaatteet ovat puolestaan metaperiaatteille alisteisia ja ikään kuin täydentävät niitä, jolloin oikeus kyberturvaan voisi olla myös korostettava, nykyaikainen oikeusperiaate verkkoyhteiskunnassamme.

2.4.2 Muut tietoturvalainsäädäntöön liittyvät keskeiset periaatteet

Oikeus tietoturvaan -metaperiaatteen lisäksi Saarenpään jaottelun mukaisia keskeisiä oikeusperiaatteita tietoturvan sääntelyjärjestelmässä ovat henkilötietojen suoja sekä teknologianeutraalisuuden periaate.

Yksityisyyden ja henkilötietojen suojan suhdetta on käsitelty myös muualla tässä tutkimuksessa[282]. Henkilötietojen suojaamisen on todettu olevan osa henkilön yksityisyyden suojaa, jota toteutetaan tietosuojalainsäädännön avulla.

[279] Esimerkiksi paperisen tiedon käsittelyn, tiedon luokittelun tai puhutun tiedon suojaamisen toimitilaratkaisuilla.
[280] Ks. kyberturvallisuusasetus, jonka määritelmän mukaan kyberuhkalla tarkoitetaan potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä verkko- ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä sekä muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti.
[281] Myös EU:n kyberturvallisuusasetuksessa (kohta 1) on korostettu, että verkko- ja tietojärjestelmillä sekä sähköisen viestinnän verkoilla ja palveluilla on yhteiskunnassa elintärkeä rooli ja järjestelmien käyttö on levinnyt laajalle kansalaisten ja organisaatioiden piirissä kaikkialla unionissa.
[282] Esimerkiksi perusoikeuksia käsittelevässä luvussa 2.5.3 (”Yksityisyys: yksityiselämän, henkilötietojen ja viestin suoja”). Ks. lisää käsitteen sisältömäärittelystä luvussa 2.2.2 (”Tietosuoja”).

Oikeusperiaatteena henkilötietojen suoja kuitenkin nähdään yksityisyydestä erillisenä uutena oikeusperiaatteena, sillä esimerkiksi Euroopan perusoikeuskirjassa nämä ovat erotettu toisistaan[283]. Henkilötietojen suoja on myös eriytynyt eurooppalaisella perusoikeustasolla omaksi perusoikeudekseen[284]. Tietosuojalla tarkoitetaan henkilötietojen käsittelyn laillisia edellytyksiä ja toimintaa, jossa kunnioitetaan henkilön perusoikeuksia ja yksityiselämää. Perusoikeustasolla tietosuoja linkittyy suoraan tiedollisen itsemääräämisoikeuden oikeusperiaatteeseen[285]. Tietosuojan voidaan katsoa olevan ihmisen ”tiedollisen kotirauhan” kunnioittamista. Se on perustuslaillinen oikeus, joka takaa jokaisen oikeuden elää elämäänsä niin kuin tahtoo kenenkään puuttumatta siihen.[286] Oikeus tietosuojaan voidaan hyvin nostaa myös nykyaikaiseksi periaatteeksi, sillä se sisältää luottamuksellisen viestinnän suojan eli viestintäsalaisuuden periaatteen, sekä se toteutuu myös muiden yksityisyyden suojaan kuuluvien oikeuksien kautta[287].

Tämän tutkimuksen kannalta tärkeä periaate on myös teknologianeutraalisuuden periaate, joka vaikuttaa lakien säätämisen taustalla. Lainvalmistelun osalta Suomessa on syntynyt vakiintunut käytäntö, jossa pyritään teknologianeutraalisuuteen eli lainsäätäjä pyrkii sääntelemään ensisijaisesti tekoja teknologian sijaan. Näin ollen säädöksissä ei yleensä ole tietoteknisiä ilmaisuja. Lainsäädännössä ei myöskään säännellä yksittäisen teknologisen ilmiön hyödyntämisestä taikka kielletä tai puolleta jonkin kilpailevan tekniikan käyttöä. Lainsäädännön teknologianeutraalisuudella on pyritty hillitsemään nykyisten säännösten muutostarpeita ja uusien säännösten säätämistarvetta sekä välttämään uusien asioiden ja niiden merkitysten ymmärtämättömyydestä johtuvia sääntelyn epäonnistumisia. Lisäksi yksilön oikeuksien näkökulmasta teknologianeutraalisuus merkitsee sitä, että ilman perusoikeuksiin liittyvää hyväksyttävää perustelua toista teknologista ratkaisua ei ole lupa asettaa toisen teknologisen ratkaisun edelle.[288] Sama ajatus oli lainsäätäjällä taustalla esimerkiksi EU:n yleistä tietosuoja-asetusta säätäessä.

Teknologianeutraalisuuden periaatetta on kuitenkin usein kritisoitu muun muassa sen takia, että se jättää monesti tietyt lainsäädännön velvoitteet hyvinkin tulkinnanvaraisiksi, löyhiksi ja tehottomiksi. Tämä voi johtua myös lainsäätäjän huonosta tietotekniikan tuntemuksesta. Tietotekniikan tuntemus ja tietty tietotekniikkasidonnaisuus ovat kuitenkin informaatio-oikeudessa välttämättömiä[289]. Asia ei tietenkään ole niin mustavalkoinen ja tähänkin toki liittyy poikkeuksia.

---

[283] Saarenpää 2016a: 219.
[284] Saarenpää 2015: 230–232; Pöysti 1999: 483.
[285] Voutilainen 2012: 33–35; Voutilainen 2019: 33.
[286] Andreasson, Koivisto & Ylipartanen 2013: 14.
[287] Neuvonen 2019: 47.
[288] Saarenpää 2005: 93; Saarenpää 2016a: 92–93, 223; Pöysti 1999: 373–375.
[289] Pöysti 1999: 374.

Esimerkiksi hallinnollisen tietoturvan osa-alueella on hyvinkin mahdollista säätää velvoitteita organisaatioille teknologianeutraalisti vailla sen suurempaa tietotekniikkatuntemusta ja tietotekniikkasidonnaisuutta. Sen sijaan, jos esimerkiksi säädetään velvollisuudesta estää luvaton pääsy salassa pidettäviin tietoihin, tulisi tietää sen hetken erilaisista teknisistä vaihtoehdoista.

Teknologianeutraalin lain säätämisen osalta on kolme tavoitetta. Kestävyystavoitteen (sustainability) mukaan lainsäädäntö on joustavaa, mahdollisimman immuunia teknologiselle kehitykselle eikä vaadi jatkuvaa päivittämistä. Kompensaatiotavoitteen (compensation) mukaisesti teknologiaa koskeva erityissääntely nähdään kuitenkin mahdollisena, mikäli lain neutraalius sekä lain suojan taso ja tehokkuus säilytetään suhteessa uusiin teknologioihin. Kolmantena tavoitteena on innovaatioiden edistäminen (innovation), jonka pyrkimyksenä on välttää kilpailun vääristämistä tekniikan tai jonkin ilmiön erityiskohtelulla. On myös kritisoitu, että tosiasiassa laki itsessään ei ole ikinä teknologianeutraalia, vaikka sille olisi asetettu teknologianeutraalisuuden vaatimus. Tämä kritiikki on kohdistunut esimerkiksi tietosuoja-asetuksen sisäänrakennetun tietosuojan periaatteeseen (*”Data Protection by Design”* tai *”Privacy by Design”*), jossa tietosuojavaatimukset tulisi huomioida jo teknisesti järjestelmän suunnittelutasolta lähtien. Myös tietosuojatyöryhmä on todennut tämän asian osalta, että tarpeen tullen erityisiä teknisiä olosuhteita kuvaavia säännöksiä tulisi omaksua.[290] Asia on monimutkainen, sillä tietosuoja-asetus teknologianeutraalina lainsäädäntönä on varsin ajaton, eikä se suosi tiettyjä tekniikoita. Kuitenkin esimerkiksi sisäänrakennettua tietosuojaa koskevassa velvoitteessa pitäisi huomioida henkilötietojen suojaaminen jo järjestelmän kehitysvaiheessa, ja teknisissä ja organisatorisissa toimenpiteissä tulisi varmistaa riskiperusteisesti kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus. Kyseinen lausuma ei ole myöskään täysin ”teknologiavapaa” ilmaisultaan. Kuitenkin tässäkin kohtaa lainsäätäjä on säännellyt ensisijaisesti tekoa eikä tiettyä teknologiaa, joka tulisi huomioida järjestelmän suunnitteluvaiheessa, jonka vuoksi edellä mainittu velvoite on silti teknologianeutraali sen oikeusperiaateajattelun lähtökohdilta.

Teknologianeutraalisuuden periaate ei ole ainoastaan tietoteknisten termien välttämistä lakitekstissä. Tapauskohtaisesti joissain tilanteissa tiettyä teknologiaa koskeva erityissääntely voi olla tarpeen, jotta lain tarjoaman suojan taso ja tehokkuus säilyvät suhteessa uusiin teknologioihin. Liian yleisluontoiselle tasolle jäädessään teknologianeutraali sääntely voi olla vaikeaselkoista sekä johtaa

[290] Riekkinen 2019: 5; Hildebrandt & Tielemans 2013: 509–511, 516–517; Euroopan WP29-tietosuojatyöryhmä WP168: *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, s. 3.

oikeustilan epävarmuuteen suhteessa uusiin teknologioihin. Se voi myös heikentää pykälän ennakoitavuutta ja tehdä sen sisällöstä epäselvän tai epätäsmällisen. Tämä voi pahimmillaan johtaa siihen, että haitallinen toiminta jää rankaisematta. Toiseksi joissain yhteyksissä samojen sääntöjen noudattaminen erilaisissa teknologisissa konteksteissa voi johtaa vaikeasti perusteltaviin johtopäätöksiin. Näin ollen toisinaan voi olla tarpeen säätää teknologiasidonnaisia erityissäännöksiä, jotta sääntelyn vaikutukset olisivat lopputulokseltaan neutraaleja.[291]

Yhteenvetona voidaan todeta, että henkilötietojen suoja ja teknologianeutraalisuus ovat oikeusperiaatteina tärkeä osa tietoturvallisuuden sääntelyjärjestelmää. Tietoturvan sääntelyjärjestelmän on otettava huomioon yksilöt ja heidän perusoikeutensa, kuten esimerkiksi yksityiselämän suoja, henkilötietojen suoja (tietosuoja) sekä luottamuksellisen viestinnän suoja. Näiden seikkojen lisäksi tietoturvan sääntelyjärjestelmän on huomioitava teknologia. Teknologianeutraalisuuden periaate auttaa lainsäädäntöä pysymään paremmin ajan tasalla ja proaktiivisena, mikä edellyttää sääntelyn ja teknologian yhteensovittamista teknologianeutraalisti niin, että se pysyy ymmärrettävänä ja johdonmukaisena.

2.5 Tietoturva perusoikeutena osana tietoturvan sääntelyjärjestelmää

2.5.1 Ihmis- ja perusoikeuksien merkitys nyky-yhteiskunnassa

Tietoturvan sääntelyjärjestelmässä heijastuvien meta- ja oikeusperiaatteiden käsittelyn jälkeen tarkoituksena on tarkastella, millainen merkitys ihmis- ja perusoikeuksilla on tietoturvan sääntelyjärjestelmässä tietojen turvaamisen kannalta nyky-yhteiskunnassa.

Ihmisoikeudet ovat alueellisessa ja globaalissa kansainvälisoikeudellisessa sopimuksessa eli ihmisoikeussopimuksessa tunnistettuja oikeuksia, jotka samalla myös määrittelevät kansainvälisesti perusoikeuksille tavoitetason. Perusoikeudet ovat perustuslaissa turvattuja yksilöiden ja toisinaan ryhmien oikeuksia, jotka ovat yleisiä, yhdenvertaisesti kaikille kuuluvia, pysyviä sekä perustuvanlaatuisia, erityisen tärkeitä oikeuksia. Sisällöllisesti perus- ja ihmisoikeuksista on kuitenkin kysymys suurimmaksi osaksi samoista oikeuksista.[292] Ensimmäinen historiallinen merkkipaalu ihmisoikeuksien suhteen sijoittuu Yhdistyneiden kansakuntien (YK) yleiskokoukseen 10.12.1948, jossa hyväksyttiin ihmisoikeuksien kansainvälinen julistus. Tämän jälkeen on solmittu kansainvälisiä ihmisoikeussopimuksia, joista

[291] Saarenpää & Riekkinen 2023: 185; 253–254.
[292] Ojanen 2015: 8; Hallberg 2011: 29–30, 35.

tärkeimmät ovat kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen sopimus (KP-sopimus) sekä taloudellisia, sosiaalisia ja sivistyksellisiä oikeuksia koskeva kansainvälinen yleissopimus (TSS-sopimus). Näistä molemmat tulivat voimaan Suomessa sopimuksien kansainvälisen voimaantulon kanssa yhtä aikaa vuonna 1976. Kolmas merkittävä ihmisoikeussopimus on Euroopan neuvoston valmistelema Euroopan ihmisoikeussopimus (EIS), joka tuli kansainvälisesti voimaan jo vuonna 1953. Myös Euroopan unionin perusoikeuskirja on merkittävä perus- ja ihmisoikeusnormistojen välimaastoon sijoittuva instrumentti, josta tuli vuoden 2009 Lissabonin sopimuksen myötä sitovaa EU:n primäärioikeutta. Ihmisoikeussopimuksilla on suuri vaikutus kansalliseen perusoikeusjärjestelmään ja perusoikeuksien sisältöön.[293]

Yhteiskuntamme oikeudellistumisen ja oikeusvaltion vahvistumisen myötä lainsäädäntömme ytimenä on ollut ihmisarvon sekä ihmisoikeuksiin perustuvien perusoikeuksien tarkka kunnioittaminen. Myös tietojenkäsittelyyn, informaatioon ja viestintään liittyvä sääntely tapahtuu enenevissä määrin lähtökohtaisesti yksilön oikeuksien kannalta. Näin ollen oikeusvaltiomme sääntelyn lähtökohtina ovat ihmis- ja perusoikeudet, joista ihmisoikeudet välittyvät perusoikeuksiin ja perusoikeuksista on pääsääntöisesti säädettävä laissa.[294] Perusoikeudet kulkevat siten ihmisoikeuksien kanssa käsi kädessä.

Ihmis- ja perusoikeuksien merkitys on kasvanut nykyisessä verkottuneessa yhteiskunnassa, minkä vuoksi tietoverkkojen ja niiden palveluiden käyttäjien edut ja oikeudet ovat keskiössä[295]. Täten nykyisessä verkkoyhteiskunnassa lainsäädännön tulee olla lähtökohtaisesti suunniteltu niin, että se turvaa ja edistää perus- ja ihmisoikeuksien toteutumista[296]. Tämä koskee myös lainsäädännön tietoturvavaatimuksia, joilla velvoitetaan organisaatioita ylläpitämään tietynlaista tietoturvatasoa. Ollakseen hyvä, hyvän tietoturvan sääntelyjärjestelmän peruselementtinä tulee olla perusoikeuksien huomioiminen, jotta sääntelyjärjestelmän avulla mahdollistetaan henkilöiden oikeuksien turvaaminen.

Perusoikeuksien vaikutus voi tulla ilmi kahdella tapaa: a) vertikaalivaikutuksena eli julkisen vallan ja yksilön välisessä suhteessa ja b) horisontaalivaikutuksena eli

---

[293] Riekkinen 2019: 47–48.
Ihmisoikeusasiakirjojen alkuperäinen historia linkittyy niin sanottuun pehmeään sääntelyyn eli ne ovat olleet soft law'ta. Esimerkiksi YK:ssa 1948 hyväksytty ihmisoikeuksien kansainvälinen julistus ja vuonna 2000 juhlallisena julistuksena hyväksytty EU:n perusoikeuskirja saivat julistuksina suuren merkityksen. Myöhemmin ne johtivat oikeudellisesti sitoviin asiakirjoihin: Vuonna 1966 hyväksyttiin KP-sopimukset ja TSS-sopimukset, sekä vuonna 2009 EU:n perusoikeuskirjasta tuli oikeudellisesti sitova. Ks. Nieminen 2020, s. 1081–1082.
[294] Saarenpää 2016a: 80–81, 110.
[295] Saarenpää 2016a: 210.
[296] Riekkinen 2019: 45.

yksilöiden keskinäisissä suhteissa[297]. Perusoikeuksien soveltamisessa ja tulkinnassa keskeisin lähde on kansallinen perustuslaki (PL 731/1999), jonka jälkeen painoarvoa tulkinnassa saavat heikommin velvoittavat, lainsäätäjän tarkoitusta kuvaavat lain esityöt.

Suomen perustuslain alussa korostetaan kolmea valtiosääntömme taustalla olevaa arvoa, jotka ovat yksilön oikeuksien ja vapauden turvaaminen, oikeudenmukaisuuden edistäminen yhteiskunnassa sekä ihmisarvon loukkaamattomuus. Perusoikeudet ja valtiosääntö ovat osa järjestelmän runkoa, jossa muun muassa lakien säätäminen ja soveltaminen rakentuvat.[298] Valtiosääntömme arvoista etenkin yksilön oikeuksien ja vapauksien turvaaminen on olennaista myös tietoturvan näkökulmasta. Esimerkiksi henkilötietojen käsittelyyn liittyviä riskejä arvioidessa, tulee näitä riskejä arvioida luonnollisen henkilön oikeuksien ja vapauksien kannalta.

Perustuslain 2 luvun perusoikeudet on myös kirjattu Euroopan ihmisoikeussopimuksessa (EIS). Perustuslain säännökset jättävät paljon tulkinnanvaraa ja niillä on yhteys politiikan todellisuuteen sekä perimmäisiä yhteiskunnallisia arvoja koskevaan keskusteluun. Osa perusoikeuksista ovat sellaisia oikeuksia, joihin voi vedota suoraan tuomioistuimissa. Tähän liittyy perusoikeusmyönteisyys, jossa perusoikeuksien soveltaminen saa painoarvoa laintulkinnassa.[299] Tämä tulee ilmi perustuslain 106 ja 107 §:ssä. Perustuslain 106 §:n mukaan perustuslain säännökselle on annettava etusija, mikäli toisen lain säännöksen soveltaminen olisi ilmeisessä ristiriidassa perustuslain kanssa. Perustuslain 107 §:n mukaan, jos alemman asteinen säädös olisi ristiriidassa perustuslain tai muun lain kanssa, sitä ei saa soveltaa. Tällainen perusoikeusmyönteisyys korostaa perusoikeuksien arvopainotusta, mikä on yksi syy sille, miksi hyvä tietoturvan sääntelyjärjestelmä ottaa huomioon perusoikeudet.

Digitalisaation myötä eri toiminnot ovat siirtyneet tietoverkkoihin. Tämä siirtyminen koskee myös perusoikeuksiamme, mikä vaikeuttaa niiden merkityksen havaitsemista. Nykyisin yksilöiden oikeuksia pyritään vahvistamaan tietojärjestelmissä ja -verkoissa jo niiden suunnitteluvaiheessa.[300] Euroopan unionin kyberturvallisuusstrategian mukaan perusoikeuksia, oikeusvaltioperiaatetta ja demokratiaa on suojeltava myös kyberavaruudessa. Samat lait ja normit, jotka sääntelevät päivittäistä elämäämme, koskevat myös verkkoympäristöä. Yksityishenkilöiden perusoikeuksia ei voida varmistaa ilman turvallisia verkkoja ja järjestelmiä. Toisaalta kaikille tulisi myös taata pääsy internettiin, sillä rajoitettu pääsy tai sen puuttuminen sekä digitaalinen lukutaidottomuus asettavat kansalaiset eriarvoiseen

[297] Nyyssölä 2018: 26.
[298] Hallberg 2011: 29.
[299] Kemppinen 2011: 43–45; Jyränki 1997: 74–75.
[300] Saarenpää 2002: 62; Saarenpää 2016a: 81.

asemaan.[301] Myös internetin hyödyntämiseen tarvittava laitteisto ja käyttötaito sekä niistä aiheutuvat kulut asettavat yksilöt eriarvoiseen asemaan ja siten estävät tehokkaan oikeuksien toteuttamisen[302]. Toisaalta voidaan pohtia, voisiko internettiin pääsy olla erillinen perusoikeus, koska sen avulla edesautetaan monien muiden perusoikeuksien toteutumista[303]. Myös kyberturvallisuuden kannalta on todettu, että siinä yhdistyy kysymys sekä inhimillisestä turvallisuudesta että ihmisoikeuksista. Näin ollen kyberturvallisuus voitaisiin mahdollisesti julistaa ihmisoikeudeksi.[304] Perusoikeuksien suojelu voidaan taata täysimääräisesti vain tarjoamalla oikeudenmukainen, turvallinen ja avoin digitaalinen ympäristö, jossa minimoidaan digitaalisen ympäristön riskit ja uhat[305]. Tästä näkökulmasta myös oikeus kyberturvaan voisi olla korostettava ulottuvuus osana perusoikeuksia yhteiskunnan digitalisoituessa ja riippuvuutemme kasvaessa tietoverkoista ja järjestelmistä.

Saarenpää on sitä mieltä, että EU-sääntelyn ei ole nähty poistavan tarvetta täydentää perustuslakia tietoturvasäännöksellä. Yksilöillä tulee olla oikeus turvallisuuden lisäksi tietoturvaan.[306] Riittävä tietoturvallisuus ja yleensä infrastruktuurin asianmukainen laatu ja turvallisuus ovat välttämättömiä edellytyksiä useiden perusoikeuksien toteutumiselle *verkkoyhteiskunnassa*[307]. Tietoturvallisuutta tarvitaan yhteiskunnan toimimiseksi sekä oikeushenkilöiden toiminnan ja yksilöiden oikeuksien turvaamiseksi[308].

Yhteenvetona korostettakoon, että ihmis- ja perusoikeuksien merkitys kasvaa verkkoyhteiskuntamme muuttuessa. Ihmis- ja perusoikeudet toimivat sääntelymme lähtökohtina, ja perusoikeuksista säädetään kansallisesti Suomen perustuslaissa. Perusoikeudet saavat painoarvoa laintulkinnassa ja niitä sovelletaan suoraan, mikä myös korostaa niiden merkitystä. Hyvä tietoturvan

---

[301] Euroopan unionin kyberturvallisuusstrategia 2013: 2, 4. Kyberturvallisuus on tärkeä ihmisten luottamuksen, mutta myös perusoikeuksien ja -vapauksien suojelemisen kannalta. Ks. myös Euroopan unionin kyberturvallisuusstrategia 2020, s. 4.
[302] Koulu 2012: 299.
[303] Ibid.: 286–287, 291. Pääsy internetiin saa merkitystä osana perus- ja ihmisoikeuksien toteuttamista. Huomioitava on se, ettei internetin merkitys pelkisty minkään yksittäisen perusoikeuden alle, vaikka esimerkiksi sananvapaus on usein keskeisessä osassa internetiin pääsyn perusoikeusluonnetta. (Koulu 2012, s. 292)
[304] Salminen 2022: 45.
[305] Euroopan unionin neuvosto, Council conclusions on digital empowerment to protect and enforce fundamental rights in the digital age 20.10.2023: 11.
[306] Saarenpää 2016a: 123, 218; Saarenpää & Riekkinen 2023: 177, 204.
[307] Pöysti 2000: 97.
[308] Myös esimerkiksi Pöystin (2000, s. 93) mukaan verkkoyhteiskunnalle ominainen globalisaatio ja uudet verkostot koettelevat myös yksilön turvallisuuden tunnetta ja identiteettiä. Osa identiteettiä ja oikeustoimikelpoisuuden käyttämisen välineistöä verkkoyhteiskunnassa on sähköinen identiteetti, kun taas yksi olennainen yksilön turvallisuuden elementti on tietoturvallisuus. Tietoturva onkin eräs verkkoyhteiskunnan tärkeä pilari.

sääntelyjärjestelmä huomioi perusoikeudet ja siten mahdollistaa yksilöiden oikeuksien turvaamisen tehokkaasti. Digitalisaation myötä yksilöiden oikeudet ovat entistä enemmän siirtyneet tietoverkkoihin, ja riippuvuutemme tietojärjestelmistä on sitä myöten kasvanut. Perusoikeuksien toteutumista ei pystytä takaamaan ilman toimivia verkkoja ja järjestelmiä, mikä puolestaan korostaa erityisesti kyberturvallisuuden merkitystä. Näin ollen perustuslaissa tulisi huomioida kyberturvallisuuden merkitys paremmin. Suomen kansallisessa perustuslaissa ei kuitenkaan ole suoranaisesti viittauksia tieto- tai kyberturvallisuuteen eikä kansallisessa lainsäädännössämme ole suoranaisesti säädetty yksilöiden oikeudesta tietoturvaan. Perustuslaista voi kuitenkin johtaa monesta kohtaa tämän oikeuden. Näistä tärkeimmät kohdat on koottu seuraaviin alalukuihin.

2.5.2 Oikeus turvallisuuteen ja omaisuuden suojaan

Perustuslain 7 §:*n mukaan jokaisella on oikeus henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen*. Säännös koskee fyysistä vapautta ja turvallisuutta, jolloin esimerkiksi turvakieltoasiakkaan yhteystietojen paljastuminen väärälle henkilölle saattaisi aiheuttaa fyysisen vaaran tietojen kohteelle[309]. Toisaalta fyysisen vapauden ja turvallisuuden henkilökohtaisen koskemattomuuden suoja kattaa myös merkittävän puuttumisen yksilön henkiseen koskemattomuuteen silloinkin, kun tällaista puuttumista ei voida katsoa samassa pykälässä kielletyksi ihmisarvon vastaiseksi kohteluksi[310]. Tietojen turvaaminen ja henkilötietojen suoja on tästäkin näkökulmasta erityisen tärkeää, jolloin oikeus tietoturvaan keskeisenä metaperiaatteena heijastuu säännöksestä.

Perustuslakivaliokunta on todennut, että perustuslain 7 §:n turvallisuusaspektissa tulee ottaa huomioon tietoturvallisuus. Tämä johtuu lähinnä siitä, että tietoturvallisuuden vaarantuminen voidaan nykyaikana pitää riskinä yksilön ja yhteiskunnan laajasti ymmärretyn turvallisuuden kannalta.[311] Tietoturvallisuus osana perustuslain 7 §:n 1 momenttia on yhdistelmä tiedollista koskemattomuutta, itsemääräämisoikeutta ja yksityisyyden suojaa[312]. Nämä seikat ovat edelleen paikkaansa pitäviä, mutta nykyaikana tulee huomioida erityisesti kyberturvallisuuden merkitys osana perustuslain 7 §:n turvallisuusulottuvuutta. Esimerkiksi järjestelmäriippuvaisen, verkottuneen yhteiskuntamme digitalisoituessa peruspalvelut siirtyvät internettiin, joka johtaa puolestaan siihen, että yksityiset tietomme ja varallisuutemme sähköistyvät ja tietomme turvallisuus on monen tekijän varassa. Sellaiset kyberrikokset, joissa rikollinen tunkeutuu esimerkiksi yksityisille laitteille ja

[309] Voutilainen 2012: 121.
[310] Lohse 2005: 1190; HE 309/1993 vp: 46.
[311] PeVL 9/2004 vp: 4; Alavesa 2016: 238.
[312] Råman 2006a: 822.

varastaa sekä yksilöiden omaisuutta että yksityisiä tietoja, järisyttävät yksilöiden turvallisuuden tunnetta. Kyberrikokset eivät kuitenkaan ainoastaan riskeeraa yksilöiden yksityiselämän, henkilötietojen ja luottamuksellisen viestinnän suojaa, vaan myös muita perusoikeuksia. Jotkin toimijat pyrkivät nimenomaan lamauttamaan yhteiskuntaa kybertoimillaan, jolloin yksilöiden turvallisuus ja terveys voivat konkreettisesti vaarantua.

Perustuslain 7 §:n oikeus turvallisuuteen saa käytännössä lisävahvistusta perustuslain 22 §:ssä säädetystä julkisen vallan velvollisuudesta turvata perus- ja ihmisoikeuksia. Useimmat perusoikeuskollisiot[313] turvallisuusvalvonnassa rajoittavat juuri muun muassa perustuslain 10 §:ssä ja 12 §:ssä säädettyä yksityiselämän suojaa ja sananvapautta vetoamalla perustuslain 7 §:n oikeuteen turvallisuuteen.[314] Perustuslain 7 §:n turvaamilla oikeuksilla on vahva painoarvo perusoikeuksien välisissä punnintatilanteissa. Lisäksi muiden perusoikeuksien rajoitukset ovat helpommin hyväksyttävissä, mikäli niiden tarkoituksena on turvata perustuslain 7 §:n oikeuksia.[315] Turvallisuus voidaan tulkita vapaudelle rajoituksia luovaksi tavoitteeksi, mutta myös rajoituksien sijaan vapauden edellytyksenä. Perusoikeustulkinnassa yksilöllinen ja kollektiivinen turvallisuus voivat toimia yhtäaikaisesti sekä yksilön oikeutena että yksilön oikeuksien rajoitusperusteena.[316]

Käytännön työssä tämä ilmenee esimerkiksi usein organisaatioissa tehtävässä järjestelmien ja laitteiden valvonnassa. Kyberturvapalveluissa pyritään erilaisilla automaattisilla työkaluilla tunnistamaan anomalioita ja ennalta ehkäisemään proaktiivisesti uhkia sekä havaitsemaan tietoturvaloukkauksia. Yhtä lailla tällaisissa palveluissa tulee huomioida yksilöiden perusoikeudet luottamuksellisen viestinnän ja henkilötietojensa suojan osalta. Tietosuojaihmiset korostavat toistuvasti luottamuksellisen viestinnän ja henkilötietojen käsittelyn minimoinnin tärkeyttä, mutta nämä automatisoidut järjestelmät vaativat yhtäaikaisesti ”polttoainetta” esimerkiksi viestien välitystiedoista toimiakseen oikein, havaitakseen poikkeamia ja turvatakseen organisaation kybertoimintaympäristön. Asia vaatii arkisessa työssä tasapainottelua ja punnintaa. Loppujen lopuksi tietosuojaihmisillä on vahvemmin lainsäädäntöä heidän perusteluidensa takana, koska he voivat suoraan vedota perustuslakiin tietosuojalainsäädännön ja sähköisen viestinnän palveluista annetun lain lisäksi. Kuitenkin organisaation kybertoimintaympäristön turvaaminen heijastuu vahvasti yhteiskunnan (kyber)turvallisuuden vahvistamiseen, sillä

[313] Tilanteita, joissa perusoikeudet ovat vastakkaisia ja tapaukseen soveltuu useampi perusoikeus, kutsutaan perusoikeuskollisioksi. Tällöin pyritään ratkaisuun, jossa perusoikeuksia punnitaan niin, että molempia voidaan toteuttaa täysmääräisesti. Perusoikeuskonkurrenssista on kyse, kun useampi perusoikeus soveltuu samaan tapaukseen ja toteuttavat samaa tarkoitusta. Ks. Neuvonen 2014, s. 34.
[314] Saraviita 2011: 158–159.
[315] Pellonpää 2011: 282.
[316] Widlund 2020: 134–135, 137; Tuori 1999a: 920–923.

organisaatiot ja yksilöt ovat monin tavoin linkittyneitä toisiinsa verkottuneessa yhteiskunnassa. Tämä ei ilmene selkeästi nykyisestä perustuslaistamme.

Yksilöiden oikeus tieto- tai kyberturvaan konkreettisesti osana perustuslain 7 §:ää korostaisi paremmin ja laajemmin yksilöiden oikeutta turvallisiin verkkojen ja järjestelmien varassa toimiviin palveluihin, mutta se korostaisi myös yksilöiden turvallisuutta osana yhteiskunnan kybertoimintaympäristön turvaamista. Se ei kuitenkaan jyräisi perustuslain 10 §:n oikeuksia yksityiselämään, henkilötietojen suojaan ja luottamuksellisen viestin suojaan, vaan selkeyttäisi tieto- ja kyberturvallisuuden merkitystä yhteiskunnassa. Näin otettaisiin huomioon entistä laajemmin ja paremmin palveluiden käyttäjien oikeuksien suojaaminen, mikä sisältäisi luottamuksellisen viestinnän ja henkilötietojen suojan ulottuvuuksien ohella muut oikeudet ja vapaudet. Kyber- ja tietoturvallisuus ovat tekijöitä, jotka pitävät yllä yksilöiden henkistä, kognitiivista ja jopa fyysistä koskemattomuutta ja ihmisarvoa, jotta yksilöt voivat tehdä tietoon perustuvia valintoja[317]. On huomioitava, että vakava tietoturvaloukkaus kybertoimintaympäristössä voi toteutuessaan aiheuttaa luonnollisille henkilöille laajaakin kärsimystä, mainehaittaa, terveydellisiä ongelmia ja varallisuuden menetystä.

Perustuslain 7 §:n tiedollisen koskemattomuuden sekä turvallisuuden oikeuksien lisäksi on huomioitava ***perustuslain 15 §****, jonka mukaan jokaisen omaisuus on turvattu.* Omaisuudensuojasäännös suojaa lähtökohtaisesti yksilöitä turvaamalla ja edistämällä muun muassa itsemääräämisoikeutta ja taloudellista vapautta sekä suojaamalla yksilöiden odotuksia ja oikeuksia varallisuusoikeuksien riittävästä pysyvyydestä ja ennakoitavuudesta. Omaisuuden perustuslaillinen suoja kattaa lähtökohtaisesti kaikki omistajan oikeusasemaan liittyvät oikeudet, kuten omistajan vapauden käyttää ja hyödyntää omaisuuttaan taikka sulkea ulkopuoliset pois sen käytöstä.[318] Kyseistä säännöstä voi soveltaa myös tietoturvaloukkauksiin. Mikäli omistusoikeuteen kuuluvia oikeuksia rajoitetaan tai vähennetään, puututaan samalla omaisuuteen, vaikka omistusoikeuden kohteena oleva esine säilyisi koskemattomana haltijallaan[319]. Esimerkiksi haittaohjelmien avulla tehdyissä tietoturvaloukkauksissa laite on fyysisesti henkilön hallussa ja omassa käytössä, mutta laitteen käyttäminen on kokonaan tai osittain mahdotonta taikka osa laitteen tärkeistä tiedostoista on haittaohjelmalla lukittuja. Tämän laatuiset kybertoimintaympäristön tietoturvaloukkaukset ulottuvat luonnollisten henkilöiden perusoikeuksien loukkaamiseen asti heikentämällä omaisuuden suojaa, joka tapahtuu rajoittamalla omistajan vapautta käyttää ja hyödyntää omaisuuttaan. Samaan aikaan tällainen omaisuuden suojan loukkaus voi heikentää myös luonnollisen henkilön

[317] Pöysti 2023: 50.
[318] Länsineva 2011: 557, 570.
[319] HE 309/1993 vp: 62.

henkistä turvallisuuden tunnetta. Kyberturvallisuudella parannetaan yksilöiden suojaa kybertoimintaympäristössä ja siten myös yksilöiden oikeutta omaisuuden suojaan.

Yhteenvetona voidaan todeta, että perustuslain 7 § ja 15 § ovat keskeisiä perusoikeuksia yksilöiden osalta kybertoimintaympäristössä. Osana perustuslain 7 §:n turvallisuusoikeutta on huomioitava yksilöiden oikeus tieto- ja kyberturvaan, jotta myös muita yksilöiden oikeuksia ja heikommassa asemassa olevia henkilöitä, kuten lapsia ja vanhuksia, on mahdollista suojata paremmin nykyisessä, järjestelmäriippuvaisessa verkkoyhteiskunnassa. Näin myös selkeytetään ja korostetaan tieto- ja kyberturvallisuuden merkitystä perustuslain 10 §:ssä suojattavien oikeuksien rinnalla. Kyberrikoksilla voidaan lamaannuttaa yhteiskuntaa ja vaarantaa siten yksilöiden turvallisuutta ja terveyttä. Vakavat kyberrikokset vaikuttavat yksilöiden turvallisuuden lisäksi turvallisuuden tunteeseen: henkilöiden yksityisten tietojen ja omaisuuden vaarantuessa kyberrikollinen astuu ikään kuin henkilön laitteen tai henkilön käyttämän palvelun kautta tämän yksityiseen elämään ja jopa kotiin. Tähän linkittyy myös oleellisesti perustuslain 15 §, jossa määritellyllä omaisuuden suojalla turvataan samalla yksilöiden oikeutta hyödyntää ja käyttää omistamiansa laitteita, tiedostoja sekä varallisuutta ilman, että ne joutuvat kyberrikollisten vahingoittamaksi tai haltuun. Kyberrikokset heikentävät sekä yksilöiden omaisuuden suojaa että henkistä turvallisuuden tunnetta kyberrikollisen tunkeutuessa henkilön yksityiselämän ja jopa kotirauhan piiriin. Samalla kyberrikoksilla voidaan heikentää yhteiskunnan eri toimintoja ja siten yksilöiden turvallisuutta, terveyttä ja muita oikeuksia. Näin ollen perustuslakia tulisi vahvistaa niin, että se huomioisi paremmin kyberturvallisuuden merkityksen.

2.5.3 Yksityisyys: yksityiselämän, henkilötietojen ja viestin suoja

Ennen digitalisoitumista yksityisyyden suoja oli pitkälti kotirauhan suojaa[320]. Nykyisessä digitaalisessa verkkoyhteiskunnassa ihmisten elämä on yhä enemmän siirtynyt verkkoon, mikä asettaa haasteita yksityisyydelle. Sähköisen viestinnän seuraamisen, yksilön paikantamisen sekä muun teknisen valvonnan myötä ulkoinen vapaus merkitsee nykyään myös yksilön oikeutta pysytellä teknisen valvonnan ulkopuolella[321]. Asia ei ole kuitenkaan niin mustavalkoinen, niin kuin edellisessä alaluvussa käsiteltyjen seikkojen perusteella voidaan havainnoida. Esimerkiksi valvontaa joudutaan usein tekemään osana turvallisten palveluiden toteuttamista. Yksityisyyden osalta keskeisiä vastaoikeuksia, joihin vedotaan, ovat useimmiten

[320] Lehtonen 2001: 281; Bruun 1984: 219–221.
[321] Saarenpää 2015: 219.

turvallisuus tai ilmaisunvapaus: kansalaisvapauksista ja -oikeuksista onkin tyypillisesti osittain luovuttu turvallisuutta vastaan[322].

Kaikki tärkeät yksityisyyden suojaan liittyvät lainsäädännön kehitykset ovat liittyneet teknologian kehittymiseen ja implementointiin, sillä ne ovat radikaalisti haastaneet olemassa olevat normatiiviset julkisuuden ja yksityisyyden konseptit[323]. Yksilöiden yksityisyyden suojaamiseen liittyy kolme ongelmaa, joista ensimmäinen liittyy eturistiriitoihin. Toinen ongelma liittyy puolestaan yksityisyyden suojan käsitteen epäselvyyteen ja kolmas tietotekniikan kehittymiseen.[324]

Yksityisyyden suoja käsitteenä on monitahoinen. Useimmiten yksityisyys käsitetään eri elämänalueilla erilaiseksi[325]. Esimerkiksi työelämässä korostetaan organisaation työntekijöiden yksityisyyttä niin, että henkilötietoja ei saa kerätä liian laajasti tai säilöä tarpeettomasti edes työntekijän suostumuksella[326], jolloin tällainen liiallinen työntekijöiden henkilötietojen käsittely katsotaan yksityisyyttä loukkaavaksi ja sopimattomaksi menettelyksi työntekijöiden ollessa heikommassa asemassa työnantajaan nähden. Vastakohtaisesti työntekijät voivat ladata todella valtavia määriä omia ja vaikkapa puolisonsa henkilötietoja (kuvia, videoita, syntymäaikoja ja niin edelleen) sosiaalisen median alustoille osana oman arjen sosiaalista jakamista ilman, että tätä toimintaa katsottaisiin suoraan sopimattomaksi tai yksityisyyttä loukkaavaksi[327].

Yksityisyyden määrittelemiseen käsitteenä vaikuttavat myös monet tekijät. Näitä tekijöitä voivat olla lainopilliset, sosiaaliset, historialliset, tekniset ja kulttuuriset tekijät. Näin ollen ei ole suotavaa yrittääkään muodostaa käsitteestä yksiselitteistä määritelmää. Useimmiten yksityisyyttä on kuitenkin ajateltu oikeudeksi olla yksin (*”The right to be left alone”*).[328] Suomalainen ja eurooppalainen yksityisyyskäsitys on laaja ja yksityisyyden sisältö muuttuu yhteiskunnan ja teknologian kehityksen rinnalla[329].

---

[322] Hildén 2019: 36.
[323] Hildén 2019: 9.
[324] Seipel 2001: 115.
[325] Lehtonen 2001: 192.
[326] Ks. Työelämän tietosuojalain 3 §:n tarpeellisuusvaatimus sekä ratkaisu TSV 5.7.2021, dnro. 3843/163/20.
[327] Huomioitava toki on, että puolisoltakin tai somesisällön muilta osapuolilta olisi hyvä kysyä lupa ennen tietojen julkaisua. Todellisuudessa tätä ei välttämättä tapahdu, eikä silloinkaan sitä pidetä välttämättä yksityisyyttä loukkaavana vaan ennemminkin huonona, epäkohteliaana käytöstapana. Esimerkiksi lapsien kuvien ja videoiden julkaisu vanhempien toimesta on todella yleistä ja ongelmallista lapsien yksityisyyden suojan kannalta, koska eritysesti pieniltä lapsilta ei ole mahdollista kysyä materiaalin julkaisuun tosiasiallista suostumusta.
[328] Wiatrowski 2016: 97–98.
[329] Riekkinen 2019: 54.

Yksityisyyteen liittyen on monia vaihtoehtoisia termejä. Esimerkiksi ***perustuslain 10 §:ssä*** käytetään yksityisyyteen viittaavana käsitteenä yksityiselämän suojaa, joka on eräänlainen yksityisyyden elementti. Yksityisyyttä ja yksityiselämän suojaa käytetään myös rinnasteisina käsitteinä. Muualla kansallisessa lainsäädännössä, esimerkiksi rikoslaissa ja laissa yksityisyyden suojasta työelämässä, yksityisyys on käytössä yleiskäsitteenä. Yksityisyyden keskeisimpiä ulottuvuuksia ovat:

a) yksityiselämän suoja;

b) henkilötietojen suoja; sekä

c) viestinnän luottamuksellisuus.

Näistä kolmesta henkilötietojen suoja on eurooppalaisella perusoikeustasolla eriytynyt omaksi perusoikeudekseen. EU:n yleisessä tietosuoja-asetuksessa yksityisyyttä ei edes mainita, kun taas esimerkiksi tietosuoja-asetuksella korvatun Euroopan henkilötietodirektiivin (1995/46/EY) yhtenä tavoitteena oli turvata direktiivin mukaisesti jäsenvaltioiden henkilötietojen käsittelyssä yksilöille heidän perusoikeutensa ja -vapautensa sekä erityisesti heidän oikeutensa yksityisyyteen.[330] Perustuslakivaliokunnan mukaan kuitenkin tietosuoja-asetuksen yksityiskohtainen sääntely, jota tulkitaan ja sovelletaan EU:n perusoikeuskirjassa turvattujen oikeuksien mukaisesti, muodostaa riittävän säännöspohjan myös perustuslain 10 §:ssä suojatun yksityiselämän ja henkilötietojen suojan osalta[331]. EU:n tietosuoja-asetuksen myötä henkilötietojen suoja vakiinnutti paikkaansa vahvemmin itsenäisenä oikeutena muiden perusoikeuksien joukossa, vaikka ennen sitä pidettiin enemmän yksityisyyden elementtinä[332].

Perustuslain 10 §:n mukaan *jokaisen yksityiselämä, kunnia ja kotirauha on turvattu*. Täten julkisen vallan tietoturvatoimenpiteet on järjestettävä tilannekohtaisesti riittävällä tasolla sekä turvata yhteiskunnan toimivuus tietoverkoissa ja julkisen hallinnon tietojenkäsittelyssä[333]. Tähän vaatimukseen liittyy läheisesti Euroopan ihmisoikeussopimuksen (EIS) yksityis- ja perhe-elämän, kodin ja kirjeenvaihdon suojaa antava 8 artikla, jonka myötä edellytetään sopimusvaltioita toteuttamaan positiivisia toimenpiteitä oikeuksien turvaamiseksi ulkopuolisilta loukkauksilta[334]. Lisäksi yksityiselämän loukkausten tulee niin ikään olla tehokkaan kriminalisoinnin ja vahingonkorvausvastuun piirissä[335]. Yksityiselämän suojaan kuuluu

330 Saarenpää 2015: 230–232; Pöysti 1999: 483.
331 Korpisaari, Pitkänen & Warma-Lehtinen 2022: 10–11; PeVL 14/2018 vp: 4.
332 Talus 2019: 222.
333 Voutilainen 2012: 120–121.
334 Viljanen 2011: 410.
335 Lehtonen 2001: 192; Perusoikeuskomitea 1992: 299.

rajoitettu ja suojattu kommunikointi yksityiselämään kuuluvissa asioissa, kuten mahdollisuus vaihtaa tietoja luottamuksellisesti[336].

Perustuslain asettaman yksityiselämän, kunnian ja kotirauhan turvaamisen lisäksi säännöksen lopussa on lisäys, jonka mukaan *henkilötietojen suojasta säädetään tarkemmin lailla*. Tässäkin yksityisyyteen liittyvä yksityiselämän suoja on erotettu henkilötietojen suojan osa-alueesta.

Käytännössä yllä mainittu perusoikeussäännöksen lisäys tarkoittaa, että henkilötietojen käsittelylle on oltava laissa säädetty perusteensa. Suomessa henkilötietojen suojaa koskevia säännöksiä on paljon, laskelmien mukaan jopa 800 eri säädöksessä[337]. Meillä on tiedollinen itsemääräämisoikeus henkilötietojemme osalta eli luonnollisella henkilöllä tulisi olla mahdollisimman suuri mahdollisuus vaikuttaa, miten, missä ja kenen toimesta hänen henkilötietojaan käsitellään. Itsemääräämisoikeutta ei tule kuitenkaan rinnastaa yksilön tietojen omistajuuteen. Tämä johtuu siitä, että henkilötietojen suoja on osa yksityisyyden suojan ihmis- ja perusoikeutta, jonka luovuttaminen ei ole mahdollista. Henkilötietojamme tarvitaan erityisesti hyvinvointivaltion palveluiden tarjoamiseen, väestön hallinnointiin ja kaupankäyntiin. Henkilötietomme ovat myös markkinoiden raaka-ainetta, sillä markkinat toimivat suurilta osin henkilötietojemme avulla. Palveluiden käyttäminen, yhteiskunnan toimien tehostaminen sekä markkinoiden tehokas toiminta edellyttävät, että luonnollinen henkilö luopuu osittain yksityisyydestään. Näin ollen itsemääräämisoikeuttamme on rajoitettu ja tietojamme voidaan käsitellä julkisen vallan tai yksityisten yhteisöjen toimesta lailla säädetyin tarkoituksin vastoin suostumustamme ja ilman oikeutta korvaukseen.[338]

Henkilötietojen käsittelyyn ja itsemääräämisoikeuteen liittyy kuitenkin usein intressipunnintaa, kuten esimerkiksi tapauksessa **KHO 2018:112**, jossa oli kysymys perusoikeuksien välisestä punninnasta.

> *Tietosuojavaltuutettu oli määrännyt poistettavaksi kaksi URL-osoitetta Google Search -hakupalvelusta silloin, kun haku tehtiin erään henkilön nimellä, koska hakutulokset olivat tarpeettomia henkilötietoja rekisterinpitäjän suorittaman henkilötietojen käsittelyn tarkoituksen kannalta. Henkilötiedot kuvasivat henkilön tekemää henkirikosta, vankeusrangaistusta ja hänen terveystietojaan. Google-hakutoiminto oli kuitenkin mahdollisuus suorittaa muilla hakusanoilla kuin hakijan nimellä. Asian ratkaisussa käytettiin EU-tuomioistuimen tuomiossa C-131/12 tarkoitettua intressipunnintaa, jonka pohjalta tietosuojavaltuutettu ja hallinto-oikeus*

[336] Pesonen 2017: 47.
[337] Voutilainen 2019: 88; Oikeusministeriön julkaisu 8/2018: 27–28.
[338] Saarenpää 2002: 51–52; Neuvonen 2014: 59–60, 68.

> *katsoivat hakijan oikeuden yksityiselämän suojaan olevan intressipunninnassa painavampi peruste kuin internetin käyttäjien oikeus saada tietoa hakijan nimellä hänen terveystiedoistansa.*[339] *EU-tuomioistuimen ratkaisussa C-131/12 on katsottu, että rekisteröidyn oikeudet syrjäytyvät lähtökohtaisesti suurella yleisöllä olevan intressin saada rekisteröidyn henkilötietoja hänen nimellään tehtävän haun perusteella. Näiden oikeuksien ja intressien välillä on kuitenkin pyrittävä löytämään oikeudenmukainen tasapaino. Hakijalla katsottiin olevan henkirikoksen tekemisen vuoksi tuomiossa C-131/12 tarkoitettu yksityiselämän ja sananvapauden välisen intressipunninnan kannalta merkityksellinen asema julkisuudessa. Toisaalta intressipunninnassa oli otettava huomioon, että tapauksessa oli kyse arkaluontoisista, erityisistä henkilötiedoista. KHO katsoi, että hallinto-oikeuden päätöstä ei muuteta. KHO:n mukaan yleisön intressi saada hakijan arkaluonteisia terveystietoja ei syrjäytä hänen oikeuttaan yksityiselämän ja henkilötietojen suojaan, joten täten hakutulosten katsottiin olevan henkilötietojen käsittelyn tarkoituksen kannalta tarpeettomia.*

Kyseisessä tapauksessa korostuu perusoikeuskollisio ja perusoikeuksien välinen punninta, jonka kohteena on yksityiselämän suoja ja sananvapaus[340]. Samanaikaisesti luonnollisen henkilön itsemääräämisoikeus omien henkilötietojensa kannalta korostuu, vaikkakin kyseessä on yhteiskuntaa kohahduttanut murha ja siten KHO:n mukaisesti intressipunninnan kannalta ”merkityksellinen asema julkisuudessa”. Perusoikeuspunninnan osalta yksityiselämän suojaa koskeva perustuslain 10§:n sääntely perustelee julkisuuden suppeamman ulottuvuuden[341]. Punninnan kannalta tapauksessa oli myös merkityksellistä, että hakutuloksissa tarkoitetut verkkosivut olivat löydettävissä hakukoneen avulla muutoinkin kuin hakijan nimellä tehtävän haun perusteella[342].

Yksityisyyden suojaa koskeva perusoikeus kattaa myös oikeuden tulla unohdetuksi, jolla on luonnollisesti yhtymäkohta internetin kehitykseen ja sen sisältämään valtavaan tietomäärään[343]. Käsitellyssä tapauksessa **KHO 2018:112** oikeus tulla unohdetuksi tietoverkossa oli näin ollen mahdollista, koska yleisön intressi saada tietoonsa arkaluontoisia, erityisiä henkilötietoja ei syrjäyttänyt rikollisen oikeutta yksityiselämän ja henkilötietojen suojaan[344]. KHO:n oikeustapauksen lopputulokseen vaikutti muun muassa se, että tiedot henkilön terveyden- ja

339 Helsingin HAO 8.12.2016 16/1028/5.
340 Mäenpää 2019: 465.
341 Kulla & Salminen 2021: 517.
342 Voutilainen 2020: 100–101; Voutilainen 2023: 117.
343 Melander 2019: 963.
344 Voutilainen 2019: 111.

mielentilasta olivat tietosuojavaltuutetun asiaa koskevan päätöksen antamisajankohtana voimassa olleen henkilötietolain (523/1999) 11 §:ssä tarkoitettuja arkaluonteisia henkilötietoja, jotka olivat myös yksityisyyden suojan ydinalueelle kuuluvia tietoja. Näin ollen rikosasioihin liittyvät henkilön terveydentilaa kuuluvat tiedot saattavat olla merkityksellisiä unohdetuksi tulemista koskevan oikeuden kannalta, vaikka tällaisilla tiedoilla olisi keskeinenkin merkitys itse rikosteon rikosoikeudellisen arvioinnin kannalta.[345] Arkaluontoisten, erityisten henkilötietojen käsittelyllä on pääsääntöisesti suurempi vaikutus henkilön yksityiselämään, minkä vuoksi perusoikeuksien välisessä punninnassa ne saavat erityispainoarvoa.

Henkilötietojen suojaa toteutetaan tietosuojalainsäädännöllä, joista esimerkkeinä ovat Euroopan unionin yleinen tietosuoja-asetus (GDPR) ja kansallinen tietosuojalaki. Tietosuojalla tarkoitetaan tässä henkilötietojen käsittelyn laillisia edellytyksiä ja toimintaa, jossa kunnioitetaan henkilön perusoikeuksia ja yksityiselämää. Yksityisyyden suojan käsite ei ole tässäkään ulottuvuudessa ehdoton, sillä se on riippuvainen muun muassa henkilötietojen käyttöyhteydestä sekä tietoja käsittelevän viranomaisen ja rekisteröidyn välisestä suhteesta.[346] Tietosuojan toteuttamiseksi tarvitaan tietoturvatoimenpiteitä, jolloin perustuslaissa turvattujen yksityiselämän ja henkilötietojen suojan toteutuminen ovat riippuvaisia tietoturvasta.

Perustuslain 10 §:ään sisältyy yksityiselämän ja henkilötietojen suojan lisäksi *viestintäsalaisuus, jonka mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton*. Muu luottamuksellinen viesti voi tässä kontekstissa olla esimerkiksi sähköposti, joka on sellaisessa sähköpostilaatikossa, mikä ei ole kaikkien saatavilla eli kyseessä ei ole yhteissähköposti, ja sähköpostiin pääsy vaatii kirjatumista henkilön tunnuksilla. Ennen perustuslaissa turvattiin vain kirjesalaisuus, mutta teknologian kehityksen ja digitalisaation myötä lakiin lisättiin, että salassapito koskee myös muun muotoista viestiä[347]. Tämän muutoksen taustalla on välineneutraalisuuden periaate. Näin ollen säännöksellä turvataan kaikki luottamuksellisiksi tarkoitetut viestit riippumatta käytetystä menetelmästä, vaikka kirjeet ja puhelut ovat säännöksen mukaan tavallisimmat luottamuksellisimman viestinnän muodot.[348] Perustuslakiuudistuksessa painotettu välineneutraalisuus heijastuu myös informaatio-oikeuden teknologianeutraalisuuden periaateesta.

> Esimerkiksi tällaiseksi muuksi luottamukselliseksi viestinnäksi voidaan tapauskohtaisesti katsoa myös käyttäjän ja tekoälypohjaisten sovellusten, kuten kielimallien, välillä käytävä keskustelu, joka sisältää käyttäjän

[345] Melander 2019: 964–965. Ks. myös Voutilainen 2020: 100–101 ja Voutilainen 2023: 117.
[346] Voutilainen 2012: 51–52.
[347] Kemppinen 2011: 18.
[348] Viljanen 2011: 405–406.

tekemät kyselyt (promptit) sekä kielimallin vastaukset. Tällöin näistä keskusteluista tallentuvaa lokia tai keskusteluhistoriaa tulee käsitellä luottamuksellisena, rajatusti ja suojata riittävillä tietoturvatoimenpiteillä, sillä prompteissa saattaa olla hyvin henkilökohtaisia kysymyksiä tai muuta henkilötietoa.

Säännös turvaa jokaiselle oikeuden luottamukselliseen viestintään, jolloin tietoturvatoimenpiteillä tulisi suojata viestin välitystä niin, ettei kukaan ulkopuolinen saa oikeudettomasti tietää viestien sisältöä[349]. Säännöksessä ei rajata, missä vaiheessa luottamuksellisen viestin suoja alkaa taikka minkälaisin toimenpitein, ja milloin se päättyy[350]. Luottamuksellisen viestinnän suoja edellyttää, että viestinnän on myös näytettävä luottamukselliselta. Näin ollen, mikäli viesti on selkeästi kuultavissa, julkisesti esillä tai vastaavasti muiden ihmisten tiedossa, se ei täytä luottamuksellisen viestin määritelmää.[351] Huomioitava on, että esimerkiksi myös organisaation julkisissa tiloissa käydyt keskustelut arkaluontoisista asioista saattavat kuulua salassapitosopimuksien, liikesalaisuuksien ja henkilötietojen suojan piiriin.

Eri välineillä ja erilaisia teknologisia ratkaisuja hyödyntäen lähetettyjen luottamukselliseksi tarkoitettujen viestien tosiallinen tietoturvataso on erilainen ja esimerkiksi sähköpostiviestejä on tietoturvan näkökulmasta usein verrattu luottamuksellisuudeltaan postikortteihin. Kuitenkin sähköpostin tai minkään muunkaan viestinnän muodon asema luottamuksellisena viestinä ei ole sidoksissa siihen, mikä on viestinnän tosiasiallinen tietoturvan taso. Käyttäjän oikeusturvan kannalta on tärkeää, että viestinnän tavasta tai välineestä riippumatta viestintä saa yksiselitteisesti luottamuksellisen viestin suojan, jos sitä ei ole tarkoitettu yleisesti vastaanotettavaksi. Näin ollen esimerkiksi sähköpostin osalta luottamuksellisen viestin suoja ei edellytä viestin lähettämistä erikseen salattuna. Kuitenkin viestinnän luottamuksellisuutta voidaan pyrkiä edistämään tietoturvaa koskevilla velvoitteilla tai erilaisilla teknisillä määräyksillä.[352]

Viestin sisällön ohella suojataan myös viestin lähettäjän ja vastaanottajan välitystietoja[353] sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilyttämiselle. Tällaisia merkityksellisiä tietoja viestin luottamuksellisuuden

[349] Voutilainen 2012: 121.
[350] Nyblin 2009: 61.
[351] Neuvonen 2014: 42.
[352] Nyblin 2009: 56–57; HE 125/2003 vp: 9.
[353] Aiemmassa lainsäädännössä on käytetty termiä ”*tunnistamistieto”*, joka on korvattu termillä ”*välitystieto”*. Välitystieto on oikeus- tai luonnolliseen henkilöön yhdistettävissä oleva tieto, jota viestinnän välittäjä käsittelee viestien välittämiseksi. Ks. HE 221/2013 vp, s. 95. Välitystiedoista lisää luvussa 3.5.4 (”Muu teknisin menetelmin toteutettu valvonta ja välitystiedot”).

säilyttämisen suhteen on katsottu olevan myös esimerkiksi puhelujen välitystiedot. Aikaisemmin luottamuksellisen viestin suojan ydinalueeseen kuului viestin sisältö, kun taas välitystietojen katsottiin jäävän tämän ydinalueen ulkopuolelle. Mahdollisuus sähköisten viestien välitystietojen sekä niiden kokoamiseen ja yhdistämiseen voivat olla ongelmallisia yksityiselämän suojan ja luottamuksellisen viestin salaisuuden suojan kannalta, jonka vuoksi nykyään on katsottu, että välitystietojen rajaaminen luottamuksellisen viestin salaisuuden perusoikeussuojan ulkopuolelle ei ole perusteltua.[354] Myös oikeuskäytännössä, **esimerkiksi KKO 2022:23**, on katsottu välitystietojen kuuluvan yksityiselämän suojan alaan, sillä tietojen yhdistäminen muihin saatavilla oleviin tietoihin voi mahdollistaa yksityiskohtaisten päätelmien tekemisen viestintäpalvelun käyttäjän yksityiselämästä[355].

Perusoikeudet eivät ole täysin absoluuttisia. Moneen perusoikeussäännökseen sisältyy sääntelyvaraus, jonka nojalla lainsäätäjällä on toimivalta säätää yksityiskohtaisemmin kyseisen perusoikeuden käyttämisestä tavallisella lailla. Lisäksi joihinkin perusoikeussäännöksiin liittyy kvalifioitu lakivaraus, joissa on säädetty perusteista, joiden nojalla perusoikeutta on sallittua rajoittaa tavallisella lailla.[356] Esimerkiksi perustuslain 10 §:n asettaman yksityiselämän, kunnian ja kotirauhan[357] turvaamiseen liittyy kvalifioitu lakivaraus, jonka mukaan lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä.

Perusoikeuksien rajoittamiseen liittyen voidaan johtaa yleisiä vaatimuksia. Sen lisäksi, että perusoikeuksien rajoituksista on säädettävä lailla, tavallisella lailla ei voida kuitenkaan säätää rajoitusta, joka ulottuu perusoikeuden ytimeen. Rajoituksien on oltava tarkkarajaisia, täsmällisiä sekä rajoitusperusteiden tulee olla hyväksyttäviä ja painavan yhteiskunnallisen tarpeen vaatima. Rajoituksien on oltava suhteellisuusvaatimuksen[358] mukaisia ja välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi sekä otettava huomioon yhteiskunnallisen intressin

---

354 Heiskanen 2020: 94–95; Ojanen 2015: 20; Helopuro, Perttula & Ristola 2009: 270; Nyblin 2009: 60; Lehtonen 2008: 552, 554; Lehtonen 2001: 116; HE 309/1993 vp: 53; HE 125/2003 vp: 8, 44; HE 162/2003 vp: 69; PeVL 18/2014: 6; PeVL 9/2004 vp: 3–4.

355 KKO 2022:23, kohta 25.

356 Ojanen 2015: 40–41. Huomioitava on myös perustuslain 23 §, jossa on säädetty perusteista poiketa perusoikeuksista poikkeusoloissa pois lukien ehdottomat perus- ja ihmisoikeudet.

357 Verkkoyhteiskunnassa yhteiskunnan muutoksien myötä kotirauhaan kohdistuvat uhat muuttuvat, jolloin myös julkisen vallan velvoite suojata kotirauhaa muuttuu. Teknologian kehittymisen myötä uudenlaiset mahdollisuudet kotirauhan rikkomiseen yleistyvät, esimerkiksi IoT-laitteiden nopean yleistymisen myötä. Ks. Riekkinen 2019, s. 58–59.

358 Esimerkiksi yksityiselämän suojaan puuttumisessa tiedustelun osalta käytettyjen menetelmien ja niillä aiheutettujen haittojen tulee olla järkevässä suhteessa tavoiteltuun päämäärään verrattuna. Oikeasuhteisuusperiaatteessa tulee ottaa huomioon myös se, että toimenpiteiden on oltava riittävän tehokkaita päämäärien saavuttamiseksi. Ks. lisää Lohse & Viitanen 2019, s. 30.

painavuus suhteessa rajoitettavaan oikeushyvään. Rajoituksissa on otettava myös huomioon oikeusturvan toteutuminen. Viimeisimpänä vaatimuksena on se, että rajoitukset eivät saa olla ristiriidassa Suomea velvoittavien kansainvälisten ihmisoikeusvelvoitteiden kanssa.[359]

Monien verkkoyhteiskunnan palvelujen järjestäminen sekä julkisen vallan että yksityisten toimijoiden toimesta ei ole mahdollista ilman tiedollisiin perusoikeuksiin kajoamista. Täten yksilön oikeuksien suojaaminen edellyttääkin laajaa sääntelyä.[360] Tästä esimerkkinä laki sähköisen viestinnän palveluista (917/2014), jonka valmistelun yhteydessä ilmeni paljon näkökulmia niin tietosuojan ja turvallisuuden takaamisesta kuin tietoverkkojen käytöstä yksilön kannalta. Sähköisen viestinnän palveluista annetun lain luottamuksellisen viestin ja yksityisyyden suojaa koskevilla säännöksillä tarkennetaan nimenomaan perustuslain säännöksiä ja sääntely kohdistuu kaikkiin viestinnän välittäjiin. Liikenne- ja viestintävaliokunnan lausunnossa todetaan lain yhdeksi keskeisimmäksi tehtäväksi palvelujen käyttäjien oikeuksien[361] suojaaminen, josta ei tule tinkiä ilman välttämättömiä perusteita. Lisäksi valiokunta korostaa lausunnossaan tietoturvallisuuden ja yksityisyyden suojan olevan myös kansallinen kilpailukykytekijä.[362]

Perustuslain 10 §:n mukaan lailla säädetyt poikkeukset perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi voivat asettaa välttämättömiä rajoituksia viestin salaisuuteen ja siten myös yksityisyyteen. Kansallinen turvallisuus on yksi tällainen rajoittava tekijä.

Kansallinen turvallisuus on moniulotteinen käsite, jonka tarkoituksena on yhtä lailla turvata valtiota ja perustuslaillista demokratiaa, mutta myös turvata sisäisen turvallisuuden uhkilta, joilla on merkittävä kytkös valtion tärkeisiin intresseihin. Näin ollen kansallinen turvallisuus oikeuttaakin valtion yksilöön suuntautuvaa vallankäyttöä.[363] Esimerkiksi lokakuussa 2018 perustuslain 10 §:ään tehtiin muutos koskien luottamuksellisen viestin salaisuuden suojaa, jonka myötä tiedustelu kansallista turvallisuutta uhkaavasta toiminnasta mahdollistui rajoittamalla viestin suojaa. Tämä myös edesauttaa tiedustelulakien säätämistä tavallisina lakeina. Ennen lakimuutosta perustuslain 10 §:n rajoitus luottamuksellisen viestin salaisuuteen kuului seuraavanlaisesti: ”*Lailla voidaan säätää (lisäksi) välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana*”. Lakimuutoksen

[359] Neuvonen 2014: 32–33; PeVM 25/1994.
[360] Råman 2006a: 822.
[361] Esimerkiksi luottamuksellisen viestin ja yksityisyyden suojaaminen.
[362] Limnéll & Lonka 2015: 208–209; LiVM 10/2014 vp: 4, 18.
[363] Widlund 2020: 134, 137.

jälkeen tämä lause erotettiin omaksi neljänneksi momentikseen ja tehtiin loppuun lisäys: ”*-- sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.*” Muutosehdotus hyväksyttiin eduskunnassa lokakuussa 2018 (5.10.2018/817), jonka myötä perustuslakia muutettiin kiireellisellä menettelyllä eli jo sen hetkisellä vaalikaudella Suomen turvallisuustilanteen heikentymisen takia.[364] Näin ollen Suomen turvallisuustilanteen on katsottu olevan tarpeeksi vakava peruste edellä todetun liikenne- ja viestintävaliokunnan lausunnon mukaisen palvelujen käyttäjien oikeuksien suojaamisen tinkimättömyydelle. Tiedustelulait hyväksyttiin 11.3.2019[365]. Lainsäädännön keskeisin tavoite on kansallisen turvallisuuden parantaminen kuitenkin niin, että perusoikeuksien suojaan puuttuminen on pyritty rajaamaan niin vähäiseksi kuin se on mahdollista ottaen huomioon myös tiedustelutoiminnan tehokkuus ja tuloksellisuus[366].

Nykyisessä verkkoyhteiskunnassa, jota on myös tituleerattu valvontayhteiskunnaksi, yksityisyys ei ole enää itsestäänselvyys. Kyseessä oleva perustuslain muutos on esimerkki siitä, kuinka turvallisuuden kohentamiseen liittyvällä valvonnan lisäämisellä saatetaan myös rajoittaa yksilön oikeuksia. Kysymys on luottamuksesta ja sen puutteesta. Toisaalta internetin ja erityisesti sosiaalisen median käyttäjät eivät edes usein välitä omasta yksityisyydestään[367]. Oikeuskirjallisuudessa on myös pohdittu, voiko yksilö luopua luottamuksellisen viestin suojastaan esimerkiksi antaen sähköpostijärjestelmän ylläpitäjälle oikeuden tutkia kaikkia sähköpostiviestejään julkishallinnossa. Perusoikeusnäkökulmasta tällaista menettelyä, jossa käyttäjä luopuisi yleisluontoisesti perusoikeuksistaan, ei ole pidetty hyväksyttävänä menettelynä.[368] Esimerkiksi luottamuksellisen viestin perusoikeussuojan luopumattomuuden takia hyväksyttävä suostumus sähköpostiviestin sisällön ja välitystietojen käsittelylle ei tule olla yleisluonteinen ja epämääräinen ”kaikki tulevat viestini”, vaan suostumuksen tulee olla yksilöity, vapaaehtoinen ja tietoinen tahdonilmaisu[369]. Lähtökohtaisesti julkisen vallan ja viranomaisten on perustuslain 22 §:n nojalla turvattava perusoikeuksien toteutuminen. Yksittäistapauksessa esitetyn pyynnön perusteella tapahtuva tutkiminen on katsottu sallituksi.[370]

---

[364] HE 198/2017 vp: 4, 28; EV 77/2018 vp: 1–2; PeVM 4/2018 vp: 2, 9–11; Eduskunta 2018b.
[365] Eduskunta 2019.
[366] HE 202/2017 vp: 1.
[367] Wiatrowski 2016: 99. Käyttäjät olettavat, että palvelut ovat ilmaisia ja vastikkeettomia, eivätkä tunne palvelujen käyttöehtoja ja liiketoimintaperiaatteita. Samanaikaisesti käyttäjät haluavat suojata yksityisyyttään, mutta toisaalta he tuovat yksityiselämänsä tietoja vapaaehtoisesti palveluihin tietämättä, minkä laajuista tietojen käyttöä heidän tiedoillaan harjoitetaan. Ks. Pesonen 2017, s. 93–94.
[368] Pesonen 2013: 67, 110.
[369] Lehtonen 2005: 167.
[370] Lehtonen 2001: 121–122; Pesonen 2013: 67, 110.

Suojasta voidaan luopua lähinnä sillä perusteella, että perustuslain tarkoituksena ei ole järjestellä viestinnän osapuolten keskinäisiä suhteita ja käyttäytymistä[371]. Myös salassapitovelvollisuus ja muut säännökset saattavat asettaa esteitä viestin sisällön ja välitystietojen ilmaisemiselle[372]. Esimerkiksi työelämän tietosuojalaissa on asetettu raamit työntekijöiden sähköpostiviestien tutkimiselle. Vaikka internetin käyttäjät eivät välttämättä välittäisi omasta yksityisyydestään, lainsäädäntö ja perusoikeudet asettavat tietyt reunakehykset yksityisyydelle valvontayhteiskunnassa.

Yhteenvetona voidaan todeta, että aivan, kuten aikaisemmin käsitellyissä perustuslain 7 §:n turvallisuusoikeuden ja 15 §:n omaisuuden suojan säännöksissä on tunnistettavissa kyberturvallisuuden ulottuvuus, perustuslain 10 §:n mukaisesti jokaisen yksityiselämä, kunnia ja kotirauha tulisi olla turvattu kybertoimintaympäristössä. Perustuslain 10 § lisää viranomaisten velvollisuuksia toteuttamaan positiivisia toimenpiteitä yksilöiden oikeuksien turvaamiseksi ulkopuolisilta loukkauksilta. Yhtä lailla kaikilla organisaatioilla tulisi olla lainsäädännön kautta velvollisuuksia pitää yllä tietoturvan vähimmäistasoa yksilöiden oikeuksien suojaamiseksi, sillä verkottuneessa yhteiskunnassa yksilöt ovat riippuvaisia myös muiden organisaatioiden kuin viranomaisorganisaatioiden tuottamista palveluista ja toiminnoista. Perustuslain 10 § kattaa yksityiselämän suojan lisäksi henkilötietojen suojan ja luottamuksellisen viestinnän suojan. Henkilötietoja suojataan tietoturvatoimenpiteillä, kuten myös kaikkia luottamuksellisia viestejä riippumatta käytetystä menetelmästä[373]. Verkkoyhteiskunnassa kehittyvää oikeutta turvalliseen ja laadukkaaseen verkkoyhteiskunnan infrastruktuuriin ja sähköiseen identiteettiin on tulkittava perustuslain yksilön oikeuksien ja aseman sekä yksilön loukkaamattomuuden näkökulmasta, jolloin myös sääntelyssä tulisi pyrkiä yksilön oikeussuojan tehokkaaseen varmistamiseen[374]. Nykyisessä verkottuneessa ja järjestelmien varassa toimivassa yhteiskunnassa kyberturvallisuuden merkitys on kasvanut. Näin ollen yksityisyyden ulottuvuuksista yksityiselämän, henkilötietojen sekä luottamuksellisen viestinnän suoja ovat yhä enemmän riippuvaisia erityisesti kyberturvallisuudesta.

---

371 Kiviniemi 2000: 69.
372 Lehtonen 2005: 167.
373 Henkilötietojen suoja ja luottamuksellisen viestinnän suoja ovat kiinteästi sidoksissa tietoturvallisuudesta huolehtimisen vaatimukseen, koska tietoturvallisuudella luodaan edellytykset sekä tietosuojan että luottamuksellisen viestinnän suojan toteutumiselle. Ks. Voutilainen 2006a, s. 48.
374 Pöysti 2000: 99.

2.5.4 Sananvapaus ja tietoturva

Perustuslain 12 §:n *sananvapauteen kuuluu oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja viestejä kenenkään ennakolta estämättä*. Tarkempia määräyksiä on annettu lainsäädännössä, esimerkiksi liikesalaisuuksien osalta sananvapautta on rajoitettu lailla[375]. Yhteiskunnallisessa keskustelussa hyväksyttäviä perusteita sananvapauden rajoittamiselle ovat olleet muassa kansallinen turvallisuus, moraali ja uskonnolliset arvot, kun taas Euroopan ihmisoikeustuomioistuimen tärkein arviointiperuste sananvapauden rajoittamiselle on ollut välttämättömyys demokraattisessa yhteiskunnassa.[376] Lailla rajoittamisen vaatimuksen myötä sananvapautta ei voi rajoittaa lakia alemman tasoisilla säännöillä, kuten järjestyssäännöillä[377].

Lähtökohtaisesti sananvapaus kuuluu kaikille ja sitä ei ole sidottu tiettyyn viestintämuotoon[378]. Sananvapaus antaa yksilöille suojaa ilmaista itseään ja kommunikoida toistensa kanssa. Toinen sananvapauden näkökulma on poliittinen, jossa sananvapauden turvaamisella pyritään turvaamaan oikeus tiedonvälitykseen, osallistuminen julkiseen, avoimeen ja vapaaseen kansalaiskeskusteluun sekä osallistumaan ja vaikuttamaan yksilöitä ja yhteiskuntaa koskevaan päätöksentekoon. ”Kenenkään ennakolta estämättä” -kielto kohdistuu julkisen vallan lisäksi muihinkin tahoihin, kuten yksityishenkilöihin. Ennakkoesteiden kielto tarkoittaa viestien sisällön ennakkotarkastusta, sananvapauteen liittyvien oikeuksien luvanvaraistamista sekä muita ennakollisia esteitä merkitseviä puuttumisia sananvapauteen.[379] Näin ollen tietoturvan näkökulmasta sananvapautta koskeva säännös tarkoittaa sitä, että kolmas osapuoli ei saisi ennakolta a) kajota toisen lähettämiin viesteihin ja tietoihin muuttamalla tai poistamalla niitä; taikka b) kajota toisen viestintävälineeseen tai -yhteyteen, jonka seurauksena viestin ja tietojen lähettäminen tai vastaanottaminen estyy. Kolmas osapuoli voi olla tässä sekä julkinen valta että muu taho, kuten yksityishenkilö. Kaikilla tulisi olla oikeus sananvapauteen kenenkään ennakolta estämättä, eli oikeus vapaaseen kommunikointiin toisten kanssa, oikeus osallistua kansalaiskeskusteluun sekä oikeus osallistua yksilöitä ja yhteisöä koskevaan päätöksentekoon. Kyberturvallisuudella mahdollistetaan sananvapaus sähköisissä palveluissa.

Sananvapauteen kuuluu myös oikeus kuvata julkisissa paikoissa, tilaisuuksissa tai tiloissa viranomaisen sitä rajoittamatta, mikäli nämä paikat, tilaisuudet ja tilat ovat säädetty julkisiksi. Kuvaamiskielto julkisissa paikoissa, tilaisuuksissa ja

375 Kemppinen 2011: 45.
376 Neuvonen 2019: 74–75; 80–81.
377 Voutilainen 2019: 240.
378 Voutilainen 2012: 53.
379 Manninen 2011: 460–461, 468–469; HE 309/1993 vp: 57.

tiloissa on sananvapauden rajoittamista.[380] Tietoturvanäkökulmasta tähän liittyy fyysisen tilaturvallisuuden ulottuvuus, joka tulee ottaa huomioon esimerkiksi toiminnan riskejä arvioitaessa, arkaluontoista materiaalia käsiteltäessä ja toiminnan tietoturvallisuutta arvioitaessa julkisissa tiloissa sekä julkisten tilojen lähellä. Kuvaamisessa on myös kyberturvallisuuteen ulottuva näkökanta, sillä kuvat usein päätyvät internettiin, jolloin niiden näkyvyys voi olla hyvinkin laajaa ja digitaalista kuvista voi paljastua henkilötietojen lisäksi muuta organisaation luottamuksellista tietoa. Organisaation julkisissa tiloissa kuvaamisesta esimerkkinä eduskunnan oikeusasiamiehen ratkaisu **EOAK 1140/2011**:

> *Tapauksessa kantelija oli ottanut valokuvia yleisölle avoimissa Kelan tiloissa ja julkaisut niitä internetissä. Kela oli pyytänyt kantelijaa poistamaan kuvat, jonka vuoksi kantelija kertoi Kelan rajoittaneen hänen sanavapauttaan. Apulaisoikeusasiamiehen käsiteltäväksi asiaksi nousi muun muassa kysymys siitä, onko sananvapautta rikottu.*
>
> *Apulaisoikeusasiamiehen mukaan sananvapauden suojan asteeseen vaikuttaa se, rajoittaako sananvapaus jotain toista perus- ja ihmisoikeutta. Kahden perusoikeuden punninnassa, tässä tapauksessa sananvapaus ja yksityisyyden suoja, tavoitteena tulee olla molempien perusoikeuksien täysmääräinen samanaikainen toteutuminen. Tämä edellyttää tapauksessa asiaan osallisten perusoikeusintressien arvioimista. Tapauksessa nähdään yksityisyyden suojan tarve asiakkaiden asioidessa etuusasioissaan lähemmäksi yksityisyyden suojan ydinalueen ulottuvuutta. Sananvapauden ydinalueeseen kuuluu poliittisesti päämäärähakuinen kansanvallan toteutukseen tähtäävä viestintä. Tapauksessa tarkoituksena on ollut kuvata yksittäistä asiakastapahtumaa, ei niinkään tiettyä henkilöä. Sananvapauden takia Kela ei voi kokonaan kieltää valokuvaamista asiakaspalvelutiloissaan, eikä valokuvaamiseen edellytetä ennakkolupaa. Täten luvan edellyttäminen ja asettaminen kuvaamisen ehdoksi Kelan asiakaspalvelutiloissa ei ole lainmukaista. Asiakkaiden yksityisyyden turvaamisen kannalta voidaan kuitenkin pitää perusteltuna, että Kela ohjeistaa ennen kuvaamista olemaan yhteydessä henkilökuntaan. Tällä tavoin pystytään parhaiten ottamaan huomioon molempien kysymyksessä olevien perusoikeuksien toteutuminen. Kelan toimistoilleen antaman ohjeistuksen tulisi sisältää käytännön menettelytapaohjeet kaikenlaisen asiakaspalvelussa tapahtuvan kuvaamisen varalta. Näin Kelan toimistot pystyisivät turvaamaan asiakkailleen yhdenmukaisen turvan heidän yksityisyytensä suojaksi.*

[380] Voutilainen 2012: 70.

Täten kuvaamiskielto julkisissa tiloissa katsotaan sananvapauden rajoittamiseksi. Lähtökohtaisesti viranomainen ei voi omilla sisäisillä määräyksillään rajoittaa kuvaamista julkisissa tiloissa tai tilaisuuksissa, jotka ovat säädetty julkisiksi, vaan rajoitusten tulee olla mainittu laintasoisissa säännöksissä[381]. Kuitenkin apulaisoikeusasiamiehen ratkaisun pohjalta asiakkaiden yksityisyyden turvaamiseksi Kelan olisi syytä ohjeistaa käytännön menettelytapaohjein tiloissa kuvaamisesta, jotta myös yksityisyyden suoja perusoikeutena toteutuisi. Ratkaisusta voidaan päätellä, että loppujen lopuksi vastuu yksityisyyden suojan ja tietosuojan toteutumisesta jää kuitenkin itse organisaatiolle, jonka takia erityisesti suojattavien tietojen käsittelyä tulee välttää julkisissa tiloissa, paikoissa ja tilaisuuksissa. Ohjeistuksien heikko lenkki on siinä, että niiden toimivuus on riippuvainen ihmisistä. Näin ollen yksityisyyden suojan toteutuminen on yllä mainitussa tapauksessa riippuvainen siitä, noudattavatko ihmiset annettuja ohjeistuksia. Kelan toimistot pystyisivät turvaamaan asiakkailleen paremman yksityisyyden suojan ohjeistuksien lisäksi myös kiinnittämällä huomiota tilaratkaisuihin, esimerkiksi erilaisilla tilaa jakavilla sermeillä. Täten fyysisillä tietoturvatoimenpiteillä voidaan parantaa asiakkaiden oikeutta henkilötietojen suojaan, mutta myös edistää sitä, että sananvapauteen liittyvä oikeus kuvata julkisissa tiloissa toteutuu.

Sananvapaussäännös on välineneutraali[382], mikä tarkoittaa, että sitä sovelletaan kaikkiin nyt ja tulevaisuudessa käytettävissä oleviin viestintäteknisiin menetelmiin. Sananvapauteen liittyy myös sisältöneutraalisuuden periaate, jolloin sen soveltamisalaan kuuluu kaikenlaiset tiedot ja viestit niiden sisällöstä riippumatta. Kaikki viestit eivät kuitenkaan ole yhtä vahvasti sananvapaudella suojattuja, sillä viestinnän sisältöä voidaan rajoittaa lailla. Sananvapauden käyttöön puuttuminen liittyy yleensä ilmaisuvapausrikoksiin eli siihen, että ilmaistu tai julkistettu viesti on sisällöltään lainvastainen tai viestiä epäillään sellaiseksi. Esimerkiksi ilmaisuvapauden aineellisista rajoituksista säädetään pääasiassa rikoslaissa.[383] Toisena vaihtoehtona on perustuslain ristiriidat, esimerkiksi yksityiselämän suojan kanssa olevissa ristiriitatilanteissa tuomioistuimet[384] ovat antaneet yksityiselämän suojalle suuremman painoarvon kuin sananvapaudelle[385]. Yksityisyys rajoittaa muun muassa sananvapautta ja julkisuutta silloin, kun käsitellään henkilötietoja eli lainmukaisesti tietoja, joista henkilö on tunnistettavissa[386]. Toisaalta vastakohtaisesti

[381] Voutilainen 2019: 246.
[382] Vrt. ”teknologianeutraali”, ks. luku 2.4.2 (”Muut tietoturvalainsäädäntöön liittyvät keskeiset periaatteet”).
[383] Manninen 2011: 462–463, 483.
[384] Esimerkiksi ratkaisussa KKO 2010:39, kohta 39: Yksityiselämän suojan tarve on sitä ilmeisempi, mitä keskeisemmin tiedot liittyvät yksityiselämän ydinalueeseen ja mitä vähemmän tietojen julkistamisella voi olla merkitystä henkilön yhteiskunnallisen toiminnan arvioinnin kannalta.
[385] Viljanen 2011: 410–411.
[386] Neuvonen 2019: 26–27.

EU:n yleisen tietosuoja-asetuksen sekä kansallisen tietosuojalain soveltamista on tietyin ehdoin rajoitettu sananvapauden turvaamiseksi, kuten esimerkiksi henkilötietojen käsittely journalistisia tarkoituksia varten tai akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten[387].

Huomioitava on myös se, että työnantajan direktio-oikeus[388] ja omistusoikeus, saattavat vaikuttaa työntekijöiden mahdollisuuteen käyttää sananvapautta. Näiden oikeuksien nojalla työnantaja voi määrätä omistamiensa viestintävälineiden ja -yhteyksien käytöstä. Esimerkiksi työsähköpostien viestit saattavat kuulua työnantajalle, vaikka niitä suojataan vastaanottajan viesteinä. Lisäksi työnantajalla on oikeus direktio-oikeuden perusteella määrätä, miten ja mihin tietoverkkoa ja sähköpostia työpaikalla käytetään.[389] Tällaiset sananvapauden käytön rajoittamiset usein parantavat organisaation tietoturvaa, ja ne eivät rajoita yksilön sananvapauden käyttöä omilla laitteillaan ja omalla ajallaan. Työvälineiden tulisi olla lähtökohtaisesti vain työkäyttöön ja henkilökohtaiset välineet henkilökohtaiseen käyttöön, jolloin myös organisaation tietosuojaperiaatteiden ja -oikeuksien toteutuminen olisi helpommin hallittavissa. Huomioitava on, että työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely kuuluu työelämän tietosuojalain 21 §:n mukaisesti yhteistoimintamenettelyn piiriin, jonka jälkeen työnantajan tulisi tiedottaa sähköpostin ja tietoverkon käytöstä. Tällainen tiedotus voi tapahtua esimerkiksi sähköpostia ja tietoverkkoa koskevin ohjeistuksin tai käyttösäännöin.

Yhteenvetona voidaan todeta, että perustuslain 10 §:n mukaisesti luottamuksellisia sähköisiä viestejä on suojattava kybertoimintaympäristössä tietoturvatoimenpiteillä niin, että ne pysyvät luottamuksellisena. Yhtä lailla kybertoimintaympäristöä turvaavat tietoturvatoimenpiteet mahdollistavat perustuslain 12 §:n mukaisen sananvapauden, joka sisältää yksilön oikeuden ilmaista, julkistaa sekä vastaanottaa tietoja, mielipiteitä ja viestejä. Tällöin tietoturvatoimenpiteillä suojataan sananvapautta niin, että kolmas osapuoli ei saisi ennakolta kajota toisen lähettämiin viesteihin ja tietoihin, taikka kajota toisen viestintävälineeseen tai -yhteyteen, jonka seurauksena viestin ja tietojen lähettäminen tai vastaanottaminen estyy. Näin ollen myös sananvapauden turvaamisen osalta tietoturvalliset, sähköiset palvelut ovat olennaisia. Vakavat puutteet kyber- ja tietoturvallisuudessa voivat alentaa sanavapautta ja tiedon saantioikeuksia[390]. Tämä korostaa sitä, että organisaatioiden sisäinen tietoturvataso on oltava kunnossa eli hyvien

[387] Voutilainen 2019: 92.
[388] Direktio-oikeus on johdettu työsopimuslaista. Ks. luku 3.5 (”Työelämän tietosuoja ja tietoturva osana tietoturvan sääntelyjärjestelmää”).
[389] Pesonen 2013: 182–183.
[390] Pöysti 2023: 50.

tietoturvakäytänteiden mukainen, jotta organisaatiot voivat ylipäätänsä tarjota tietoturvallisia palveluita.

Vastakohtaisesti organisaatioissa tietoturvatoimenpiteillä rajoitetaan työntekijöiden sananvapautta. Esimerkiksi työnantajan direktio- ja omistusoikeus asettavat rajoituksia työntekijöiden sananvapauteen työn tekemiseen käytettävän sähköpostin ja tietoverkon osalta, mikä osaltaan parantaa organisaatioiden tietoturvaa. Näin ollen organisaatioiden tietoturvatoimenpiteillä sekä turvataan että rajoitetaan sananvapauden toteutumista. Huomioitava on, että sananvapauteen kohdistuu muitakin rajoituksia, kuten ilmaisukielto lainvastaisen sisällön julkistamisesta tai kuvaamiskielto julkisesta tilasta kotirauhan suojaamaan paikkaan. Lähtökohtaisesti kuvaaminen julkisissa tiloissa ja tilaisuuksissa on sallittua, jolloin organisaatioissa tulee huomioida erityisesti riittävät fyysiset tietoturvatoimenpiteet sekä tiedonkäsittelysäännöt tietojensa ja perustuslain 10 §:n oikeuksien suojaamiseksi. Tämä kuvastaa hyvin sitä, kuinka moniulotteinen on sananvapautta turvaava perustuslain 12 § tietoturvallisuuden näkökulmasta.

2.5.5 Julkisuusperiaate ja salassapitointressi

Julkisuusperiaate voidaan nähdä kolmitahoisena: asiakirjajulkisuutena, käsittelyjulkisuutena ja asianosaisjulkisuutena. Asiakirjajulkisuus liittyy nimenomaan oikeuteen saada tieto viranomaisen asiakirjasta, joka on julkinen. Käsittelyjulkisuus ilmenee kansalaisen oikeutena seurata asioiden käsittelyä hallintoviranomaisen (esimerkiksi tuomioistuimen) toimesta tapahtuvassa käsittelyssä, ellei tätä oikeutta ole rajoitettu tiettyjen säännösten perusteella. Asianosaisjulkisuus liittyy asianosaisen oikeuteen tutustua aineistoon häntä koskevassa asiassa.[391] Tietoturvallisuuden (ja kyberturvallisuuden) näkökulmasta asiakirjajulkisuus on näistä kolmesta oleellisin.

Perutuslain 12 §:*ään liittyvän julkisuusperiaatteen mukaan viranomaisen asiakirjat ja tallenteet ovat julkisia, ellei niiden julkisuutta ole lakiin perustuvin syin rajoitettu (esimerkiksi valtion etuun ja maanpuolustukseen liittyvät syyt).* Tietoturvan perinteisten kolmen ulottuvuuden kannalta etenkin eheys ja käytettävyys korostuvat julkisuusperiaatteen toteutumisessa. Valtaosaa asiakirjoista käsitellään nykyään sähköisissä järjestelmissä ja palveluissa, joten asiakirjojen tulee olla käytettävissä (saatavilla), kun henkilöt tarvitsevat niitä, ja tietojen tulee olla oikeita ja johdonmukaisia eli eheitä. Oikeus tutustua julkisiin asiakirjoihin muodostuu käytännössä sisällöttömäksi ja julkisuusperiaate ei toteudu, jos asiakirjojen

[391] Korhonen 2003: 36–37.

eheyttä ei suojata luvattomalta muuttamiselta[392]. Mikäli asiakirjan julkisuutta on lakiin perustuvin syin rajoitettu, korostuu tietoturvan kolmesta ulottuvuudesta erityisesti luottamuksellisuus.

Julkisuuslain 5 §:n mukaan asiakirjaksi katsotaan kirjallinen tai kuvallinen esitys taikka viesti, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai muiden apuvälineiden avulla ja koskee sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa kohdetta tai asiaa. Asiakirjan käsite on väline- ja teknologianeutraali, jolloin mikä tahansa tallennettu ja toisinnettavissa oleva tieto kuuluu asiakirjan käsitteen piiriin[393]. Oikeuskäytännössä viranomaisen tietojärjestelmän lokitiedoista on katsottu muodostuvan viranomaisen asiakirja[394]. Täten asiakirja voi olla sekä perinteinen paperimuotoinen asiakirja tai sähköisesti tallennettu tietoaineisto[395]. Tällöin asiakirjan on laatinut viranomainen taikka viranomaisen palveluksessa tai toimeksiannon alla oleva taho, tai se on toimitettu viranomaiselle käsittelyä varten taikka viranomaisen lukuun toimivalle toimeksiantotehtävän suorittamista varten.[396]

Julkisuuslain asiakirjamääritelmään on myös poikkeuksia, jotka on täsmennetty julkisuuslain 5 §:ssä. Esimerkiksi viranomaisen asiakirjana ei pidetä lähtökohtaisesti muun muassa muistiinpanoja, viranomaisen yksityiseen lukuun suoritettavaan tehtävään liittyvää asiakirjaa tai sisäistä käyttöä varten hankittuja asiakirjoja.

Hallinnollisena periaatteena salassapito on vanhempi kuin julkisuusperiaate. Salassapito ja toisaalta julkisuuden laajuus voidaan nähdä vallankäyttöön liittyvänä kokonaisuutena, jossa julkisuutta sallitaan vain siinä laajuudessa, mikä ei haittaa vallankäyttäjiä. Salassapito ei kuitenkaan johdu yksinomaan päätöksen tekijöiden tai päätöksenteon suojan tarpeista, vaan asiassa tulee huomioida myös kansalaisten yksityiselämää koskevat tiedot ja niiden suojaaminen.[397] Julkisuusperiaatteen vaatimukset kulkevat rinnakkain tietosuojaperiaatteiden asettamien vaatimusten kanssa niin, että niitä on punnittava tapauskohtaisesti aina, kun tehdään informaation käsittelyä koskevia teknisiä ratkaisuja[398]. Viranomaisen hallussa olevat yksityishenkilöä koskevat tiedot ovat pääosin suojattuja eikä tietoja anneta

[392] Andersson & Nordén: 64.
[393] Voutilainen 2019: 47.
[394] Kuopion HAO 11.11.2011 11/0424/2
[395] Ks. myös VAHTI 2/2010: 19.
[396] Huomioitava on, että julkisuuslain mukainen asiakirjan määritelmä tulee todennäköisesti täsmentymään lähitulevaisuudessa nykyaikaisten tietojenkäsittelytapojen mukaiseksi. Ks. Oikeusministeriön asettaman työryhmän mietintö julkisuuslain ajantasaistamiseksi tarvittavista lainsäädännön muutosehdotuksista (Oikeusministeriön julkaisuja 2023:32, s. 113–125 on erityisesti käsitelty lakiehdotuksen 6 §:n viranomaisen asiakirjan määritelmää).
[397] Wallin & Nurmi 1991: 2–3.
[398] Voutilainen 2006a: 45–46.

ulkopuolisille[399]. Myös julkisen asiakirjan osalta tulee punnita erityisesti henkilötietojen julkaisemisen tarpeellisuutta ja tapaa. Offline ja online -käsittelymaailmojen välillä on ero, jonka vuoksi tiedon saatavuus julkisuusperiaatteen mukaisesti ei ole yksiselitteinen: verkkoympäristössä hakukoneiden olemassaolo ja mahdollisuus googlettaa joku, antaa tiedon hakijalle mahdollisuuden yhdistää valtavia määriä tietoa eri lähteistä[400]. Tällöin on henkilötiedon luonne ja käyttötarkoitussidonnaisuus huomioon ottaen pohdittava, onko tarkoituksenmukaista julkaista julkinen asiakirja avoimeen internettiin rajoittamattoman ajan vai mahdollistaa asiakirjajulkisuus hallitummin. Julkisissa asiakirjoissa yksilöä kuvaavien asioiden julkistaminen vaatii tapauskohtaista punnintaa, sillä henkilöä koskevan tiedon julkistaminen saattaa edellyttää asianomaisen henkilön suostumusta[401].

Salassapidon lähtökohtana tulee aina pohtia salassapidon intressiä, joka toteutuessaan muodostaa välittömän perusteen rajoittaa tiedonsaantia viranomaisen asiakirjoista. Salassapitointressi syntyy esimerkiksi, jos julkisuus loukkaisi tärkeitä yleisiä ja yksityisiä etuja, joilla on sidos perusoikeuksiin. Jos vain osa asiakirjasta on salassa pidettävää, tällöin viranomaisen asiakirjan julkisesta osasta on annettava tieto.[402] Viranomaisen salassa pidettävien asiakirjojen salassapitoperusteista on myös säädetty julkisuuslain 24 §:ssä, jossa esimerkiksi yksi oleellinen peruste tietoturvan näkökulmasta salaamiselle on kohdan 7 mukainen rakennusten sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat, joiden julkisuus voisi vaarantaa kyseiset turvajärjestelyt. Salassapitoa toteuttaessa on huomioitava niin hallinnollisen, fyysisen kuin teknisen tietoturvallisuuden vaatimukset.

Esimerkiksi ratkaisussa **KHO 12.10.2017 taltio 5055** asiakirjajulkisuutta rajoitettiin muun muassa liike- ja ammattisalaisuuksien tuomien julkisen taloudellisen edun salassapitointressillä sekä järjestelmän testausraporttien julkaisemiseen liittyvän tietoturvariskin takia, joka vahingoittaisi tai vaarantaisi turvallisuutta tai poikkeusoloihin varautumista.

> *Yleisradion toimittaja oli pyytänyt saada HUS-kuntayhtymän sairaanhoitopiirin PACS-tietojärjestelmän hankintaan liittyviä asiakirjoja (mm. tarjous ja liitteet liittyen järjestelmän ylläpitoon ja päivitykseen) sekä järjestelmän testausraportin asiakirjajulkisuuteen vedoten. HUS-*

[399] Pesonen 2017: 139. Tietoja voi antaa, jos asiakirja on henkilöä itseään koskeva, asianosaisjulkinen tai yleisöjulkinen (myös s. 139). Ks. myös julkisuuslain 24 §.
[400] Talus 2019: 237–238. Toki verkkoympäristössäkin tulee käsitellä julkisesti saatavilla olevia henkilötietoja asianmukaisesti. Tällöin julkisen henkilötiedon käsittelylle tulee olla lainmukainen peruste, ellei käsittely ole yksityisiin tarkoituksiin tehtyä (ks. myös Talus 2019 238–239).
[401] Pesonen 2017: 140.
[402] Voutilainen 2012: 54, 74.

kuntayhtymän toimitusjohtaja kuitenkin kieltäytyi toimittamassa tiettyjä liitteitä, jotka sisältävät liike- ja ammattisalaisuuksia.

Ratkaisussa on sovellettu julkisuuslakia. Helsingin hallinto-oikeus toteaa, että liike- tai ammattisalaisuutta ei julkisuuslaissa ole tarkemmin määritelty, mutta hallituksen esityksen HE 30/1998 mukaan asiakirjat ovat salassa pidettäviä ilman lisäedellytyksiä. Salassapitotahto ei kuitenkaan ole yksistään ratkaiseva, vaan salassapitointressejä on arvioitava kokonaisuutena. Asiakirjojen on katsottu sisältävän liike- ja ammattisalaisuuksia, joista tiedon antaminen aiheuttaisi taloudellista vahinkoa, heikentäisi mahdollisuuksia edullisiin hankintoihin sekä vaikuttaisi haitallisesti julkisyhteisön kilpailuasemaan. Näin ollen hallinto-oikeuden mukaan julkisuuslain edellyttämän salassapitoperusteen on julkinen taloudellinen etu. Myös muut järjestelmätietoja sisältävät liitteet katsottiin sisältävän liike- ja ammattisalaisuuksia ja ovat siten salassa pidettäviä. Lisäksi osajulkisuuden toteuttaminen ei ole mahdollista asiakirjapyynnön kohteena olevien asiakirjojen osalta, sillä tällöin ne eivät ole oikein luettavissa tai ymmärrettävissä niiden sisältämien liike- ja ammattisalaisuuksien peittämisen jälkeen.

Testausraporttien osalta hallinto-oikeus katsoi dokumenttien olevan julkisuuslain mukaisia viranomaisen asiakirjoja. Koska ne sisältävät poikkeusoloihin varautumista sekä tietoja tietojärjestelmän turvajärjestelyistä, salassapito perustuu julkisuusolettamaan. Nämä asiakirjat on pidettävä salassa, koska huomioon ottaen HUS:n toiminnan luonne ja laajuus tiedon antaminen testausasiakirjoista vahingoittaisi tai vaarantaisi turvallisuutta tai poikkeusoloihin varautumista. Tietojen joutuminen ulkopuoliselle johtaisi merkittävään tietoturvariskiin. Raportit sisältävät myös liike- ja ammattisalaisuuksia, jolloin ne kuuluvat ehdottoman salassapidon piiriin.

Asia eteni korkeimpaan hallinto-oikeuteen, koska yleisradio valitti, että yleisluonteiset lausumat eivät voi olla liike- tai ammattisalaisuuksia, ne eivät vaaranna järjestelmän turvajärjestelyjä tai onnettomuuksiin ja poikkeusoloihin varautumista tai sisällä muutenkaan sen kaltaista tietoa, joka edellyttäisi testausraporttien täydellistä salaamista. Asiakirjoja ei tule salata enempää kuin suojattavan edun vuoksi on tarpeellista. KHO kuitenkin hylkäsi valituksen.

Viranomaisen on punnittava eri suuntaisia julkisuus- ja salassapitointressejä, jolloin esimerkiksi salassapitotahto ei ole riittävä peruste, vaan salassapidon arvio on

tehtävä lain mukaisin objektiivisin perustein[403]. Edellä mainittu tapaus on hyvä esimerkki salassapitointressin toteutumisesta viranomaisen asiakirjojen suhteen. Täten viranomaisen tietojärjestelmien testausraportit sisältäessään tietoja turvajärjestelyistä voivat ilman salassapitoa vaarantaa turvallisuutta tai poikkeusoloihin varautumista huomioon ottaen viranomaisen toiminnan luonne. Tällöin salassapitointressiksi katsotaan valtion etuun ja maanpuolustukseen liittyvät syyt, joista johdettuna tietojen julkaiseminen voisi loukata myös muita etuja, joilla on sidos perusoikeuksiin. Kyseisessä tapauksessa on myös huomioitava se seikka viranomaisen asiakirjojen osalta, että niiden on oltava viranomaisen hallussa, eli viranomaisen toimipaikalla taikka viranomaisessa toimivalla henkilöllä, ollakseen viranomaisen asiakirjoja[404]. Tapauksessa ei ollut KHO:n käsiteltävissä asiakirjoissa yleisradion toimittajan pyytämää testausraporttia, joten asiakirja ei ollut käytettävissä, eikä näin ollen tuomioistuimen päätös koskenut tämän asiakirjan julkisuusasemaa. HUS:n mukaan he eivät voineet yksiselitteisesti tietää, mistä asiakirjasta on kyse.

Yrityksillä ei ole velvollisuutta antaa tietoja muuten kuin lakiin kirjatuin perustein viranomaiselle tai poikkeuksellisesti toiselle yksityiselle taholle. Julkisuuslait eivät koske näitä tietoja paitsi silloin, kun tieto on viranomaisen hallussa. Tällöin esteen julkisuudelle muodostavat yritysten liike- ja ammattisalaisuuksien suojaksi säädetyt normit ja yksilöä suojaava yksityiselämän ja henkilötietojen suoja. Yritykset pitkälti itse määrittelevät, mikä informaatio on salaista kullakin alalla ja mikä on yleisesti saatavilla tai siksi tarkoitettua. Näillä tiedoilla on yleensä merkitystä yrityksen kilpailukyvylle. Eri alojen omat salassapitomääräykset eivät kuitenkaan ratkaise sitä, mitkä tiedot ovat viranomaisen hallussa salassa pidettäviä tai julkisia. Tiedon salassapito määräytyy asiakirjakohtaisesti, vaikka se olisikin yksityisen laatima asiakirja. Kuitenkin yksityinen liike- ja ammattisalaisuus on pääsääntöisesti suojattu eikä se ole yleisen tiedonsaantioikeuden piirissä. Yrityssalaisuudeksi katsottavien tietojen luovuttaminen on sidottu siihen aiheuttaako tiedon antaminen haittaa elinkeinotoiminnalle.[405]

Asiakirjasalaisuuden lisäksi salassapitovelvollisuus on voitu ilmaista lainsäädännössä vaitiolovelvollisuutena[406] tai muuna ilmaisukieltona. Näiden velvollisuuksien rikkominen voi tulla arvioitavaksi salassapitovelvollisen aseman sekä salattavien tietojen sisällön perusteella erilaisilla rikosnimikkeillä, kuten

[403] Kulla & Salminen 2021: 505–506.
[404] Kulla 2018: 407.
[405] Pesonen 2017: 133–134.
[406] Vaitiolovelvollisuutensa nojalla virkamies ei saa luvatta paljastaa sellaista seikkaa, joka sisältyy salassa pidettävään asiakirjaan tai jonka hän muutoin tietää salassa pidettäväksi. Ks. Laurikkala 2020, s. 48–49. Ks. myös julkisuuslain 23 § 1 momentti vaitiolovelvollisuudesta ja hyväksikäyttökiellosta.

yrityssalaisuuden rikkominen.[407] Lisäksi organisaatioiden liikesalaisuuksia on mahdollista pyrkiä suojaamaan myös sopimuksellisin keinoin[408]. Huomioitava on, että julkisuuslain mukainen liikesalaisuus ei ole täysin yhtenevä rikoslain yrityssalaisuuden kanssa. Ratkaisevaa ei ole yksinomaan yrityksen salassapitotahto, vaan arvioida pitää myös yrityksen subjektiivisen salassapitotahdon lisäksi objektiivista salassapitointressiä.[409]

Yhteenvetona todettakoon, että asiakirjajulkisuuteen liittyy nimenomaan yksilöiden perusoikeus saada tieto viranomaisen julkisesta asiakirjasta, jolloin julkisuusperiaatteen turvaamisen osalta korostuvat tietoturvallisuuden ulottuvuuksista etenkin eheys ja käytettävyys. Vastakohtaisesti asiakirjojen julkisuuden rajoittaminen salassapitointressin turvin, esimerkiksi kansallisen turvallisuuteen tai tietojärjestelmien turvajärjestelyjen vaarantumiseen vedoten, korostaa tietoturvallisuuden ulottuvuuksista luottamuksellisuutta. Näin ollen asiakirjojen tulee olla oikea-aikaisesti saatavilla ainoastaan oikeutetuille henkilöille, ja niissä olevan informaation tulee olla oikeanlaista ja virheetöntä. Julkisuusperiaatteen ja salassapitointressin välillä tulee huomioida myös henkilötietojen suojaamisen taustalla vaikuttavat tietosuojaperiaatteet, jolloin julkisen asiakirjan osalta on punnittava erityisesti henkilötietojen julkaisemisen tarpeellisuutta ja tapaa. Punnittavaksi tulevat tietosuojalainsäädännön rajoitusten ohella liike- ja ammattisalaisuuksien suojaksi säädetyt normit. Lainsäädännön vaatimukset asettavat toiminnallisia vaatimuksia viranomaisen järjestelmille, jolloin esimerkiksi viranomaisen asianhallintajärjestelmien ja muut keskeisiä asiakirjoja sisältävien järjestelmien tulee olla tietoturvallisia ja vikasietoisia. Tähän liittyy keskeisesti hyvän hallinnon periaate, johon katsotaan kuuluvan vaatimus julkisen vallan tietojärjestelmien häiriöttömästä ja laadukkaasta toiminnasta[410]. Sekä asiakirjojen julkisuuden että salassapidon osalta pyritään tietoturvatoimenpiteiden avulla turvaamaan perusoikeuksia. Tämä on hyvä esimerkki siitä, miten oikeus tietoturvaan metaperiaatteena heijastuu perusoikeuksien taustalla olevana ”oikeutena oikeuksista”.

---

[407] Voutilainen 2019: 251–254. Mainittuja rikosnimikkeitä voivat olla esimerkiksi turvallisuussalaisuuden paljastaminen (RL 12 luku 7 §) ja tuottamuksellisen turvallisuussalaisuuden paljastaminen (RL 12 luku 8 §), salassapitorikos (RL 38 luku 1 §) ja salassapitorikkomus (RL 38 luku 2 §), virkasalaisuuden rikkominen (RL 40 luku 5 §), yrityssalaisuuden rikkominen (RL 30 luku 5 §), yrityssalaisuuden väärinkäyttö (RL 30 luku 6 §) ja yritysvakoilu (RL 30 luku 4 §).

[408] Näitä seikkoja on tarkastelu jäljempänä osana henkilöstöturvallisuutta, ks. luku 3.5.6 (”Henkilöstöturvallisuus: työntekijöiden luotettavuus ja tiedon salassapito”).

[409] Pesonen 2017: 136. Ks. myös KHO 2007:83: X Oy halusi pitää yksikköhinnat salaisuuksinaan ja yhtiöllä oli objektiivisesti arvioiden salassapitointressi. Julkisuuslain 11 §:n 2 momentin 6 kohdan sanamuodon mukaisesti tarjouksen hinta on tarjouksen tekijän liike- ja ammattisalaisuus, josta asianosaisella on kuitenkin oikeus saada tietoa. Yksikköhintoja pidettiin kuitenkin X Oy:n liikesalaisuuksina, koska niiden julkisuus olisi antanut muille elinkeinoharjoittajille kilpailuetua.

[410] Ks. Saarenpää 2016a: 82, 136.

2.5.6 Perusoikeuksien turvaaminen oikeusvaltiossa ja hyvä hallinto

Oikeuksiin on usein sidottu velvollisuuksia. Esimerkiksi perustuslain 7 §:n oikeus henkilökohtaiseen turvallisuuteen korostaa julkisen vallan positiivisia toimintavelvoitteita yhteiskunnan jäsenten suojaamiseksi rikoksilta ja muilta oikeuden vastaisilta teoilta[411]. Nämä julkisen vallan positiiviset toimivelvoitteet koskevat myös velvoitteita tieto- ja viestintärikoksilta suojaamiseksi ja turvallisuuden toteuttamiseksi, jolloin julkisen vallan tulee toteuttaa tietoturvatoimenpiteitä.

Hyvä esimerkki velvollisuudesta toteuttaa tietoturvatoimenpiteitä sisältyy Euroopan ihmisoikeustuomioistuimen ratkaisuun **EIT 17.7.2008, I. V. Finland**:

> *Tapauksessa käsiteltiin potilaan yksityisyyden suojan loukkausta, kun potilastietojärjestelmä oli ominaisuuksiltaan puutteellinen ja henkilörekisteriin pääsi käsiksi potilasta hoitaneiden henkilöiden lisäksi myös muu henkilöstö. Potilas työskenteli samassa sairaalassa ja sai tietää, että työkaverit olivat saaneet tietää hänen arkaluontoisesta sairaudestaan potilastietojärjestelmän kautta. Sairaalassa työskennelleen potilaan ei ollut mahdollista selvittää, kuka oli käynyt katsomassa hänen tietojaan ja loukannut hänen yksityisyyttään. Ihmisoikeustuomioistuimen ratkaisun mukaan valtion positiivisiin velvollisuuksiin kuuluu suojata henkilöiden yksityiselämää. Tätä velvollisuutta ja silloisen henkilörekisterilain vaatimuksia oli rikottu potilastietojärjestelmän puutteellisen toteutuksen vuoksi.*

EIT:n tapauksessa käsitellyssä järjestelmässä oli puutteellisen identiteetin ja pääsynhallinnan (IAM – Identity and Access Management) lisäksi puutteellinen lokitustoiminto[412], sillä potilastietojärjestelmästä pystyi näkemään vain viisi viimeisintä rekisterissä käyntiä eikä niitäkään ollut mahdollista henkilöittää eli kohdistaa tiettyyn työntekijään.

EIT:n tapauksesta päätellen yksityiselämän suojaan puuttumista on muun muassa se, että terveystietoihin pääsy ei ole kontrolloitua. Valtiolla on positiivinen velvollisuus ryhtyä toimenpiteisiin luonnollisen henkilön yksityis- ja perhe-elämän tehokkaaksi turvaamiseksi. Täten valtiolla on velvollisuus suojata henkilön terveystietoja siten, ettei ulkopuolisilla ole niihin pääsyä. [413] Tietoja suojatessaan

---

[411] HE 309/1993 vp: 47.
[412] Tässä yhteydessä lokilla tarkoitetaan tapahtumatietoja, jotka muodostuvat tietojärjestelmissä. ATK-sanakirja 1 2008, s. 162: Loki on tiedosto, johon kirjataan aikajärjestyksessä merkinnät tapahtumista ja niihin liittyvistä seikoista. Loki voi olla myös ohjelma, joka tuottaa lokitiedostoa. Lokia kerätään yleensä automaattisesti ja samaan järjestelmään liittyviä lokeja voi olla useita.
[413] Korja 2016b: 191; Heikkilä & Hirvelä 2017: 641, 682.

viranomaisen on salassapitointressin ja tiedonsaantioikeuksien toteuttamisen lisäksi otettava asianmukaisesti huomioon käytettävissä olevat tekniset mahdollisuudet, tietojen laatu, määrä ja ikä sekä suojaamiskustannukset. Näin ollen tietojärjestelmät on suojattava asianmukaisesti toimilla, joilla sekä estetään tietojärjestelmiin kohdistuvat tunkeutumiset, häiriöt ja vahingot että mahdollistetaan vain oikeutettujen tiedon saaminen.[414] Pääsynhallinta on yksi tietojärjestelmän käyttöön liittyvistä tietoturvatoimenpiteistä ja näin ollen tuomioistuin katsoi, että valtiolla on velvollisuus huolehtia lainsäädännön tasolla pääsynvalvonnan asianmukaisesta sääntelystä. Johtopäätöksenä voidaan todeta, että tietoturvallisuudella on myös ihmisoikeuksiin ulottuva näkökanta, sillä tietoturvallisuus tietojärjestelmän ominaisuutena on nostettavissa yhdeksi keskeisistä keinoista turvata yksilön ihmisoikeuksia sähköisessä toimintaympäristössä.[415] Yhtä lailla ihmisoikeustuomioistuimessakin otetaan kantaa yhteiskunnan tietotekniseen kehitykseen[416]. Tapaus korostaa myös kyberturvallisuuden merkitystä, sillä sen avulla turvataan yksilöiden oikeuksia sähköisessä toimintaympäristössä velvoittaen organisaatioita turvaamaan asianmukaisesti teknisin keinoin järjestelmänsä niissä käsiteltävän tiedon kriittisyyden mukaan.

Euroopan ihmisoikeussopimuksen (EIS) vaikutukset sekä valtion positiivinen toimintavelvollisuus ulottuvat myös yksityisten välisiin suhteisiin. Ihmisoikeussopimuksen mukaista suojaa pyritään takaamaan henkilötietojen käsittelyedellytyksiä koskevalla ja korvausvastuuseen johtavalla lainsäädännöllä sekä oikeuksien turvaa ylläpitävällä oikeuskäytännöllä. Kyseisestä EIT:n tapauksesta on myös todettu, että Suomen kansallisen lain pitäisi pystyä tarjoamaan asianmukaiset takeet siitä, ettei potilastietoihin päästä eikä niitä paljasteta.[417] Kyseisellä EIT:n ratkaisulla on merkitystä, sillä siitä voidaan tulkita kyberturvallisuuden olevan ihmis- ja perusoikeuksiin ulottuva oikeus. Tietoturvatoimenpiteillä edistetään kyberturvallisuuden toteutumista organisaatiossa, jolloin riittävän tietoturvatason ylläpitäminen on myös velvollisuus, joka on otettava huomioon organisaation toimintaa ja tietojärjestelmiä suunniteltaessa.

Perustuslain 22 §*:n mukaan julkisen vallan on turvattava perus- ja ihmisoikeuksien toteutuminen*. Tätä voidaan tulkita niin, että viranomaisen on velvollisuuksiensa mukaan otettava huomioon toiminnassaan tietoturva-asiat[418]. Perusoikeuksien tosiasiallinen toteutuminen vaatii julkisen vallan aktiivisia toimenpiteitä oikeuksien suojaamiseksi muun muassa ulkopuolisilta loukkauksilta (esim.

[414] Mäenpää 2016: 254.
[415] Voutilainen 2019: 36–37, 201.
[416] Saarenpää & Riekkinen 2023: 81.
[417] Korpisaari, Pitkänen & Warma-Lehtinen 2018: 9–10, 162; Korpisaari, Pitkänen & Warma-Lehtinen 2022: 12–13.
[418] Voutilainen 2012: 121.

tietoturvaloukkaukset) tai tosiasiallisten edellytysten luomiseksi oikeuksien käyttämiselle (esim. palveluiden käytettävyys)[419]. Näin ollen julkisen vallan on turvattava perusoikeuksien toteutuminen eli muun muassa kaikki tässä tutkimuksessa aikaisemmin mainitut oikeudet, jotka ovat myös kytköksissä tieto- ja kyberturvallisuuteen: oikeus turvallisuuteen (PL 7 §) ja omaisuuden suojaan (PL 15 §), oikeus yksityiselämän, henkilötietojen ja luottamuksellisen viestin suojaan (PL 10 §), oikeus sananvapauteen (PL 12 §), oikeus saada tieto viranomaisen julkisesta asiakirjasta (PL 12 §) sekä oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivästystä (PL 21 §). Perustuslain 22 §:n julkisen vallan turvaamisvelvoitetta voidaan pitää rinnasteisena perus- ja ihmisoikeusmyönteisen tulkinnan periaatteen kanssa[420]. Perustuslain 22 § on kuitenkin epäitsenäinen, joten sitä voidaan soveltaa vain yhdessä jonkin toisen perusoikeussäännöksen tai ihmisoikeusmääräyksen kanssa[421].

Perustuslain 2 §:*n oikeusvaltioperiaatteen mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia*[422]. Tästä on johdettavissa, että myös tietoturvaan liittyvien viranomaisvastuiden tulee perustua lainsäädäntöön[423]. Tietoturvallisuuden ja verkkoyhteiskunnan infrastruktuurin perusteet ovat yksilön asemaan olennaisesti vaikuttavia, ja näin ollen ne ovat myös lailla järjestettäviä asioita[424].

Perustuslain 21 §:*n mukaan jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivästystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa*. Tähän liittyy myös oikeus saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi. Aivan kuten julkisuusperiaatteessakin, tietoturvan perinteisistä ulottuvuuksista etenkin käytettävyys ja eheys korostuvat sähköisiä viranomaisjärjestelmiä käytettäessä asioinnissa.

Hyvän hallinnon periaatteiden ja oikeudenmukaisen oikeudenkäynnin vaatimusten ohella julkista valtaa koskee vaatimus tietojärjestelmien laadukkaasta ja häiriöttömästä toiminnasta. Informaatiota käsitellään viranomaisten tietojärjestelmissä, ja tästä syystä tietojärjestelmät eivät ole ainoastaan toimistoautomaation teknisiä apuvälineitä vaan myös oikeudellisen toiminnan keskeisiä elementtejä digitaalisessa yhteiskunnassa. Näin ollen esimerkiksi hallintopäätös ei lähtökohtaisesti saa viivästyä tietojärjestelmien toimimattomuuden vuoksi eikä

[419] Lavapuro & Tuori 2011: 810; HE 309/1993 vp: 75.
[420] Saraviita 2011: 295.
[421] Voutilainen 2006a: 19; Tuori 1999b: 667.
[422] He 1/1998 vp: 74.
[423] Suomen tietoturvallisuusstrategia 2016: 27.
[424] Pöysti 2000: 106.

hallintohenkilöstö voi siirtää oman toiminnan viivästyksiä tietojärjestelmien syyksi. Tietojärjestelmiin liittyvillä syillä ei voida perustella poikkeamista hyvän hallinnon viranomaismenettelyille asettamista vaatimuksista. Tällöin viranomaisen tulisi tietojärjestelmiänsä käyttäessään ja kehittäessään kiinnittää huomiota siihen, että järjestelmät mahdollistavat hyvän hallinnon turvaavat toimitavat.[425]

Tapauksessa **KKO 2005:3** ilmenee hyvin, kuinka viranomaiselle siirtyy vastuu sähköpostin vastaanottamisesta takaamalla omien tietojärjestelmiensä toimivuus tietojärjestelmähäiriöiden kohdalla:

> *Käräjäoikeuden käyttämä sähköpostipalvelin ei sähköpostijärjestelmän vian johdosta ottanut viestiä vastaan ja viesti jäi siten lopulta saapumatta. Viesti koski asianosaisen tyytymättömyyden ilmoitusta käräjäoikeuden ratkaisuun ja valitukselle oli siten asetettu määräaika. KKO:n ratkaisun mukaan sähköpostin osalta oli kuitenkin esitetty luotettava selvitys lähettämisajankohdasta, jonka vuoksi tyytymättömyyden ilmoitus hyväksyttiin ja alempien oikeuksien päätökset kumottiin. KKO:n ratkaisu perustui sähköisestä asioinnista viranomaistoiminnassa annetun lain (24.1.2003/13, asiointilaki) 10 §:n 2 momenttiin, jonka mukaan sähköinen viesti katsotaan saapuneeksi sinä ajankohtana, jona se on lähetetty, jos lähettämisajankohdasta voidaan esittää luotettava selvitys. Lähinnä säännös koskee sananmukaisesti vain tilanteita, joissa viesti on saapunut perille, mutta epäselvyyttä on sen saapumisajankohdasta. Vastaavaa periaatetta on kuitenkin perusteltua noudattaa myös, mikäli viranomaisen tiedonsiirtojärjestelmä on ollut epäkunnossa, mutta sekä viesti että sen lähettämisajankohta on sittemmin luotettavasti selvitetty*[426].

Ratkaisu edustaa mutkatonta suhtautumista sähköiseen asiointiin, jolloin sähköisestä asioinnista ei pyritä tekemään riskialtista, poikkeuksellista ja tiukoin edellytyksin hyväksyttävää. KKO:n ratkaisu perustunee myös ajatukseen, että viranomaisen on huolehdittava tiedonsiirtomenetelmiensä toimintakunnosta ja että viranomaisen tietojärjestelmän epäkuntoisuudesta johtuvan virheen ei tulisi vaikuttaa kielteisesti oikein toimineen asianosaisen asemaan.[427] Mikäli asianosainen voi esittää selvityksen lähetyksen toimittamisesta ajoissa viranomaisen tietojärjestelmään, järjestelmän asianmukainen toiminta viestin välittämisessä on viranomaisen vastuulla[428]. Ratkaisusta ilmenee, että lain säännös lähtee liikkeelle sähköisen viestinnän lähettäjävastuusta, mutta viranomaisen järjestelmävirheen vuoksi

[425] Saarenpää 2016a: 136–137; EOAK 537/2010: 6.
[426] Ks. KKO 2005:3, kohta 3.
[427] Turunen 2005: KKO:n ratkaisut kommentein 2005:I.
[428] Koponen 2017: 221.

vastuu viestin saapumisesta siirtyy vastaanottajaviranomaiselle[429]. Tyytymättömyyden ilmaisu hyväksyttiin, koska sähköisestä asioinnista viranomaistoiminnassa annetun lain eli asiointilain 10 §:n 2 momentin[430] mukaisesti sähköpostin osalta oli esitetty luotettava selvitys lähettämisajankohdasta. Kyseessä on asiointilain 8 §:n lähettäjän vastuu, jonka mukaan lähettäjä vastaa siitä, että viesti lähetetään viranomaisen ilmoittamaan osoitteeseen ja että se saapuu viranomaiselle määräaikaan mennessä[431]. Ratkaisu korostaa julkisen vallan positiivista velvollisuutta turvata perus- ja ihmisoikeuksien toteutuminen huolehtimalla järjestelmiensä riittävästä tietoturvallisuuden tasosta. Tietoturvallisuuden perinteisistä ulottuvuuksista[432] ratkaisun keskiössä on saatavuuden (käytettävyyden) turvaaminen. Tapauksesta ilmenee selvästi se, että perusoikeuksien toteutuminen on vahvasti kytköksissä myös kyberturvallisuuteen nykyisessä verkottuneessa ja järjestelmäkeskeisessä yhteiskunnassa: tietojärjestelmien tulee olla toimivia sekä niissä olevien tietojen luottamuksellisia, käytettävissä ja eheitä, jotta yksilöiden oikeudet eivät vaarannu.

Rinnasteinen ratkaisu sähköpostijärjestelmän vikaisesta toiminnasta on myös tapauksessa **KKO 2011:63**:

> *Käräjäoikeuden sähköpostipalvelin tulkitsi asianosaisen lähettämän valituksen roskapostiksi, jolloin valitus siirtyi käräjäoikeuden kirjaamoon vasta määräajan jälkeen. Asiointilain 10 §:n 2 momentin mukaisesti sähköpostiviestin otsikkokentän perusteella pystyttiin todentamaan lähetysaika, joka katsotaan myös viestin saapumisajaksi tietojärjestelmään eikä viesti ollut tällä perusteella myöhässä käräjäoikeuden oman järjestelmän virheestä johtuen.*

Tapaus korostaa oikean informaation merkitystä, sillä kysymyksessä oli toisaalta olemassa olevan tiedon tarkastaminen, ja toisaalta riittävän selvityksen hankkimisesta ratkaisun tueksi. Hovioikeus ei olisi saanut hyväksyä käräjäoikeuden päätöstä hankkimatta selvitystä valituksen saapumisesta tietojärjestelmiin etenkin, kun asianosainen oli tuonut ilmi seikkoja, jotka horjuttivat viestin

---

[429] Koulu 2012: 300.

[430] Sähköisestä asioinnista viranomaistoiminnassa annetun lain 10 §:n mukaan sähköinen viesti katsotaan saapuneeksi viranomaiselle silloin, kun se on viranomaisen käytettävissä vastaanottolaitteessa tai tietojärjestelmässä siten, että viestiä voidaan käsitellä. Jos saapumisajankohdasta ei ole selvitystä sen takia, että viranomaisen käyttämä sähköinen tiedonsiirtomenetelmä on ollut epäkunnossa, poissa käytöstä taikka selvitystä ei muusta vastaavasta syystä voida esittää, sähköinen viesti katsotaan saapuneeksi sinä ajankohtana, jona se on lähetetty. Tällöin lähettämisajankohdasta tulee pystyä esittämään luotettava selvitys.

[431] Voutilainen 2020: 230. Ks. myös Voutilainen 2023: 300–301.

[432] Ks. luku 2.2.1 (”Tietoturva”)

saapumisajankohtaa koskevan tiedon luotettavuutta.[433] KKO:n ratkaisu osoittaa myös, että viranomaisella on velvollisuus huolehtia tietojärjestelmien toimivuudesta. Viranomaisen on selvitettävä, johtuuko viestin saapumisen viivästyminen sen oman tietojärjestelmän toiminnan virheistä tai puitteista, mikäli viestin lähettäjä voi osoittaa oman tietokoneensa tietojen perusteella lähettäneensä viestin tiettyyn aikaan.[434] Näin ollen viestin lähettäjän vastuuseen eivät kuulu viranomaisen viestien vastaanottoon tarkoitetussa tietojärjestelmässä olevat häiriöt tai virhetoiminnallisuudet[435]. Viranomaisella katsotaan olevan myös vastuu roskapostitoiminnan asianmukaisuudesta[436]. Aikaisemmin mainitun perustuslain 21 §:n vaatimus koskien jokaisen yksilön oikeutta saada asiansa asianmukaisesti ja ilman aiheetonta viivästystä käsiteltyä viranomaisessa ei toteudu, jos järjestelmissä on häiriötä. Näin ollen on myös perusteltua, että valitus katsottiin saapuneen ajoissa.

Edellisiin esimerkkeihin verrattuna vastaavanlaiset taustat ovat myös ratkaisussa **KKO 2019:86**:

> *Tapauksessa sähköpostitse lähetetty valitus ei ollut saapunut määräajassa käräjäoikeuteen suuresta koostaan johtuen ja näin ollen käräjäoikeuden sähköpostijärjestelmä ei pystynyt vastaanottamaan viestiä liitetiedostoineen. Asiamies ei ollut saanut lähetyksestä vastaanottokuittausta, eikä muulloinkaan varmistanut viestin perillemenoa. Näin ollen KKO katsoi, että viestin jääminen saapumatta perille oli lähettäjän vastuulla.*

Siinä missä edellisiä KKO:n tapauksia 2005:3 ja 2011:63 yhdisti järjestelmävirhe tai -vika, tässä tapauksessa katsottiin sähköpostin myöhästymisen johtuvan sähköpostin kokorajoituksista, jolloin KKO katsoi kyseessä olevan ominaisuus eikä niinkään virhe tai vika.

Lähettäjän vastuuseen kuuluvat hänen oman toimintansa lisäksi hänestä riippumattomat virheet tai viipeet, jotka eivät ole niin poikkeuksellisia, ettei niihin olisi voinut varautua eikä viivästys johdu viranomaisen tietojärjestelmähäiriöstä. Näin ollen lähettäjän tulisi selvittää, onko vastaanottajaviranomainen ohjeistanut sähköisten asiakirjojen lähettämiseen liittyvistä teknisistä rajoitteista, sekä epäselvissä tilanteissa varmistaa sähköisen asiakirjan saapuminen perille.[437] KKO totesi, että laissa ei ole sääntelyä siitä, minkä suuruisia sähköposteja viranomaisen sähköpostijärjestelmän pitää kyetä vastaanottamaan. Lisäksi KKO:n mukaan yleisesti

433 Tornberg 2016: 293.
434 Lindfors 2011: KKO:n ratkaisut kommentein 2011:II.
435 Voutilainen 2022: 224.
436 Kulla & Salminen 2021: 75.
437 Voutilainen 2020: 230–231; Voutilainen 2023: 300–301; HE 17/2002 vp: 37–38, 41.

tunnettuna voidaan pitää sitä, että kaikissa sähköpostijärjestelmissä voi olla ominaisuutena liitetiedostojen kokorajoituksia. Tässä tapauksessa kokorajoituksesta oli myös ohjeistettu tuomioistuimissa asioivia oikeuslaitoksen verkkosivuilla. Kokorajaa (20 Mt) ei myöskään katsottu liian alhaiseksi, joten näin ollen käräjäoikeuden sähköpostijärjestelmää ei voitu pitää virheellisenä kokorajoituksen takia.[438] Ratkaisuun liittyy oletus hallinnon asiakkaiden kyvystä ymmärtää digitaalisissa palveluissa käytön rajoitteet tai tarpeellisten tahdonilmaisujen merkitys[439]. Valituksen perillemeno estyi tietoteknisestä syystä eikä kokorajoitus ollut välttämätön vaan lähinnä kustannuskysymys, mitä ei kuitenkaan otettu huomioon KKO:n ratkaisussa[440]. Vaikuttaisi siltä, että siinä, missä perusoikeuksien tosiallinen toteutuminen, edellytysten luominen oikeuksien käyttämiselle ja oikeuksien suojaaminen vaativat julkiselta vallalta aktiivisia toimenpiteitä, näillä aktiivisilla toimenpiteilläkin on hintalappunsa.

KKO:n ratkaisussa on huomioitu vain asiointilain 10 §:ssä mainittu tietojärjestelmän epäkuntoisuus tai häiriö, mutta jätetty valitettavasti ottamatta kantaa, mitä tarkoitetaan laissa käsitteellä ”muu vastaava syy” ja olisiko tietojärjestelmän riittämätön kapasiteetti voinut olla tämä muu vastaava syy. Lisäksi KKO:n väitteestä siitä, että kaikissa sähköpostijärjestelmissä voi olla kokorajoituksia ominaisuutena ja se olisi yleisesti tunnettua, puuttuu perusteltu dokumentaatio ja verifiointi. KKO:n kannanotto myös siihen, että sähköpostin kapasiteetin ollessa 20 megatavua ei ole liian alhainen, on perustelematon. Järjestelmän pitäisi pystyä vastaanottamaan laajan tapauksen liitetiedostoja, jotka voivat sisältää kapasiteetin nopeasti täyttäviä videoita tai muuta vastaavaa aineistoa.[441]

Toinen erikoinen seikka edellä mainitussa tapauksessa liittyi käräjäoikeuden sähköpostijärjestelmän kuittausominaisuuteen. Asiointilain 12 §:n 1 momentin mukaan viranomaisen on viipymättä ilmoitettava automaattisesti tai muutoin sähköisen asiakirjan vastaanottamisesta lähettäjälle. Järjestelmässä oli kuittausominaisuus, mutta asiamies ei ollut saanut viestin lähetyksestä sitä, eikä hän ollut omilla toimillaankaan pyrkinyt selvittämään viestin perillemenoa. KKO:n ratkaisun mukaan selvittämistoimia ei voida kuitenkaan pitää tarpeettomina yksin sillä perusteella, ettei asiamies ollut saanut lähetyksestään myöskään virheilmoitusta. Laissa ei ole säädetty velvollisuudesta virheilmoituksen lähettämiseen. Näin ollen KKO katsoi, että kantajat olivat laiminlyöneet huolehtia viestin perillemenosta.[442] KKO:n lausuma siitä, ettei laissa ole säädetty virheilmoituksen lähettämisen velvollisuudesta, on ongelmallinen. Automaattisen virheilmoituksen lähettäminen

[438] KKO 2019:86, kohta 20 ja 21.
[439] Voutilainen 2022: 227.
[440] Lehtonen 2021: 275–276.
[441] Lehtonen 2021: 276–277.
[442] KKO 2019:86, kohta 22 ja 23.

kuuluu niin ikään hyvän tavan käytänteisiin valtionhallinnon sähköpostijärjestelmien osalta. Joka tapauksessa virheilmoituksen puuttuminen ei vapauta lainoppinutta asiamiestä selvittämästä sähköpostin perillemenoa vastaanottokuittauksen puuttuessa.[443]

Asiointilaki korvasi lain sähköisestä asioinnista hallinnossa, jonka esitöiden perusteluissa on rinnastettu tietojärjestelmän kapasiteetin riittämättömyys ja toimintahäiriö. Näin ollen kapasiteetin riittämättömyyttä ja sähköpostin kokorajoitusta voidaan myös pitää asiointilain käsitteenä ”muu vastaava syy”. Muun muassa näitä seikkoja KKO ei ollut ottanut ratkaisussaan huomioon, minkä vuoksi ennakkopäätösarvo ei ole merkittävä. Olennainen huomioitava seikka joka tapauksessa on KKO:n ratkaisujen 2005:3 ja 2011:63 tavoin se, että sähköposti jäi saapumatta käräjäoikeuden sähköpostijärjestelmään valtionhallinnon sähköpostijärjestelmän vian takia. Viranomaisen tulee huolehtia perustuslain 21 §:ssä turvatusta oikeudesta muutoksenhakuun niin, että viranomaisen sähköpostijärjestelmässä ei ole perusoikeuden vaarantavaa puutetta tai virhettä.[444] Sähköpostijärjestelmän virheilmoituksen puuttuminen vaikuttaa eräänlaiselta järjestelmäpuutteelta, jolloin virheilmoituksen olemassaolo olisi voinut edesauttaa yksilön oikeuksien toteutumista. Lisäksi olennaista tapauksessa on se, että vaikka KKO:n toteaman mukaisesti käräjäoikeuden sähköpostissa ei olisi vikaa tai virhettä, kokorajoitus on ilmeisesti ollut myös eräänlainen puute, joka on haitannut perustuslain 21 §:ssä turvattua perusoikeutta muutoksenhakuun. Siitä huolimatta, olisiko KKO ottanut ratkaisussaan huomioon lain esityöt, KKO:n olisi tullut ratkaisussaan myös perusoikeusmyönteisesti punnita perusoikeuksien toteutumista. Perustuslain 21 §:n yksilön oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivästystä korostaa sekä viranomaisen järjestelmien tietoturvavaatimuksia että viranomaiselle asetettua vaatimusta tietojärjestelmien laadukkaasta ja häiriöttömästä toiminnasta.

Yhteenvetona todettakoon, että monesta perustuslain perusoikeudesta on johdettavissa yksilöiden oikeus turvallisuuteen kybertoimintaympäristössä. Yksilöiden oikeuksiin liittyy velvollisuuksia, joiden osalta perustuslaissa on nimenomaan vastuutettu julkista valtaa. Perustuslain 22 §:n mukaan julkisen vallan on turvattava perus- ja ihmisoikeuksien toteutuminen. Näin ollen julkisen vallan tulisi **turvata** edellä tässä tutkimuksessa mainittuja keskeisiä perusoikeuksia, kuten oikeutta turvallisuuteen sekä oikeutta omaisuuden, henkilötietojen ja luottamuksellisen viestin suojaan, myös kybertoimintaympäristössä. Esimerkiksi perustuslain 7 §:ssä turvattu oikeus henkilökohtaiseen turvallisuuteen korostaa julkisen vallan positiivisia toimintavelvoitteita muun muassa yhteiskunnan jäsenten

443 Lehtonen 2021: 278.
444 Lehtonen 2021: 279–281.

suojaamiseksi tieto- ja viestintärikoksilta. Yhtä lailla Euroopan ihmisoikeustuomioistuin on todennut ratkaisussaan **EIT 17.7.2008, I. V. Finland**, että valtion positiivisiin velvollisuuksiin kuuluu suojata henkilöiden yksityiselämää. Tietoturvallisuus ulottuu laajalti perus- ja ihmisoikeuksiin, ja nimenomaan tietoturvatoimenpiteillä turvataan yksilöiden oikeuksia verkottuneessa, järjestelmäriippuvaisessa yhteiskunnassamme. Jokaisella tulisi olla oikeus tietoturvaan kybertoimintaympäristössä, eli oikeus kyberturvaan, yhteiskunnan digitalisoituessa ja peruspalveluiden siirtyessä internettiin. Tähän liittyy oleellisesti myös perustuslain 21 §, jonka mukaan jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivästystä lain mukaan toimivaltaisessa viranomaisessa. Täten erityisesti viranomaisen tietojärjestelmille kohdistuu vaatimus laadukkaasta ja häiriöttömästä toiminnasta, mikä korostaa tietoturvan ulottuvuuksista erityisesti tiedon eheyttä ja käytettävyyttä. Tietoturvallisuus tietojärjestelmän ominaisuutena on kaikkine ulottuvuuksineen (*luottamuksellisuus, eheys ja käytettävyys*) eittämättä keskeinen keino turvata yksilöiden oikeuksia sähköisessä toimintaympäristössä[445].

Julkisella vallalla on myös positiivisia toimintavelvoitteita **edistää** kyberturvallisuutta nykyisessä järjestelmäriippuvaisessa verkkoyhteiskunnassamme. Tähän linkittyy edellä mainittujen pykälien ohella perustuslain 2 §, jonka mukaan julkisen vallan käytön tulee perustua lakiin ja julkisessa toiminnassa on noudatettava tarkoin lakia. Näin ollen tietoturvallisuuteen liittyvät viranomaisvastuut tulee perustua lakiin, kuten myös sellaiset tietoturvallisuuden ja verkkoyhteiskunnan keskeiset seikat, jotka olennaisesti vaikuttavat yksilöiden asemaan[446]. Perusoikeuksien turvaaminen verkottuneessa yhteiskunnassa ei tule kuitenkaan olla yksin julkisen vallan ”vastuulla”. Esimerkiksi on huomioitava, että yhteiskunnan sähköisten palveluiden tuottamiseen ja kehittämiseen osallistuu paljon muitakin organisaatioita kuin viranomaisorganisaatioita. Julkisen vallan positiivinen toimintavelvoite suojata yksilöitä ja edistää tietoturvaa yhteiskunnassa vaatii laajaa vaikuttavuutta ja tämä toteutuu tehokkaasti lainsäädännön avulla, jossa vähimmäisvaatimuksilla on mahdollista ulottaa tietoturvavaatimuksia laajemmin myös muihin organisaatioihin. Tietoturvan tulisi näyttäytyä koko yhteiskunnan vastuuna ja tämä tulisi ilmetä tietoturvan sääntelyjärjestelmästä: hyvä tietoturvan sääntelyjärjestelmä huomioi ja suojaa tehokkaasti perusoikeuksia.

---

445 Voutilainen 2019: 36–37, 201.
446 Pöysti 2000: 106

2.6 Tietoturvan sääntelyjärjestelmän keskeiset säädökset

2.6.1 EU-oikeuden tietoturvavelvoitteet

Tietomurto, kyberhyökkäys, palvelunestohyökkäys, tietojenkalastelukampanja ja identiteettivarkaus. Nämä ovat sanoja, jotka tulevat vastaan uutisissa lähes päivittäin. Teknologian kehitys ja sitä myöten yhteiskunnan digitalisoituminen ovat menneet viimeisen vuosikymmenen aikana hurjaa vauhtia eteenpäin, joten kehityksellä on myös kääntöpuolensa. Perinteinen rikollisuus on siirtynyt entistä enemmän verkkoihin. Uutisoinneissa nousee yhä enemmän esiin kansallisen turvallisuuden lisäksi organisaatioihin kohdistuneita kyberhyökkäyksiä sekä henkilötietojen tietoturvaloukkauksia. Pahimmillaan kyseiset uutiset vaikuttavat negatiivisesti organisaation nykyisten ja potentiaalisten asiakkaiden yritysmielikuvaan sekä asiakaskäyttäytymiseen, jolloin organisaation imago ja kilpailukyky saattavat kärsiä. Mainehaittojen lisäksi organisaatioille voi koitua myös suoria kustannuksia, kuten esimerkiksi tulojen menetysten lisäksi sanktioita. Tietoturvalainsäädännön kehitys on pyrkinyt pysymään teknologian ja digitalisaation kehittymisen perässä, mikä on huomattavissa erityisesti viimeisen 10 vuoden aikana kiihtyneestä EU-sääntelystä.

EU-oikeus voidaan jakaa sekä primääri- että sekundäärioikeuteen. Primäärioikeutta ovat esimerkiksi perussopimukset, jotka asettavat rajat toimivallalle sekä tavoitteita toiminnalle ja joiden perusteella on mahdollista antaa jäsenvaltioille velvoittavia EU-säädöksiä. Täten säädöksen antaminen edellyttää, että perussopimuksessa on määräys, johon säädöksen antaminen perustuu. Tähän liittyy kuitenkin toissijaisuusperiaate, jonka mukaan EU toimii ainoastaan, mikäli jäsenvaltiot eivät kykene saavuttamaan asetettuja tavoitteita riittävällä tavalla, vaan ne voidaan saavuttaa paremmin EU-tasolla.[447] EU:n tietoturva- ja tietosuojasäädöksissä lukeekin usein, että säädöksen tavoitteena on ”yhdenmukaistaa” tietoturva- ja tietosuojasääntelyä EU:ssa[448] tai esimerkiksi kehittää kyberturvallisuusvalmiuksia unionissa[449].

[447] Oikeusministeriön julkaisu 11/2012: 11, 15–16.
[448] Ks. esim. tietosuoja-asetuksen kohta 9–10, sekä CER-direktiivin kohta 1.
[449] Ks. NIS 2 -direktiivi kohta 1.

Tässä tutkimuksessa EU:n sekundäärioikeus on keskeisenä tarkastelukohteena. Sekundäärioikeudella tarkoitetaan EU:n toimielinten antamia oikeudellisesti sitovia säädöksiä, joita ovat asetukset, direktiivit ja päätökset[450].

Taulukko 2. EU:n sekundäärioikeuden velvoittavuus

Säädöstyyppi	Sitovuus[451]
Asetus, esim. tietosuoja-asetus (GDPR)	Asetukset ovat suoraan jäsenvaltioissa sovellettavaa lainsäädäntöä, jotka eivät edellytä muita toimenpiteitä kuin vähintään seuraamuksista säätämistä. Asetuksilla on välitön oikeusvaikutus eli kansalaiset voivat vedota niihin suoraan ja asetusta sovelletaan myös sellaisenaan kansallisissa tuomioistuimissa ja viranomaisissa.
Direktiivi, esim. NIS 1 -direktiivi ja NIS 2 -direktiivi	Direktiivit ovat jäsenvaltioille osoitettuja säädöksiä, joiden osalta jäsenvaltioiden on mahdollista käyttää harkintavaltaansa. Direktiivit edellyttävät toteuttamaan direktiivin toimenpiteet ja saattamaan kansallisen lainsäädännön direktiivin sisällön kanssa yhtenäiseksi. Näin ollen direktiivit eivät ole suoraan sovellettavissa niin kuin asetukset, vaan ne tulevat voimaan vasta kansallisen täytäntöönpanon jälkeen. Yleensä direktiivin säännöt sisällytetään lainsäädäntöön antamalla oma kansallinen säädös tai säännös sille. Jos kyseessä on vähimmäisdirektiivi (minimidirektiivi), direktiivistä tai sen yksittäisessä säännöksestä (minimisäännös) on säädetty vähimmäistaso. Tällöin kansallisesti pidemmälle menevät säännökset ovat mahdollisia. Täysharmonisoivassa direktiivissä (tai täysharmonisoivissa säännöksissä) säädetään EU:ssa noudatettavasta yhdenmukaisesta sääntelystä, johon lainsäädännölliset poikkeukset eivät ole mahdollisia.
Päätös, esim. Neuvoston puitepäätös 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä	Päätökset voivat olla osoitettuja yksityisylle taholle tai jäsenvaltiolle, mutta ne voivat olla myös yleisen säädöksen kaltaisia ilman, että päätöstä on osoitettu kenellekään. Päätökset ovat asetusten tavoin kaikilta osin velvoittavia. Yleensä päätökset ovat yksittäisiä ratkaisutapauksia hallinnollisissa menettelyissä. Jos päätös kohdistetaan jollekin tietylle taholle, päätös koskee ja velvoittaa vain tätä tahoa.

EU:n tietoturvaa koskeva lainsäädäntö on ottanut kehitysharppauksia kiihtyvällä tahdilla vuodesta 2001. Tällöin Euroopan neuvosto laati Budapestissa **tietoverkkorikollisuutta koskevan yleissopimuksen eli tietoverkkorikossopimuksen**, joka on ensimmäinen tietotekniikkarikoksia koskeva yleissopimus ja

[450] Sitovien säädösten lisäksi toimielimet voivat antaa myös suosituksia ja lausuntoja. Säädöstasoltaan korkeimpia ovat perussopimuksen nojalla annetut EU:n lainsäätäjien säädökset, kun taas alempitasoisia ovat niiden nojalla annetut säädökset, jotka yleensä ovat komission antamia. Ks. Oikeusministeriön julkaisu 11/2012, s. 11, 15–16.
[451] Oikeusministeriön julkaisu 11/2012: 17.

kyberrikollisuuden torjunnan kehittämisen perusta[452]. Yleissopimuksessa esitetiin kriminalisoitavaksi useat tietoverkkojen avulla tehdyt rikokset, jotka kohdistuvat datasiirron ja tietojärjestelmien luottamuksellisuuteen, eheyteen ja käytettävyyteen. Yleissopimus tuli kansallisesti voimaan syyskuussa vuonna 2007, kun eduskunta ja presidentti hyväksyivät sopimuksen.[453] Myöhemmin yleissopimusta on täydennetty kahdella lisäpöytäkirjalla[454] sekä täsmentävällä päätöksellä jäsenvaltioiden valtuuttamisesta ratifioimaan tietoverkkorikollisuutta koskevan yleissopimuksen toinen lisäpöytäkirja tiiviimmästä yhteistyöstä ja sähköisen todistusaineiston luovuttamisesta **2023/436/EU**.

Yleissopimuksen jälkeen Euroopan unionin neuvosto teki vuonna 2005 **puitepäätöksen (2005/222/YOS) tietojärjestelmiin kohdistuvista hyökkäyksistä**, jossa kriminalisoidaan laiton tunkeutuminen tietojärjestelmään, laiton järjestelmän häirintä ja laiton datan vahingoittaminen. Puitepäätöksessä on samoja määräyksiä kuin tietoverkkorikossopimuksessa ja molempien tarkoitus on sama: antaa suojaa yhteiskunnalle tietotekniikkarikoksia ja niiden aiheuttamia vahinkoja vastaan muun muassa yhtenäistämällä lainsäädäntöä, lisäämällä kansainvälistä yhteistyötä sekä laajentamalla rangaistussäännöksiä.[455]

Edellä mainittu puitepäätös korvattiin vuonna 2013 **direktiivillä tietojärjestelmiin kohdistuvista hyökkäyksistä eli tietoverkkorikosdirektiivillä (2013/40/EU)**. Direktiivissä esitettiin kriminalisoitavaksi puitepäätöksen tavoin laiton tunkeutuminen tietojärjestelmään, laiton järjestelmän häirintä ja laiton datan vahingoittaminen. Puitepäätökseen verrattuna direktiivi ottaa huomioon myös tietojen laittoman hankkimisen teknisin keinoin sekä rikosten tekemiseen käytettävät välineet, jotka tässä kontekstissa ovat direktiivissä täsmennettyjen rikosten tekemiseen suunnitellut tietokoneohjelmat ja tietojärjestelmään tai sen osaan pääsyn mahdollistava salasana, koodi tai muu vastaava tieto. Näin ollen direktiivin tehtävänä on ollut puuttua uusiin uhkakuviin, jotka liittyvät tietojärjestelmähyökkäyksiin. Direktiivillä on pyritty myös ottamaan käyttöön uusia rikosoikeudellisia seuraamuksia sekä edistämään oikeudellista yhteistyötä. Se sisältää lisäyksiä aiempiin instrumentteihin nähden, esimerkiksi säännöksiä bottiverkkoihin ja

---

[452] Suomen kyberturvallisuusstrategia 2013: 30; HE 153/2006 vp: 4; It-viikko.fi 2007.
[453] Ks. myös Melander & Rautio 2022: 1285.
[454] Ensimmäinen lisäpöytäkirja atk-järjestelmien avulla tehtyjen rasismiin tai muukalaisvihaan perustuvien tekojen kriminalisoimisesta on jo vuodelta 2003. Jälkimmäinen lisäpöytäkirja tiiviimmästä yhteistyöstä ja sähköisen todistusaineiston luovuttamisesta on vuodelta 2023, ja tämä pöytäkirja korostaa mm. sitä, että hallituksilla on velvollisuus suojella yhteiskuntaa ja yksilöitä rikoksilta paitsi verkon ulkopuolella myös verkossa. Pöytäkirja mahdollistaa tehokkaamman keinon hankkia tilaajatietoja ja liikennetietoja viranomaisten yhteistyön avulla, sekä tallennetun datan nopeutetun luovuttamisen menettelyn hätätilanteissa.
[455] HE 153/2006 vp: 4, 50; It-Viikko.fi 2007; Melander & Rautio 2022: 1285.

identiteettitiedon väärinkäyttöön liittyen. Tietoverkkorikosdirektiivin pohjalta keskeisimmät lakimuutokset tulivat rikoslakiin (laki rikoslain muuttamisesta 368/2015), jonka pohjalta myös muutettiin pakkokeinolakia ja poliisilakia. Rikoslain lisäykset tulivat 35 luvun 3 a–c §:ään koskien datavahingontekoa, törkeää datavahingontekoa ja lievää datavahingontekoa. Lisäys tuli myös rikoslain 38 luvun 9 a §:ään, jossa säädetään identiteettivarkaudesta. Muut konkreettiset muutokset olivat muun muassa enimmäisrangaistuksien korotuksia viestintäsalaisuuden loukkauksen (RL 38:3), tietomurron (RL 38:8) ja törkeän tietomurron osalta (RL 38:8a). Tietomurto kattaa myös pääsyn tietojärjestelmässä olevaan dataan ja tiedon hankkimisen siitä. Lisäksi törkeää tietoliikenteen häirintää (RL 38:6) ja törkeää tietojärjestelmän häirintää (RL 38:7b) koskevaan sääntelyyn lisättiin törkeää datavahingontekoa vastaavat kvalifiointiperusteet. Näiden tekojen enimmäisrangaistus on viisi vuotta vankeutta.[456]

Kuten voi päätellä, tietoturvaan liittyvä sääntely on kehittynyt paljonkin 2000-luvulla tietoverkkoihin ja -järjestelmiin kohdistuvien kyberuhkien kriminalisointien myötä. Huomioitava kuitenkin on se, että tietoturvavaatimuksia on kohdistunut ja kohdistuu edelleen organisaatioille henkilötietoja, yksityiselämää ja sananvapautta suojaavasta lainsäädännöstä ja sopimusvelvoitteista.

Yksi ensimmäisistä tällaisista sopimuksista on ollut vuoden 1950 **Euroopan ihmisoikeussopimus (EIS)**, jonka 8 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. EIS 10 artiklan mukaan jokaisella on oikeus sananvapauteen, joka sisältää oikeuden vastaanottaa ja levittää tietoja ja ajatuksia. **YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen sopimus (KP-sopimus)** vuodelta 1966 (Suomessa voimaan 1976) määrää 17 artiklassa, ettei kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon saa mielivaltaisesti tai laittomasti puuttua, ja jokaisella on oikeus lain suojaan tällaista puuttumista tai hyökkäämistä vastaan. Yhtä lailla sopimuksen 19 artikla turvaa sananvapautta. **Euroopan neuvoston yleissopimus nro 108 (tietosuojasopimus)** vuodelta 1981 oli puolestaan ensimmäinen tietosuoja-alan oikeudellisesti sitova kansainvälinen väline, jonka tarkoituksena on ollut turvata henkilötietojen automaattisessa tietojenkäsittelyssä jokaiselle yksilölle hänen oikeutensa ja perusvapautensa ja erityisesti hänen oikeutensa yksityisyyteen [457] . Myös vuonna 2000 juhlallisena

[456] HE 232/2014 vp: 3; LaVM 29/2014 vp: 1–2; Eduskunta 2015. Ks. myös Melander & Rautio 2022: 1285.

[457] Euroopan parlamentti 2024b.
OECD:n 1980 hyväksymä yksityisyyden suojaa ja kansainvälistä henkilötietojen siirtoa koskeva suositus eli tietosuojasuositus huomioitiin Euroopan neuvoston tietosuojasopimusta samanaikaisesti valmisteltaessa. Sekä OECD:n tietosuojasuositus sekä Euroopan neuvoston tietosuojasopimus ovat perusperiaatteiltaan samansisältöisiä. Ks. Alapuranen 2020, s. 15.

julistuksena julkaistu ja vuonna 2009 Lissabonin sopimuksen myötä hyväksytty **EU:n perusoikeuskirja** sisältää 7, 8 ja 11 artiklojen mukaisesti oikeuden yksityisyyteen, henkilötietojen suojaan ja sananvapauteen.

Vuonna 1995 hyväksyttiin **henkilötietodirektiivi (1995/46/EY)**, jonka sisältöön vaikutti Euroopan neuvoston tietosuojasopimus sekä OECD:n tietosuojasuositus. Yksityisyyden suojaan liittyviä säännöksiä sisältyy myös **sähköisen viestinnän tietosuojadirektiiviin (2002/58/EY)**.[458]

Suuria muutoksia nimenomaan organisaatioiden toimintaan on todennäköisesti aiheuttanut **EU:n yleinen tietosuoja-asetus (679/2016/EU) eli GDPR**, joka oli osa EU:n tietosuojauudistusta rikosasioiden tietosuojadirektiivin (680/2016/EU) kanssa. Tietosuojalainsäädännön myötä on tullut suoraan tietoturvaan liittyviä vaatimuksia organisaatioille, mutta myös tietosuojavaatimukset ovat epäsuorasti parantaneet organisaatioiden tietoturvaprosesseja ja -kypsyystasoa.

Ensimmäinen ehdotus kokonaisvaltaisesta tietosuojalainsäädäntöuudistuksesta tuli vuoden 2012 alussa, mutta itse sisällöstä päästiin sopuun vasta joulukuussa 2015. Tietosuojauudistus hyväksyttiin kokonaisuudessaan keväällä 2016. Sekä tietosuoja-asetus että rikosasioiden tietosuojadirektiivi tulivat sovellettavaksi 25.5.2018. Lainsäädäntöuudistus korvasi sekä henkilötietodirektiivin 1995/46/EY että tietosuoja-alan puitepäätöksen **2008/977/YOS**. Uudistuksen tarpeen taustalla oli riskilähtöinen ja teknologiariippumaton sääntely, joka huomioi tiedonkeruumenetelmien riskit ja uudet teknologiat, sekä velvoittaa henkilötietojen käsittelijöitä mitoittamaan suojausmekanismit käsittelyyn liittyvään riskiin nähden. Myöskään aikaisempi direktiivitasoinen sääntely ei riittävällä tasolla yhdenmukaistanut jäsenmaiden lainsäädäntöä.[459] Tietosuoja-asetuksen tarkoituksena on ollut henkilötietojen käsittelyyn liittyvien käytäntöjen yhdenmukaistaminen koko EU:ssa. Tietosuoja-asetus parantaa rekisteröityjen oikeuksia lisäten samalla sekä rekisterinpitäjien että henkilötietojen käsittelijöiden vastuita[460]. Tietosuoja-asetus koskettaa EU:n lisäksi sen ulkopuolella toimivia organisaatioita, jotka käsittelevät EU:n jäsenvaltioiden kansalaisten henkilötietoja[461]. Rikosasioiden tietosuojadirektiivi[462] ohjaa puolestaan EU:n viranomaisten henkilötietojen käsittelyä muun muassa rikosten tutkinnassa. Rikosasioiden tietosuojadirektiivin keskeisenä tarkoituksena on helpottaa henkilötietojen vaihtoa jäsenvaltioiden viranomaisten

[458] Alapuranen 2020: 15–16.
[459] VAHTI 1/2016: 6; Saarenpää & Riekkinen 2023: 179–180.
[460] Tietosuoja-asetus yhdistää tietoturvan rekisteröityjen oikeuksiin ja vapauksiin. Ks. Pöysti 2023, s. 43.
[461] VAHTI 1/2016: 6; HE 9/2018 vp: 1.
[462] Tutkimuksen fokuksen vuoksi rikosasioiden tietosuojadirektiivin käsittely on jätetty vähemmälle.

kesken sekä samalla taata johdonmukainen ja laadukas henkilötietojen suoja rikosasioita käsiteltäessä.[463] Eduskunta hyväksyi 13.11.2018 hallituksen esityksen pohjalta lain henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) sekä muut muutoslait, joilla saatettiin rikosasioiden tietosuojadirektiivi voimaan 1.1.2019.[464]

Tietoturvan osalta toinen merkittävä EU-tasoinen lainsäädännöllinen uudistus tietosuojauudistuksen ohella oli verkko- ja tietojärjestelmien riskienhallintaa ja varautumista sääntelevä **verkko- ja tietoturvadirektiivi eli NIS 1 -direktiivi (1148/2016/EU)**. Tätä uudistusta valmisteltiin yhtäaikaisesti EU:n yleisen tietosuoja-asetuksen kanssa. Euroopan parlamentin ja neuvoston asettama NIS 1 -direktiivi tuli voimaan 8.8.2016, ja se velvoitti jäsenvaltioita julkaisemaan direktiivin tavoitteisiin liittyvän lainsäädäntönsä kahden vuoden siirtymäajan puitteissa 9.5.2018 mennessä. NIS 1 -direktiivin tavoitteena oli lisätä verkko- ja tietojärjestelmien turvallisuutta koko EU:n alueella parantaen samalla kansallista varautumista.[465] NIS 1 -direktiivin katsotaan olevan ensimmäinen yleiseurooppalainen kyberturvallisuutta käsittelevä säädös. Direktiivin myötä jäsenvaltioiden tehtävänä oli määritellä tietoturvallisuuden varmistamiseksi ja riskien hallitsemiseksi tiettyjä viranomaistehtäviä. Tämän lisäksi jäsenvaltioiden oli velvoitettava myös keskeiset palveluntarjoajat tekemään riskienhallintatoimenpiteitä ja raportoimaan tietoturvapoikkeamista kansallisille viranomaisille. Suomessa oli jo ennestään asetettu tietyille, keskeisille palveluntarjoajille toimialakohtaisia määräyksiä, joihin NIS 1 -direktiivi toi muutoksia vain vähän. Näitä NIS 1 -direktiivin mukaisia toimialoja ovat olleet muun muassa energia-, finanssi-, terveydenhuolto-, liikenne-, ja juomavesihuoltoalat sekä digitaalisten infrastruktuurien ylläpitäjät. Riskienhallintatoimenpiteet ja tietoturvapoikkeamien raportointi koskivat myös digitaalisia palvelun tarjoajia, joita ovat olleet direktiivin mukaan esimerkiksi hakukoneet, sähköiset kauppapaikat ja pilvipalvelut.[466]

Euroopan unionissa käynnissä olleen kokonaisvaltaisen kyberturvallisuuden uudistuksen myötä Euroopan unioni on pyrkinyt myös vahvistamaan kyberturvallisuussääntöjään. Tämän tuloksena Euroopan unioni otti käyttöön kyberturvallisuuden sertifiointijärjestelmän, joka koskee tieto- ja viestintätekniikan palveluita, tuotteita ja prosesseja.[467] Näin ollen Euroopan parlamentti ja neuvosto hyväksyivät keväällä 2019 suoraan jäsenvaltioissa sovellettavan EU:n **kyberturvallisuusasetuksen (2019/881/EU)**, joka painottaa kriittisen infrastruktuurin sertifioimista ja takaa EU:n kyberturvallisuusvirastolle (ENISA) paremmat

[463] OM005:00/2017, VAHTI 1/2016: 6.
[464] HE 31/2018 vp: 1; OM005:00/2017; EV 113/2018 vp: 1–31.
[465] Andersson 2018: 8; Liikenne- ja viestintäministeriön julkaisuja 9/2017: 5.
[466] LVM037:00/2016; Andersson 2018: 8; Digitaleurope 2016.
[467] Eurooppa-neuvosto 2018.

resurssit[468]. EU:n kyberturvallisuusasetus on ollut myös keskeinen lakiuudistus tietoturvallisuuden osalta, sillä sen luoman EU:n laajuisen sertifiointikehyksen myötä asetus tulee parantamaan muun muassa tietojärjestelmien turvallisuutta. Osa pykälistä, jotka koskevat lähinnä kansallisen viranomaisen järjestäytymistä kyberturvallisuussertifioinnin osalta ja arviointilaitoksia, tulivat voimaan kahden vuoden siirtymäajan puitteissa kesäkuussa 2021.

Edellä mainittu NIS 1 -direktiivi kumottiin joulukuussa 2022 ja sen korvasi **kyberturvallisuusdirektiivi (2022/2555/EU) eli NIS 2 -direktiivi**. NIS 2 -direktiivin implementointiaika on 21 kuukautta, joten se on toimeenpantava kansalliseen lainsäädäntöön syksyllä 2024. NIS 2 -direktiivin rinnalla on yhtä aikaa valmisteltu **direktiiviä kriittisten toimijoiden häiriönsietokyvystä (2022/2557/EU) eli CER-direktiiviä**, joka tuli voimaan joulukuussa 2022 samalla siirtymäajalla kuin NIS 2 -direktiivi[469]. Siinä missä NIS 1 -direktiivi sääntelee verkko- ja tietojärjestelmien riskienhallintaa ja varautumista, NIS 2 -direktiivi keskittyy verkko- ja tietojärjestelmien kyberturvallisuusriskien hallintaan ja CER-direktiivi puolestaan enemmän varautumiseen ja häiriönsietokykyyn[470]. NIS 2 -direktiivi implementoidaan kansallisella kyberturvallisuuslailla. Tällöin NIS 1 -direktiivin täytäntöönpanosäännökset kumotaan sektorikohtaisista laeista. Lisäksi tiettyjä julkishallinnon toimijoita koskevat kyberturvallisuuden riskienhallintatoimenpiteiden ja niiden valvomisen vaatimukset implementoidaan säätämällä tiedonhallintalakiin uusi 4a-luku. Tiedonhallintalaki on erityislaki suhteessa esitettyyn yleislakiin, eli kyberturvallisuuslakiin.[471] Yhtä lailla CER-direktiivin täytäntöönpanosta annettiin hallituksen esitysluonnos lausuntokierrokselle tammikuussa 2024, jossa ehdotetaan säädettäväksi yleislaki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta[472].

Edellä kuvatun tietoturva- ja tietosuojalainsäädännön kehityksen ohella EU on painottanut toisessa digitaalistrategiassaan 2020–2030 turvallisia digitaalisia

---

[468] Euroopan parlamentin päätöslauselma RC-B8-0154/2019; Euroopan parlamentti 2019; Eurooppa-neuvosto 2020.

[469] Huomioitava on myös finanssialan digitaalista häiriönsietokykyä koskeva asetus (2022/2554/EU, ”DORA-säädös”), joka hyväksyttiin 28.11.2022. Tällä säädöksellä vahvistetaan lähinnä rahoitusalan toimijoiden eli pankkien, vakuutusyhtiöiden ja sijoituspalveluyritysten tietojärjestelmien turvallisuutta, joten se on rajattu spesifisti toimialakohtaisesti. Ks. Eurooppa-neuvosto 2022. Lisäksi ks. DORA-säädöstä koskeva hallituksen esitys HE 67/2024 vp, jossa on käsitelty mm. DORA-säädöstä täydentäviä kansallisia säännöksiä.

[470] NIS 2 -direktiivin sisältöä on eniten käsitelty luvussa 4.3 (”Sääntelyjärjestelmän verkko- ja tietojärjestelmien tietoturvariskien hallinta”). Myös CER-direktiiviä on luonnollisesti käsitelty tässä yhteydessä, mutta suppeammin tutkimuksen rajaukset varautumisen suhteen huomioon ottaen.

[471] HE 57/2024 vp: 1, 53, 61, 298, 301.

[472] Luonnos: Hallituksen esitys laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi.

ympäristöjä ja palveluita[473]. Digitaalistrategian lisäksi Euroopan komissio julkaisi vuonna 2020 Euroopan datastrategian (C 494/37) luodakseen kattavan ja selkeän datan sääntelykehyksen[474]. Näiden strategioiden myötävaikutuksesta syntyivät seuraavat säädökset: datanhallinta-asetus, digimarkkinasäädös, digipalvelusäädös, datasäädös, tekoälysäädös ja asetus eurooppalaisesta terveysdata-avaruudesta. Kaikki kyseiset säädökset ovat nimistä riippumatta asetuksia, mikä kuvastaa hyvin siirtymää direktiivitasolta asetustasolle, kun säädellään verkoista ja toiminnasta verkoissa[475].

> **Datanhallinta-asetus** eli asetus eurooppalaisen datan hallinnoinnista (2022/868/EU, Data Governance Act) tuli voimaan 3.6.2022 ja sen soveltaminen alkoi 24.9.2023. Datanhallinta-asetuksen ensisijaisena tavoitteena on lisätä datan saatavuutta ja yhtenäistää sen jakamista EU-alueella luomalla toimivat sisämarkkinat.[476] Datanhallinta-asetuksella on pyritty lisäämään datan saatavuuden lisäksi sekä datan uudelleenkäytettävyyttä että datan jakamista ja se on ollut digitaalistrategian ohella julkaistun Euroopan datastrategian (C 494/37) kulmakivi.[477] Asetuksessa muun muassa vahvistetaan edellytykset, jotka koskevat julkisen sektorin hallussa olevien tiettyjen datan luokkien uudelleenkäyttöä[478] unionissa, kuitenkaan vapauttamatta julkisen sektorin elimiä lainsäädännön mukaisista salassapitovelvoitteistaan. Asetus painottaa henkilötietojen suojaa koskevan oikeuden ja lainsäädännön soveltamista ensisijaisesti ristiriitatilanteissa, mikäli datassa käsitellään henkilötietoja. Uudelleenkäytön ehtona on 5 artiklan mukaisesti muun muassa se, että datan suojattu luonne on säilytettävä. Tällöin datan on oltava henkilötietojen osalta anonymisoitu sekä kaupallisesti luottamuksellisten tietojen ollessa kyseessä muutettu, koottu yhteen tai käsitelty millä tahansa muulla suojamenetelmällä. Lisäksi etäyhteyksin dataan käsiksi pääsy ja uudelleenkäyttö on oltava mahdollista ainoastaan julkisen sektorin elimen tarjoamassa tai valvomassa turvatussa käsittely-ympäristössä. Dataa voidaan käyttää ja uudelleen käyttää myös korkeiden turvallisuusvaatimusten mukaisesti fyysisissä tiloissa, joissa turvattu käsittely-ympäristö sijaitsee. Datanhallinta-asetus täytäntöönpano tuo

[473] Euroopan digitaalistrategia 2023: 1, 4–7.
[474] Sitra työpaperi 2022: 9.
[475] Saarenpää & Riekkinen 2023: 193.
[476] Valtiovarainministeriö 2023.
[477] Euroopan digitaalistrategia 2023: 4–7.
[478] Datanhallinta-asetuksen artiklan 2 mukaisesti uudelleenkäytöllä tarkoitetaan sitä, että luonnolliset henkilöt tai oikeushenkilöt käyttävät julkisen sektorin elinten hallussa oleva dataa kaupallisiin tai muihin kuin kaupallisiin tarkoituksiin. Lisäksi tällaiset tarkoitukset poikkeavat alkuperäisestä julkisesta tehtävästä, jota varten kyseessä oleva data tuotettiin. Tästä pois luetaan julkisen sektorin elinten välinen datan vaihto, jos se tapahtuu pelkästään näiden elinten julkisten tehtävien hoitamiseksi.

hallituksen esityksen HE 50/2023 myötä uusia viranomaistehtäviä, kuten asetuksessa tarkoitettuja rekisterinpito- ja valvontatehtäviä[479].

Digimarkkinasäädös eli asetus kilpailullisista ja oikeudenmukaista markkinoista digitaalialalla (2022/1925/EU, Digital Markets Act) tuli voimaan 1.11.2022 ja sen soveltaminen alkoi 6 kuukauden siirtymäajan puitteissa 2.5.2023. Digimarkkinasäädöksen tavoitteena on varmistaa kilpailulliset ja oikeudenmukaiset markkinat digitaalialalla sekä suojata yrityksiä ja kuluttajia EU:n sisämarkkinoiden ”portinvartioiden” eli suurten alustayritysten epäoikeudenmukaisiksi havaituilta käytänteiltä. [480] Asetusta sovelletaan ydinalustapalveluihin[481] ja asetuksen 2 artiklan määritelmän mukaan portinvartijalla tarkoitetaan ydinalustapalveluja tarjoavaa yritystä, jolla on merkittävä vaikutus sisämarkkinoihin, sen tarjoama ydinalustapalvelu on tärkeä yhdysväylä yrityskäyttäjille loppukäyttäjien tavoittamiseksi sekä sillä on vakiintunut ja kestävä asema toiminnassaan tai on ennakoitavasti tällainen asema lähitulevaisuudessa. Asetuksessa ei ole suoranaisia käytännön tietoturvavelvoitteita, jotka vaikuttaisivat organisaatioiden tietoturvatasoon. Tosin digimarkkinasäädöksen 8 artiklassa on täsmennetty, että portinvartioiden on varmistettava, että aikaisemmin artikloissa 5–7 asetetut toimenpiteet toteutetaan erityisesti tietosuoja-asetusta ja kyberturvallisuutta koskevan lainsäädännön mukaisesti.

Digipalvelusäädös eli asetus digitaalisten palvelujen sisämarkkinoista (2022/2065/EU, Digital Services Act) tuli voimaan pian digimarkkinasäädöksen jälkeen 16.11.2022 ja säädöksen soveltaminen alkoi 17.2.2024. Asetuksen tavoitteena on laittomaan sisältöön puuttuminen sekä lisätä huolellisuusvelvollisuuksia verkkoalustoille ja korotettuja velvollisuuksia erittäin suurille toimijoille.[482] Keskeisenä tarkoituksena on vahvistaa yhdenmukaiset säännöt välityspalvelujen tarjoamisesta sisämarkkinoilla. Asetusta sovelletaan välityspalveluihin, joita tarjotaan unionissa sijaitsevalle tai toimipaikan omaavalle palvelun vastaanottajalle. Välityspalvelulla tarkoitetaan asetuksessa tietoyhteiskunnan palvelua, joka on joko pelkkää siirtotoimintaa, välimuistiin tallentamista tai säilytyspalvelua. Asetuksen 5 jaksossa on keskitytty erittäin suurten verkkoalustojen ja erittäin suurten verkossa

[479] HE 50/2023: 1. Hallituksen esityksen mukaan rekisterinpito- ja valvontatehtävät koskevat datan välityspalveluita ja tunnustettuja data-altruismipohjaisia organisaatioita. Tehtäviin sisältyy myös mahdollisuus määrätä seuraamusmaksu. Näin ollen roolien osalta muutokset on tehty sähköisen viestinnän palveluista annettuun lakiin sekä uuden seuraamusmaksun takia sakon täytäntöönpanosta annettuun lakiin.
[480] Valtiovarainministeriö 2023.
[481] Työ- ja elinkeinoministeriö 2023. Ydinalustapalveluiksi luetaan asetuksessa esimerkiksi käyttöjärjestelmät, pilvipalvelut, hakukoneet, verkkoyhteisöpalvelut jne.
[482] Valtiovarainministeriö 2023.

toimivien hakukoneiden tarjoajien[483] lisävelvoitteisiin järjestelmäriskien hallitsemiseksi. Näiden toimijoiden on huolellisesti tunnistettava, analysoitava ja arvioitava järjestelmäriskit, joita aiheutuu unionissa niiden palvelujen ja niihin liittyvien järjestelmien suunnittelusta, toiminnasta ja niiden palvelujen käytöstä unionissa. Riskien arvioinnissa on 34 artiklan mukaisesti otettava vähintään huomioon järjestelmäriskit, kuten laittoman sisällön levittäminen näiden palvelujen kautta sekä mahdolliset tosialliset tai ennakoidut kielteiset vaikutukset kansalaiskeskusteluun, vaalimenettelyihin ja yleiseen turvallisuuteen sekä tällaiset vaikutukset, jotka liittyvät sukupuolittuneeseen väkivaltaan ja kansanterveyden sekä alaikäisten suojeluun, mistä on vakavia kielteisiä seurauksia henkilön fyysiselle ja henkiselle hyvinvoinnille. Lisäksi on huomioitava mahdolliset tosiasialliset tai ennakoidut kielteiset vaikutukset perusoikeuskirjan perusoikeuksien käyttämiseen. Näin ollen järjestelmäriskeissä ei ole suoraan tietoturvanäkökulmaa, kuten aluksi saattaisi luulla. Tosin perusoikeuskirjan 8 artiklassa vahvistettu henkilötietojen suoja ja tämän huomioiminen osana järjestelmäriskejä todennäköisesti sisältää myös tietoturvariskejä. Lisäksi digipalvelusäädöksen 35 artiklan mukaan erittäin suurten verkkoalustojen ja erittäin suurten verkossa toimivien hakukoneiden tarjoajien on otettava käyttöön riskien mitigointitoimenpiteitä, jotka voivat olla esimerkiksi sisäisten prosessien, resurssien, testauksen ja dokumentoinnin tai valvonnan tehostaminen järjestelmäriskin havaitsemiseksi. Vaikka asetuksessa ei ole suoranaisia, yleisiä tietoturvavelvoitteita organisaatioille, tällaiset mitigointitoimenpiteet parantavat varmasti tietoturvaa. Toki edellä mainitut vaatimukset, kuten aikaisemmin täsmennettiin, koskevat vain rajattua organisaatiojoukkoa. Digipalvelusäädöksen myötä kansallisella tasolla säädettiin laki verkon välityspalvelujen valvonnasta (18/2024), joka keskittyy pääosin toimivaltaisten viranomaisten valvontavastuisiin ja -toimenpiteisiin sekä hallinnollisiin seuraamusmaksuihin, mikäli digipalveluasetusta ei noudateta. Myös muihin jo voimassa oleviin säädöksiin tehtiin muutoksia, esimerkiksi sähköisen viestinnän palvelulaista kumottiin tietoyhteiskunnan palveluiden vastuuvapauksia koskevia säännöksiä[484].

[483] Digipalvelusäädöksen 33 artiklan mukaan *erittäin suurella* verkkoalustalla ja verkossa toimivalla hakukoneen tarkoitetaan sellaista, jonka unionissa olevien palvelun aktiivisten vastaanottajien kuukausittainen keskimäärä on vähintään 45 miljoonaa.

[484] Ks. HE 70/2023 vp, s. 1 ja 138–140. Digipalvelusäädöksen toimeenpano edellyttää myös täydentävien säännösten antamista asetuksen valvonnasta. Verkon välityspalvelujen valvontalain säätämisen lisäksi on muutettu kuluttajansuojaviranomaisten eräistä toimivaltuuksista annettua lakia, sähköisen viestinnän palveluista annettua lakia, Liikenne- ja viestintävirastosta annettua lakia, sakon täytäntöönpanosta annettua lakia ja oikeudenkäynnistä markkinaoikeudessa annettua lakia.

Datasäädös eli asetus datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (2023/2854/EU, Data Act) julkaistiin ehdotuksena[485] helmikuussa 2022 ja Euroopan parlamentti ja neuvosto hyväksyivät sen 27.11.2023[486]. Asetuksen tavoitteena on helpottaa erityisesti käyttäjien ja pienempien yritysten pääsyä dataan ja edistää kilpailua datamarkkinoilla[487]. EU:n datasäädöksessä keskitytään tuotteiden tai tuotteisiin liittyvän palvelun, esimerkiksi ohjelmiston, vaatimuksiin niiden sisältämän datan osalta. Keskiössä ovat kuluttajan oikeudet, mutta myös organisaationäkökulmasta datasäädös lisää oikeudellisen suunnittelun vaatimuksia datasäädöksessä tarkoitettujen tuotteiden ja palveluiden osalta[488]. Huomioitava on, että datasäädöksessä (kuten datanhallinta-asetuksessakin) keskiössä on data, informaation tai tiedon sijaan. Dataa tullaan keräämään ja hyödyntämään jatkuvasti yhä enemmän ja esimerkiksi datafuusion avulla datamassoja yhdistelemällä on mahdollista saada luotua uutta tietoa[489]. Käytännössä datasta pystytään muodostamaan merkityksellistä informaatiota ja informaatiosta tietoa[490]. Näin ollen EU:n dataa koskevat säädökset porautuvat tiedon alkujuureen eli (raaka)dataan, jolloin tarkoituksena on luoda yhdenmukaisia sääntöjä datan hallinnoinnille.

Tekoälyteknologioiden kehitystahti on kiihtynyt viime vuosina ja niiden käyttö eri muodoissaan on lisääntynyt, mikä on johtanut sääntelytarpeen kasvamiseen[491]. **Tekoälysäädös** eli asetus tekoälyä koskevista yhdenmukaistetuista säännöistä (2024/1689/EU, Artificial Intelligence Act) on eräänlainen vastaus sääntelytarpeeseen. Asetuksen tavoitteena on kieltää haitalliset tekoälykäytänteet sekä asettaa erityisvaatimuksia korkean riskin tekoälyjärjestelmille. Lisäksi EU:n tekoälyä koskevat säännöt toimivat globaalina suunnannäyttäjänä tekoälyä koskevalle sääntelylle ollessaan maailman ensimmäinen oikeudellisesti sitova kehys tekoälyn sääntelylle.[492] Huhtikuussa 2021 julkaistu ehdotus, ja jälkeenpäin 14.6.2023 tarkistettu

[485] COM (2022) 68 final.
[486] Eurooppa-neuvosto 2023.
[487] Euroopan digitaalistrategia 2023: 4–7; Valtiovarainministeriö 2023.
[488] Ks. esimerkiksi myöhemmin käsitellyssä luvussa 4.4 (”Järjestelmien oikeudellisen suunnittelun vaatimukset sääntelyjärjestelmässä”) CRA:n (kyberkestävyyssäädöksen ehdotusluonnos) tuomia tietoturvavaatimuksia, joissa keskitytään digitaalisia elementtejä sisältävien tuotteiden tietoturvaan. Näin ollen näkökulma datasäädöksen ja CRA:n välillä on eri, eli esimerkiksi datasäädös keskittyy vaatimuksissaan ohjelmiston vaatimuksiin siihen liittyvän datan osalta ja CRA puolestaan ohjelmiston tietoturvavaatimuksiin itsessään.
[489] Kosola 2016.
[490] Ks. lisää Finto.fi - Suomalainen asiasanasto- ja ontologiapalvelu 2024.
[491] Saarenpää & Riekkinen 2023: 122
[492] Valtiovarainministeriö 2023.

luonnos tekoälysäädöksestä [493] sisältää tietoturvanäkökulmasta kattavia vaatimuksia suuririskisten tekoälyjärjestelmien osalta. Esimerkiksi tekoälysäädöksen mukaan tällaisille suuririskisille tekoälyjärjestelmille on perustettava, pantava täytäntöön ja dokumentoitava riskienhallintajärjestelmä[494]. Lisäksi suuririskisissä tekoälyjärjestelmissä on mahdollistettava teknisesti tapahtumien automaattinen tallentaminen eli lokitus järjestelmän koko elinkaaren ajalta[495]. Tekoälysäädöksen sisällöstä viimein sovittiin 9.12.2023 ja parlamentti hyväksyi säädöksen 13.3.2024[496].

Asetus eurooppalaisesta terveysdata-avaruudesta (Regulation on the European Health Data Space, COM (2022) 197 final) tähtää myös sääntelyllään datan hallinnointiin. Euroopan komissio antoi 3.5.2022 ehdotuksensa asetuksesta, joka täydentää EU:n yleistä tietosuoja-asetusta ja jonka tarkoituksena on luoda eurooppalainen terveysdata-avaruus (EHDS) asettamalla sääntöjä, yhteisiä standardeja ja käytänteitä, rakenteita ja hallintamallin sähköisten terveystietojen ensisijaiselle käytölle ja toisiokäytölle. Asetuksen tarkoituksena on mahdollistaa, että terveystietoja voidaan välittää tietoturvallisesti EU-maiden välillä ja siten mahdollistaa hoidon jatkuvuus sekä kansainvälisen tieteellisen tutkimuksen, innovoinnin ja tietoon perustuvan päätöksenteon. Lisäksi sääntely luo kansalaisille lisää oikeuksia hallita ja määrätä terveystietojaan. Sääntelyn osalta on kuitenkin todettu, että tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin on kiinnitetty huomiota vain muutamilla suojatoimilla, jolloin kansallisella tasolla voisi olla mahdollista säätää paljon kattavammin erityyppisiä suojatoimia henkilötietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Perustuslakivaliokunta on myös esittänyt huolensa arkaluontoisten tietojen käsittelyyn liittyvistä uhkista, sillä tällaisia tietoja sisältäviin laajoihin tietokantoihin liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat muodostaa uhan henkilön identiteetille. Sääntelyyn tulisi lisätä esitettyä enemmän erilaisia tietoturvaa lisääviä suojatoimia. Valtioneuvosto myös katsoo, että itsearviointi ei ole riittävä keino varmistaa potilastietojärjestelmien tietoturvaa ja että siltä on perusteltua edellyttää jatkossakin korkeaa tasoa.[497] Myös myöhemminkin tätä vaatimusta ulkopuolisen toimijan tekemästä tietoturvallisuuden arvioinnista on korostettu kansallisella tasolla ja katsottu, että tietoturvallisuuden arviointilaitoksen tekemä

493 COM (2021) 206 final; P9_TA (2023)0236.
494 Tekoälysäädöksen 9 artikla.
495 Ks. lisää tekoälysäädöksen 12 artikla.
496 Euroopan parlamentti 2024a; Eurooppa-neuvosto 2024a.
497 U 61/2022 vp: 2–3, 15–16, 19, 22, 28–29.

> käytännön työ ja tarkastukset eivät ole korvattavissa[498]. Viimeisimpänä kehityksenä EU:n neuvosto ja Euroopan parlamentti ovat päässeet alustavaan yhteisymmärrykseen uudesta laista 15.3.2024, ja seuraavaksi neuvoston ja parlamentin on vielä vahvistettava yhteisymmärrys. Esimerkiksi alustavasti on sovittu muun muassa opt-out-mahdollisuudesta eli jäsenmaat voivat antaa mahdollisuuden kieltää tietojensa antamisen ensisijaiseen tai toissijaiseen terveystietojen käyttöön lukuun ottamatta tiettyjä yleisen edun mukaisia tarkoituksia.[499]

Muita keskeisiä tulevia EU-lainsäädäntöuudistuksia, joista on jo ehdotusluonnokset saatavilla, ovat sähköisen viestinnän tietosuoja-asetus (ePrivacy-asetus)[500] sekä digitaalisia elementtejä sisältävien tuotteiden tietoturvallisuutta parantava kyberkestävyyssäädös (CRA – Cyber Resilience Act)[501]. Huhtikuussa 2023 Euroopan komissio antoi myös ehdotuksen kybersolidaarisuutta koskevaksi säädökseksi (Kybersolidaarisuussäädös, COM (2023) 209 final), jonka tarkoituksena on kyberturvallisuuspoikkeamien valmiuden, havaitsemisen ja reagoinnin parantaminen sisältäen eräänlaisen kyberturvallisuuden hätämekanismin sekä Euroopan kyberturvallisuusjärjestelyn, joka koostuu turvallisuusoperaatiokeskuksista eri puolella EU:ta.[502]

Yhteenvetona voidaan todeta, että EU:n viimeisen vuosikymmenen sääntelyssä korostuvat yhteiskunnan trendeistä palveluiden digitalisoituminen, kyberuhkat sekä datan määrän kasvu, joita kaikkia on pyritty hallitsemaan sääntelyllä. Useissa alakohtaisissa Euroopan unionin säädöksissä on merkittäviä säännöksiä, jotka liittyvät kyber- ja tietoturvallisuuteen suoraan tai epäsuorasti yleisten riskinhallinta- ja vaatimustenmukaisuusvaatimusten kautta[503]. Lainsäädännön kehitys on ollut mullistavaa, koska aikaisemmin tietoturvaan liittyvä sääntely keskittyi erityisesti tietoverkkoihin ja -järjestelmiin kohdistuvien kyberuhkien kriminalisointiin. Lisäksi tietoturvavaatimuksia on tullut henkilötietoja ja yksityiselämää suojaavan

---

[498] StVL 2/2024 vp: 7. Ks. myös tietoturvan arvioinneista luku 4.4.5 (”Tietoturvan vähimmäisvaatimukset ja tietoturvatason arviointi”).
[499] Eurooppa-neuvosto 2024b.
[500] Ks. ehdotus sähköisen viestinnän tietosuoja-asetuksesta: COM (2017) 10 final. Asetuksen julkaisupäivä ja täydellinen sisältö eivät ole vielä tiedossa, mutta se kumoaisi sähköisen viestinnän tietosuojadirektiivin 2002/58/EY. Asetus tulee tulevaisuudessa todennäköisesti muuttamaan sähköisen viestinnän palveluista annetussa laissa (917/2014) säädettyjä organisaatioiden tietoturvavelvoitteita, joita on käsitelty myös tässä tutkimuksessa. Keväällä 2024 Euroopan unionin neuvosto on kehottanut komissiota tarkastelemaan sähköisen viestinnän tietosuojadirektiivin toimivuutta ja puutteita (Euroopan unionin neuvosto, EU:n digitaalipolitiikan tulevaisuus – Neuvoston päätelmät 21.5.2024: 9).
[501] COM (2022) 454 final. Kyberkestävyyssäädösehdotuksen (CRA) sisältöä on käsitelty yksityiskohtaisemmin tässä tutkimuksessa luvussa 4.4 (”Järjestelmien oikeudellisen suunnittelun vaatimukset sääntelyjärjestelmässä”)
[502] Euroopan komissio 2023.
[503] Pöysti 2023: 44.

lainsäädännön kautta. Nykyisin EU:n tietoturvasääntelyn painopiste on siirtynyt enemmän organisaatioihin kohdistuviin tietoturvavaatimuksiin, joiden myötä suuria muutoksia on tapahtunut organisaatioiden tietoturva- ja tietosuojatoiminnassa. Keskeisimpiä organisaatioiden tietoturvatasoa parantavia EU-säädöksiä ovat olleet erityisesti tietosuoja-asetus sekä NIS 1 ja 2 -direktiivit niiden asettaessa eniten vaatimuksia organisaatioiden tietoturvakäytänteisiin. Myös valmisteilla olevissa lainsäädäntöuudistuksissa keskiössä on edelleen kyberturvallisuuden korostaminen ja yksilöiden yksityisyyden suojaaminen.

EU:n kokonaisvaltaisen tietoturvasääntelyn vahvistaminen ja ripeä tahti ovat johtaneet käytännössä hajanaisen ja reaktiivisen sääntelyn ilmiöön kansallisella tasolla. Siinä missä EU reagoi toimintaympäristön muuttuviin uhkiin pyrkimällä lisäämään ja yhdenmukaistamaan vähimmäissääntelyä tietoturvan osalta, kansallisella tasolla reagoidaan muuttuvaan EU-sääntelyyn yhtä reaktiivisesti. Hajanainen ja reaktiivinen kansallinen tietoturvasääntely vaikeuttavat tietoturvaa koskevien säännösten tavoitettavuutta ja ymmärrettävyyttä. Tietoturvan sääntelyjärjestelmä näyttäytyy haastavana kokonaisuutena hahmottaa, mikä vaatii tietoturvan sääntelyjärjestelmän kokonaisvaltaista tuntemista. Seuraavaksi käsitelläänkin eri kansallisia säädöksiä, joissa tietoturvavaatimuksia ilmenee.

2.6.2 Kansallisen lainsäädännön tietoturvavelvoitteet

EU-lainsäädäntöuudistuksien myötä kansalliseen tietoturva- ja tietosuojalainsäädäntöön on tullut viime vuosina paljon muutoksia, jolloin tietoturvavaatimukset ovat hajaantuneet useaan eri säädökseen.

Vaikka aikaisemmin mainittua tietosuoja-asetusta sovelletaan sellaisenaan kaikissa EU-maissa, kansallisella tasolla päätettiin, että henkilötietolaki kumotaan ja otetaan käyttöön uusi tietosuojalaki (1050/2018) täsmentämään tietosuoja-asetusta. Muutoksia tehtiin myös rikoslakiin ja sakon täytäntöönpanosta annettuun lakiin. Tietosuojalaki ja muut lait hyväksyttiin eduskunnassa 13.11.2018, ja ne tulivat voimaan 1.1.2019.[504] Tietosuojalain lisäksi tulee huomioida ennen tietosuojalakia säädetty työelämän tietosuojalaki eli laki yksityisyyden suojasta työelämästä (759/2004), sillä se asettaa reunaehtoja organisaatioiden tietoturvavalvonnalle työntekijöiden henkilötietojen ja yksityisyyden osalta. Siinä missä työelämän tietosuojalaki on ”helposti lähestyttävä” sen työelämänäkökulman ja selkeän sisällön takia, kansallinen tietosuojalaki on sen sijaan muutamien yksityiskohtaisempien

[504] Eduskunta 2018a; HE 9/2018 vp:1.

täsmennysten kera varsin kevyt ja irrallinen säädös. Tietoturvavaatimusten osalta tietosuojalain 6 § on oleellisin[505].

Myös laki sähköisen viestinnän palveluista (917/2014) on yksi keskeinen tietoturvaan ja yksityisyyden suojaan liittyvä säädös. Säädöksessä tietoturvasta huolehtiminen on ulotettu koskemaan kaikkia viestinnän välittäjiä, jotka lain mukaan ovat teleyrityksien ja yhteisötilaajien lisäksi kaikki muut sellaiset tahot, jotka välittävät sähköistä viestintää muutoin kuin henkilökohtaisiin tai tavanomaisiin yksityisiin tarkoituksiin[506]. Keskeisiä säännöksiä ovat muun muassa 138 § (käsittely viestinnän välittämiseksi ja palvelun toteuttamiseksi sekä tietoturvasta huolehtimiseksi), 247 § (viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuus huolehtia tietoturvasta), 272 § (toimenpiteet tietoturvan toteuttamiseksi) sekä 18 luvun yhteisötilaajaa koskeva erityissääntely.

Alkuperäisen NIS 1 -direktiivin muutokset kohdistuivat hyvinkin reaktiivisesti sekä lakiin sähköisen viestinnän palveluista että useampaan toimialakohtaiseen säädökseen. Tätä tutkimusta varten tarkasteltuja toimialakohtaisia säädöksiä tietoturvallisuuden osalta ovat olleet muun muassa:

- vesihuoltolaki (119/2001)
- laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta (485/2004)
- laki liikennejärjestelmästä ja maanteistä (503/2005)
- alusliikennepalvelulaki (623/2005)
- laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023)
- vakuutusyhtiölaki (521/2008)
- laki eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista (629/2010, nimike muutettu lailla 720/2021)
- sähkömarkkinalaki (588/2013)
- laki luottolaitostoiminnasta (610/2014)
- ilmailulaki (864/2014)

[505] Ks. tietosuojalain 6 §:ään liittyen erityisesti luku 3.3.5 (”Muut tietosuojalainsäädännön tietoturvavaatimukset”.
[506] HE 221/2013 vp: 1, 92.

- laki liikenteen palveluista eli liikennekaari (320/2017)
- maakaasumarkkinalaki (587/2017)
- raideliikennelaki (1302/2018)

NIS 2 -direktiivin velvoitteet implementoidaan yleislakina toimivaan kyberturvallisuuslakiin, jolloin NIS 1 -direktiivin täytäntöönpanosäännökset kumotaan sektorikohtaisista laeista. Suomi teki poikkeavan ratkaisun NIS 1 -direktiivin täytäntöönpanossa noudatetun hajautetun sääntelytavan osalta, sillä merkittävä osa jäsenvaltioista otti käyttöön NIS 1 -direktiivin implementoinnin yhteydessä yhden kyberturvallisuuslain. Yhden lain malli nähdään nyt myös Suomessa kannattava NIS 2 -direktiivin implementoinnin suhteen, sillä se yhtenäistäisi kansallista kyberturvallisuussääntelyä sekä täyttäisi paremmin NIS 2 -direktiivin tavoitteen eli osoittaisi kyberturvallisuusvelvoitteiden vähimmäistason.[507] Hallituksen esityksen HE 57/2024 perusteella joitain tietoturvaan liittyviä vaatimuksia jää vielä toimialakohtaiseen lainsäädäntöön.

Tietoturvalainsäädäntöä esiintyy myös muissa kansallisissa säädöksissä, kuten esimerkiksi valmiuslaissa (1552/2011) ja huoltovarmuuspäätöksessä (1048/2018). Lisäksi on huomioitava kansallinen rikoslaki (39/1889). Tietojenkäsittelyn turvaaminen perustuu Euroopan neuvoston piirissä solmittuihin kansainvälisiin sopimuksiin. Kriminalisointi turvaa tietojenkäsittelyä asettamalla rangaistavaksi teoiksi keskeiset tietoturvauhat.[508] Näin ollen rikoslaki on myös keskeinen säädös tietoturvallisuuden kannalta. Rikoslain 38 luvussa on säädetty tieto- ja viestintärikoksista, jossa tietoturvaa loukkaavia rikoksia ovat muun muassa salassapitorikokset, viestintäsalaisuuden loukkaukset, tietoliikenteen häirintä, tietojärjestelmän häirintä, tietomurto, suojauksen purkujärjestelmärikos ja tietosuojarikos.

Tietoturvaan liittyviä lainsäädännön vaatimuksia on kehitetty vuosien saatossa keskittyen suuresti viranomaisiin, vaikka linkittyneessä verkkoyhteiskunnassa tulisi ottaa myös muut organisaatiot kattavasti huomioon, jotta tietoturvan toteutuminen olisi kattavampaa koko yhteiskunnassa[509]. Huomioitava on kuitenkin se, että viranomaisen tietoturvavaatimukset heijastuvat usein myös muihin organisaatioihin, kuten viranomaisen järjestelmätoimittajiin ja muihin sopimuskumppaneihin. Viranomaisen tietoturvan vähimmäisvaatimukset lainsäädännössä ovat hyvä esimerkki teknologianeutraalista vähimmäistasosääntelystä.

---

[507] HE 57/2024 vp: 123–124.
[508] Neuvonen 2019: 326–327.
[509] Tutkimuksesta on rajattu pois julkisen sektorin tietojen käsittelyn vaatimusten yksityiskohtainen tarkastelu. Ks. luku 1.3 (”Tutkimuksen rajaukset”).

Julkisen hallinnon tiedonhallintaa koskevien säädösten keskittämiseksi on säädetty tiedonhallintalaki (906/2019). Tämä viranomaisen tiedonhallintaa koskevan yleislain yksi keskeinen osa-alue on tietoturvallisuusvaatimukset, jotka kuvastavat tietoturvan vähimmäistasoa julkisessa hallinnossa. Tiedonhallintalaki on korvannut julkisen hallinnon tietohallinnon ohjauksesta annetun lain säännökset sekä viranomaisen toiminnan julkisuudesta annetun lain hyvää tiedonhallintotapaa koskevat säännökset: muun muassa julkisuuslain 18 § kumottiin kokonaan ja julkisuusasetuksesta jäi voimaan 2a luku. Lakiuudistus kumosi tai muutti myös joitain viranomaisen toiminnan julkisuudesta annetun lain, sähköisestä asioinnista viranomaistoiminnassa annetun lain ja eräiden muiden lakien säännöksiä.[510] Tietoturvallisuusasetus (TTA 681/2010), jossa käsiteltiin viranomaisen tiedon tietoturvallisia käsittely- ja riskienhallintavaatimuksia, korvattiin myös tiedonhallintalain myötä. Tällöin kansallisen salassa pidettävän tietoaineiston luokittelu muuttui ja tietoturvatasot poistuivat, jolloin tilalle tuli tietoturvallisuuden vähimmäistaso. Päivitetyt säännökset tukeutuvat enemmän riskienhallintaan, jolloin muun muassa johto velvoitetaan vastaamaan jäännösriskien hyväksymisestä.[511] NIS 2 -direktiivin toimeenpano julkishallinnon kyberturvallisuusvelvoitteiden ja niiden valvonnan osalta toteutetaan tiedonhallintalain 4a-luvulla, jolloin tiedonhallintalaki on erityislaki suhteessa yleislakina toimivaan kyberturvallisuuslakiin[512].

Viranomaisen sääntelyn osalta on huomioitava myös tietoturvavaatimuksia sisältävä laki digitaalisten palvelujen tarjoamisesta (306/2019, digipalvelulaki), jolla on pantu täytäntöön Euroopan parlamentin ja neuvoston saavutettavuusdirektiivi (2016/2102/EU). Lain keskeisenä näkökulmana on viranomaisen digitaaliset palvelut ja sen tarkoituksena on edistää muun muassa digitaalisten palvelujen tietoturvallisuutta, saatavuutta ja sisällön saavutettavuutta ja siten parantaa jokaisen yksilön yhdenvertaisuutta käyttää digitaalisia palveluita[513].

Kansallinen tietoturvalainsäädäntömme on ollut hajanaista. Hajanaisuus vaikeuttaa tietoturvan sääntelyjärjestelmän kokonaiskuvan muodostamista, mikä aiheuttaa haasteita sen tavoitettavuudelle ja ymmärrettävyydelle. Lainsäätäjät eivät myöskään ole aikaisemmin nähneet tarvetta säätää erityistä tietoturvalakia, mikä

[510] HE 284/2018 vp: 1, 8, 34; PeVL 73/2018 vp: 5.
[511] Valtiovarainministeriö 2018.
[512] NIS 2 -direktiivistä johtuvaa tiedonhallintalain sääntelyä sovelletaan rajatumpaan joukkoon kuin tiedonhallintalain 4 luvun tietoturvallisuussääntelyä sovelletaan. Lähtökohtana on direktiivin vähimmäistason täyttäminen. Ks. HE 57/2024 vp, s. 53.
[513] Digipalvelulaissa on vahva julkisen sektorin näkökulma: viranomaisen on suunniteltava ja ylläpidettävä digitaaliset palvelunsa varmistaen tietoturvallisuus ja tietosuoja sekä löydettävyys ja helppokäyttöisyys.

on osaltaan vaikeuttanut käytännön tietoturvatyön toteutumista[514]. Johdonmukaisella ja yhtenäisellä tietoturvasääntelyllä parannettaisiin tietoturvasäännöksien tavoitettavuutta ja ymmärrettävyyttä. Tällöin sääntely näyttäytyisi myös hyvän tietoturvatavan mukaisesti kohtuullisena ja oikeudenmukaisena.[515] Näistä syistä johtuen tavoitettavuuden ja ymmärrettävyyden ohella johdonmukaisuus ja yhtenäisyys ovat keskeisiä kriteerejä hyvälle tietoturvan sääntelyjärjestelmälle, jotta se olisi hyvä.

Yhteenvetona voidaan todeta, että keskeisimpiä organisaatioiden tietoturvaan vaikuttavia kansallisia säädöksiä ovat kansallinen tietosuojalaki ja työelämän tietosuojalaki sekä sähköisen viestinnän palveluista annettu laki. Näiden lisäksi tulee huomioida toimialakohtaisesta lainsäännöstä tulevat tietoturvavaatimukset sekä muun muassa NIS 2 -direktiivin toimeenpaneva kansallinen kyberturvallisuuslaki. Osana organisaatioiden tietoturvan sääntelyjärjestelmää on tärkeää huomioida myös rikoslaki, koska siinä on säädetty muun muassa tieto- ja viestintärikoksista. Lainsäädännössä ilmenevää hyvää tietoturvatapaa ja hyviä käytänteitä vertailtaessa on mahdollisesti tukeuduttava myös viranomaisen tiedonhallintalakiin hyvänä esimerkkinä tietoturvan vähimmäisvaatimusten teknologianeutraalista sääntelystä.

Nykyinen organisaatioiden tietoturvan sääntelyjärjestelmä ilmentää hajanaista tietoturvasääntelyä, joka vaatii lainsäädännön kokonaiskuvan hallintaa. Lisäksi nykyinen tietoturvan sääntelyjärjestelmä näyttäytyy reaktiivisena, koska kansallisella tasolla meillä ei ole ollut yhtä kattavaa tietoturvalakia ja EU-sääntelyn myötä uudet lakimuutokset joudutaan huomioimaan usein jopa toimialakohtaisesti. Hajanainen ja reaktiivinen sääntely aiheuttaa sen, että tietoturvaa koskevat säännökset saattavat vaikeuttaa käytännön työtä ja tietoturvalainsäädäntö on vaikeasti tavoitettava erityisesti tietoturvan osalta epäkypsemmille organisaatioille ja yrittäjille. Esimerkiksi laki sähköisen viestinnän palveluista sisältää keskeisiä tietoturvavaatimuksia, mutta jo säädöksen nimi itsessään ei viittaa millään tavalla tietoturvaan. Kaikki nämä seikat johtavat siihen, että nykyinen tietoturvalainsäädäntö ei suojaa tehokkaasti perusoikeuksia. Kansallinen tietoturvaa koskeva lainsäädäntö tulee kehittymään jatkuvasti pysyäkseen teknologian kehittymisen, yhteiskunnan digitalisoitumisen sekä uudistuvan EU-lainsäädännön perässä. Muuttuva toimintaympäristö ja sen uudet uhkat vaativat teknologianeutraalin lainsäädännön rinnalle hyviä käytänteitä, jotta lainsäädäntö pysyisi proaktiivisempana.

---

[514] Laaksonen, Nevasalo & Tomula 2006: 21, 27.
[515] Ks. luku 1.5 (”Hyvä tapa tietoturvan sääntelyjärjestelmän elementtinä”), jossa on myös käsitelty hyvän sääntelyjärjestelmän elementtejä hyvyyden osalta.

2.7 Tietoturvan sääntelyjärjestelmä ja hyvät käytänteet

Erinäiset tietoturvaviitekehykset[516] ja -ohjeistukset toimivat organisaatioille työkaluina hyvien käytäntöjen tunnistamiselle sekä tietoturvan vähimmäistason toteuttamiselle. Esimerkiksi hyviä tietoturvakäytänteitä ovat ohjanneet pitkään kansallisella tasolla VAHTI-tietoturvaohjeet, joita on hyödynnetty tietoturvatyössä muun muassa elinkeinoelämässä, yrityksissä ja kunnissa[517]. Nyttemmin VAHTI-ohjeet ovat pitkälti lainsäädännön muutoksien myötä vanhentuneet, ja niitä ei enää ole aikaisemmassa sijainnissaan saatavilla[518]. Toisena esimerkkinä kansallisista toimijoista on huomioitava tietosuojavaltuutetun toimiston julkaisemat tietosuojaa koskevat ohjeistukset ja linjaukset, jotka ovat myös oleellisia hyvien tietoturvakäytänteiden sekä tietoturvan kehittämisen ja ylläpitämisen kannalta[519]. Nämä liittyvät pitkälti Euroopan tietosuojaneuvoston (*EDPB – European Data Protection Board*) ohjeisiin ja suosituksiin sekä ennen tietosuojaneuvoston perustamista yhteistyöelimenä toimineen WP29-työryhmän ohjeistuksiin[520].

Edellä mainittujen ohjeistuksien lisäksi keskeisiä ohjeistuksia tai suosituksia tietoturvan osalta julkaisee Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus sekä valtiovarainministeriön tiedonhallintalautakunta. Suomalaisia organisaatioita ohjeistavia tahoja ja ohjeistuksia on varsin paljon sekä ohjeistuksissa käytetty termistö on kirjavaa, mikä tekee ohjeistuksien huomioimisesta ja toteuttamisesta haastavaa[521].

Valtaosa kansallisista tietoturvan viitekehyksistä sekä ohjeistuksista ja suosituksista ovat käytännesääntöjä. Käytännesäännöillä pyritään määrittelemään yhteiset toimintatavat, torjumaan alan yksityiskohtainen sääntely laissa tai tuomaan lisäselvyyttä lain aukkokohtiin[522]. Käytännesääntöjä on myös kuvattu soft law -tyyppiseksi aineistoksi, joilla tarkoitetaan pääsääntöisesti määräyksiä ilman

[516] Esimerkiksi auditointi- ja arviointikriteeristöt.
[517] Ks. Valtiovarainministeriö 2017a ja 2017b. VAHTI-ohjeiden keskeisenä tekijätahona toimi valtiovarainministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI.
[518] Suomidigi 2023. Ks. myös Saarenpää 2016a, s. 143: VAHTI-ohjeistuksilla ei ole aikaisemminkaan ollut erityistä lainsäädännöllistä asemaa.
[519] Tietosuojavaltuutetun toimiston päätehtävänä on valvoa henkilötietojen käsittelyn lainmukaisuutta sekä siihen liittyvän tietosuojaoikeuksien ja lainsäädännön toteutumista. Tämä toteutuu muun muassa edistämällä henkilötietojen käsittelyyn liittyvää tietoisuutta, tekemällä tarkastuksia ja selvityksiä sekä määräämällä mahdollisia hallinnollisia seuraamuksia, antamalla lausuntoja henkilötietojen käsittelyyn liittyvistä rikoksista ja lainsäädännöllisistä uudistuksista sekä hyväksymällä käytännesääntöjä ja vakiosopimuslauseita. Tietosuojavaltuutetun toimisto myös vastaanottaa ilmoituksia ja pyyntöjä henkilötietojen käsittelyyn liittyvistä epäkohdista, tietosuojavastaavista ja tietoturvaloukkauksista. Ks. Tietosuojavaltuutetun toimisto 2019a.
[520] Euroopan tietosuojaneuvosto 2024; Tietosuojavaltuutetun toimisto 2024.
[521] Kinnunen 2015: 156–157.
[522] Riekkinen 2016b: 377.

oikeudellista sitovuutta[523]. Soft law itse käsitteenä on ristiriitainen, sille ei ole vakiintunutta suomenkielistä vastinetta ja sillä voi olla eri tilanteissa täysin eri merkitys, jolloin sen määritteleminen yleisellä tasolla on vaikeaa. Joka tapauksessa soft law mahdollistaa joustavan, muuttuneen tilanteen vaatiman tulkinnan. Yksi tunnistettu soft law -ryhmä muodostuu erilaisista hallinnollisista ohjeista, suunnitelmista, toimintaohjelmista, suosituksista ja vastaavista, jotka ovat tulleet lainsäätäjän hyväksymän lain sijaan tai sen rinnalle helpon ”säätämis”-menettelyn vuoksi.[524] Näin ollen tietoturvaan liittyvät käytännesäännöt kategorisoituvat tähän ryhmään. Soft law voi olla viranomaispohjaista, mutta se voi olla myös itsesääntelyä ja itsesääntelyyn pohjautuvia ammattieettisiä ohjeita[525].

Soft law -käytännesäännöt ovat ikään kuin kertomuksia lain sisällöstä, sillä niiden avulla välitetään lakitekstiä yksityiskohtaisemmalla tavalla ohjeita. Käytännesäännöt on nähty kuitenkin ongelmallisina, koska niihin ei liity laintasoista velvoittavuutta eikä niiden noudattamatta jättämisestä aiheudu sanktioita. Jotta käytännesäännöt yltäisivät tehokkuudeltaan lain tasolle, niiden tulisi olla sovellettavissa kaikkiin alan toimijoihin.[526] Näiden keskeisten eroavaisuuksien lisäksi lakia toteutetaan ja valvotaan suoraan viranomaisten toimesta, jolloin soft law -ratkaisuja (kuten käytännesääntöjä) noudattavien osapuolien on nähty olevan alttiita epätasapuolisemmalle kohtelulle[527]. Esiin nostetut ongelmallisuudet painottavat juridista näkökulmaa, mutta asiaa voi tarkastella myös käytännön toiminnan kannalta. Tästä näkökulmasta käytännesäännöt eivät ole niin ongelmallisia tai epätasapuolisia, vaikka niihin ei liittyisikään suoraan laintasoista velvoittavuutta. Huomioitava on, että usein käytännesääntöjen noudattaminen on luottamusta lisäävä tekijä sopimusosapuolten ja muiden toimijoiden välillä. Näin ollen ei ole tavatonta, että esimerkiksi hankinnoissa tarkastetaan kilpailutusvaiheessa organisaatioiden hankkimat sertifioinnit ja noudattamat käytännesäännöt, taikka jopa vaaditaan käytännesääntöihin pohjautuvia tietoturva-arviointeja luottamuksen lisäämiseksi sekä organisaation tai palvelun tietoturvatason todentamiseksi. Tästä näkökulmasta käytännesäännöt ovat varsin tehokkaita ja niiden noudattamatta

[523] Riekkinen 2016b: 377; Voutilainen 2006a: 32.
[524] Nieminen 2020: 1082, 1084–1085; Korkea-aho 2005: 73–74. Korkea-aho on myös kategorisoinut soft law:n neljään ryhmään: ensimmäinen ryhmä on täydentävä soft law eli esimerkiksi viranomaisten antamia suosituksia, toinen ryhmä on sopeuttava soft law, kolmas ryhmä on kilpaileva soft law ja neljäs ryhmä on korvaava soft law, jolla korvataan kovan sääntelyn eli ”hard law:n” puutetta (ks. myös Korkea-aho 2005, s. 73–79).
[525] Nieminen 2020: 1086–1087. Ammattieettisiä ohjeita on myös käsitelty osana lukua 1.5 (”Hyvä tapa tietoturvan sääntelyjärjestelmän elementtinä”).
[526] Korja 2016b: 435, 437.
[527] Wahlgren 2018: 161. Esimerkiksi ammattikuntien eettiset ohjeet eivät ole lakeja, vaan ne ovat tarkoitettu noudatettavaksi eettisistä syistä ja oikeudellista velvoittavuutta ohjeiden noudattamiseen ei ole (Nieminen 2020: 1092). Tällöin toki kannustimena on etiikan mukaisesti toimiminen ja ”pelotteena” on ammattikunnasta erottaminen.

jättäminen saattaa johtaa jopa palveluiden käyttämättömyyteen ja sopimuksien purkamiseen, mikäli tietoturvataso ei vastaa sitä, mitä on sopimuksella sovittu.[528]

Yhtenä esimerkkinä käytännesäännöistä on tietoturvan viitekehyksenä toimiva kansallinen tietoturvallisuuden auditointikriteeristö Katakri 2020, jota on myös tässä tutkimuksessa tarkasteltu. Katakri on valittu esimerkkiviitekehykseksi tähän tutkimukseen hyvien tietoturvakäytänteiden osalta sen selkeän rakenteen ja tunnettavuuden vuoksi, vaikkakin keskeinen Katakrin näkökulma on viranomaisten tietojen suojaaminen. Toinen syy on se, että Katakri 2020 on päivitetty uusiutuneen kansallisen lainsäädännön, lähinnä tiedonhallintalain mukaan. Tällöin sen voisi nähdä täydentävänä soft law'na aivan kuten tiedonhallintalakia täydentävä *Suositus tietoturvallisuuden vähimmäisvaatimuksista*[529].

> Katakria käytetään apuna organisaatioiden turvallisuuden kehittämisessä sekä arviointityökaluna, jolla arvioidaan organisaatioiden kyvykkyyttä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Näin ollen Katakri ei itsessään aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siinä kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja kansainvälisiin tietoturvallisuusvelvoitteisiin. Lisäksi Katakri antaa toteutusesimerkkejä hyviin tietoturvallisiin käytänteisiin liittyen. Katakri 2020 perustuu lakiin julkisen hallinnon tiedonhallinnasta (906/2019) ja valtioneuvoston asetukseen asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019).[530]

Katakrin rinnalle on kehitetty pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) [531] sekä julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)[532], jossa on myös tietosuojan vähimmäisvaatimuksia. Kyseiset kriteeristöt ovat hyviä esimerkkejä tyypillisistä soft law -tyyppisistä käytännesäännöstöistä, jotka eivät ole sinällään sitovia, mutta taustalta on muun muassa laintasoisena velvoitteena viranomaisen tiedonhallintalaki. Käytännön työssä moni tietoturva-ammattilainen on pitänyt Julkria ja PiTuKria selkeämpänä ja yksinkertaisempana vaihtoehtona kuin Katakri. Huomioitava kuitenkin on, että Katakri on näistä edelleen ainoa kriteeristö, jota hyväksytyt tietoturvan arviointilaitokset voivat virallisesti arvioida.

---

[528] Ks. myös lisää luvusta 4.4.5 (”Tietoturvan vähimmäisvaatimukset ja tietoturvatason arviointi”).
[529] Valtiovarainministeriön julkaisuja 2024:19.
[530] Andersson 2018: 4; Katakri 2020: 5.
[531] Traficomin julkaisuja 13/2020.
[532] Valtiovarainministeriön julkaisuja 2023:46.

Edellä mainittujen viitekehyksien rinnalla on muitakin tietoturvallisuuden ja tietoturvariskien hallinnan viitekehyksiä, joita käytetään organisaatioissa tietoturvan kehittämisessä ja arvioinnissa. Siten ne lisäävät organisaatioiden hyviä tietoturvakäytänteitä ja parantavat siten organisaatioiden tietoturvallisuutta. Tästä esimerkkinä ovat kansainväliset ISO-standardit.

> ISO (International Organization for Standardization) on kansainvälinen, itsenäinen standardisoimisliitto, jolla on 162 kansallista jäsentä[533]. Suomen Standardisoimisliitto SFS ry on ISO:n jäsen ja standardisoinnin keskusjärjestö, jonka tehtävänä on muun muassa koordinoida kansallista standardisoimistyötä[534]. ISO-standardeja on valtava määrä, mutta kolme keskeisintä tietoturvallisuuden ja riskienhallinnan osalta ovat tietoturvallisuuden hallintajärjestelmän vaatimuksia koskeva standardi ISO/IEC 27001:2022 [535] , organisaation tietoturvariskien hallinnan standardi ISO/IEC 27005:2018 [536] sekä riskienhallinnan standardi ISO 31000:2018[537].

Standardi tarkoittaa käsitteenä teknisiä määritelmiä, järjestelmäkuvauksia ja vaatimuksia sisältävää normistoa, jonka on antanut jokin tunnustettu standardointielin. Standardien laadintaan osallistuvat toimialojen taloudelliset toimijat

---

533 International Organization for Standardization 2018a.
534 Suomen Standardisoimisliitto SFS ry 2018a.
535 Syksyllä 2022 julkaistu ISO / IEC 27001:2022 korvaa aikaisemman *ISO/IEC 27001:2013*-standardin. Sisällöltään niissä ei ole kuitenkaan suuria eroja. Kyseinen standardi on kehitetty tietoturvallisuuden hallintajärjestelmän luomiseksi, implementoimiseksi, ylläpitämiseksi ja kehittämiseksi. Tietoturvallisuuden hallintajärjestelmän lähtökohtana on riskienhallinta ja hallintajärjestelmän ylläpidossa tulisi keskittyä jatkuvaan parantamiseen. ISO 27001 -sertifiointi lisää organisaation sidosryhmien luottamusta kertomalla, että tietoturva ja riskienhallinta on toteutettu organisaatiossa asianmukaisesti. Standardin implementointi edellyttää myös, että organisaation johto on sitoutunut tietoturvatyöhön sekä organisaatiossa on selkeät tietoturvavastuut ja tietoturvapolitiikat, joista henkilökunta on tietoinen.
536 *ISO/IEC 27005:2018* tarjoaa yksityiskohtaista tietoturvariskien hallinnan opastusta sisältäen kaikki riskienhallinnan eri vaiheet. Standardi pohjautuu ISO/IEC 27001 -standardiin. Vuoden 2018 versio on päivitetty vastaamaan muuttuneen ympäristön haasteisiin, esimerkiksi GDPR:n asettamiin vaatimuksiin. Ks. International Organization for Standardization 2018b.
537 ISO:n standardeista *ISO 31000:2018* soveltuu kaiken tyyppisten riskien käsittelyyn ja se keskittyy riskienhallinnan keskeisiin periaatteisiin. ISO 31000:n tarkoituksena on auttaa organisaatioita ymmärtämään riskien positiiviset mahdollisuudet ja negatiiviset seuraukset. Vuoden 2018 päivitetyssä julkaisussa on otettu huomioon viiden vuoden aikana muuttunut toimintaympäristö, esimerkiksi monimutkaistuneiden talousjärjestelmien uudet riskitekijät, kuten digitaalinen valuutta. ISO 31000:n tarkoituksena on tarjota opastusta eikä niinkään vaatimuksia, minkä takia standardia ei ole tarkoitettu sertifiointiin. Ks. Suomen Standardisoimisliitto SFS ry 2018b.
Muun muassa julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) tuottama riskienhallinnan toimintaohje, jota on käytetty myös tässä tutkimuksessa lähteenä, perustuu ISO 31000 -standardiin. Ks. Valtiovarainministeriön julkaisuja 22/2017a, s. 9.

järjestöjensä välityksellä, jolloin standardoinnin toimijoina toimivat muut yhteiskunnan ja oikeusjärjestyksen valtakeskukset kuin lainsäätäjä ja hallinto.[538] Standardien laadinta ja noudattaminen perustuvat usein sopimuksiin tai alalla vallitsevaan käytäntöön[539]. Näin ollen standardit eroavat käytännesäännöistä. Lähtökohtaisesti standardisointi on myös kaikille vapaaehtoista ja sen tulisi olla organisaation liiketoimintatarpeista lähtevää. Suomen Standardisoimisliitto SFS koordinoi tietoturvatekniikoiden standardisointia[540].

Käytännesääntöjen on katsottu olevan merkittävässä asemassa muun muassa tietosuojan sekä hallinnon tietojärjestelmien tietoturvallisuuden täsmentämisessä nopeasti muuttuvassa, tekniikkasidonnaisessa verkkoyhteiskunnassa[541]. Käytännesäännöt auttavat pitämään teknologianeutraalin lainsäädännön ajankohtaisempana. Näin ollen tietoturvan sääntelyjärjestelmän tulisi huomioida organisaatioiden hyvien käytänteiden muodostama kokonaisuus. Lisäksi hyvä tietoturvan sääntelyjärjestelmä mahdollistaa organisaatioiden hyvät käytännesäännöt tietoturvan toteuttajana ja ottaa huomioon hyvän tietoturvatavan lainsäädäntötasolla.

Hyvän tavan ja käytännesääntöjen myötä tietoturvastandardit voivat saada oikeudellista velvoittavuutta. Standardien noudattaminen on pääsääntöisesti vapaaehtoista, mutta oikeusnormistossa voidaan lailla tai alemman asteisella normilla edellyttää tietyn standardin noudattamista. Täten esimerkiksi oikeusnormistossa olevan viittauksen perusteella standardi voi saada välitöntä oikeudellista velvoittavuutta, jolloin standardi tulee osaksi oikeusnormistoa. Standardi voi myös täydentää tai täsmentää lainsäädännössä asetettuja vaatimuksia, jolloin se saa oikeudellista merkitystä tulkintaohjeena. Tällöin se myös liittyy oikeusnormiin soveltamistilanteessa tarkentavana informaationa eli normia tulkitaan standardin avulla. Huomioitava kuitenkin on, että standardoinnin käyttäminen ei saisi korvata tai kokonaan poistaa julkisen vallan vastuuta perusoikeuksien ja muiden yleisten etujen piiriin kuuluvien tavoitteiden toteuttamisesta.[542] Standardien noudattaminen osana oikeusnormistoa tulisi tarvittaessa huomioida hyvässä tietoturvan sääntelyjärjestelmässä, sillä se edistäisi lainsäädännön proaktiivisuutta sekä teknologianeutraalisuuden periaatteen toteutumista. Näin organisaatioiden hyvät käytännesäännöt tulisivat paremmin huomioitua sääntelyjärjestelmässä, mikä myös parantaisi tiedon ja yksilöiden perusoikeuksien tehokasta suojaamista järjestelmäriippuvaisessa verkkoyhteiskunnassa.

[538] Pöysti 1997: 533.
[539] Pöysti 1997: 534.
[540] Suomen tietoturvallisuusstrategia 2016: 26.
[541] Pöysti 2000: 96.
[542] Pöysti 1997: 515, 533–534, 537.

Standardointi ja käytännesääntöjen kehittäminen ovat keskeisiä välineitä ohjata tietojenkäsittelyn infrastruktuuria ja muuntaa esimerkiksi yksityisyyden ja itsemääräämisoikeuden suoja osaksi tietojenkäsittelyjärjestelmien teknisiä ominaisuuksia sekä noudatettavia hyviä teknisiä käytänteitä. Myös esimerkiksi henkilötietojen suojan konkreettisessa toteuttamisessa ja tekniselle infrastruktuurille asetettavissa vaatimuksissa standardointi ja itsesääntely ovat merkittävässä asemassa.[543] Standardien kehittämisen ohella myös normien kehittäminen (Euroopan unionissa) on tärkeää, sillä sekä standardien että normien avulla voidaan muokata merkittävällä tavalla internetin yleisen saatavuuden ja eheyden kannalta keskeisten uusien teknologioiden sekä teknisen ja loogisen infrastruktuurin normeja ja standardeja. Näin muun muassa varmistetaan, että internet pysyy turvallisena sekä digitaaliteknologioiden käytössä ja kehittämisessä kunnioitetaan ihmisoikeuksia ja niiden käyttö on laillista ja turvallista.[544]

Yhteenvetona voidaan todeta, että tietoturvan osalta ohjeistavia tahoja on paljon sekä käytännesääntöjä ja standardeja on monia niin kansallisella tasolla kuin kansainvälisestikin. Tämä korostaa erityisesti kritiikkiä liittyen käytännesääntöihin soft law -tyyppisenä aineistona: tyypillisesti tavoitteena on sääntelyn määrän vähentäminen, mutta sen määrä tosiasiallisesti kasvaa, jos niin sanottua ”pehmeää sääntelyä” käytetään täydentämään lainsäädäntöä[545]. Kritiikki on ymmärrettävää. Toisaalta nykyisessä tietoturvan sääntelyjärjestelmässä tietoturvasäännökset ovat hajaantuneet eri säädöksiin, säännökset eivät huomioi hyviä käytänteitä riittävällä tasolla sekä yhteiskunnan muutosten ja teknologianeutraalin lainsäädännön takia yksityiskohtaisten tietoturvavaatimusten sääntely on kannattamatonta, ellei jopa mahdotonta, jolloin tietoturvalainsäädännön rinnalle tarvitaan täydentävää sekä korvaavaa soft law’ta.

Soft law -käytännesääntöihin ei liity oikeudellista sitovuutta ja ne on siksi nähty ongelmallisena ja osin myös epätasapuolisena. Huomioitava kuitenkin on se, että käytännesäännöt ja standardit toimivat usein konkreettisena osana tietoturva-arviointeja ja siten niiden noudattaminen on luottamusta lisäävä tekijä, joka heijastuu hankintoihin, sopimuksiin ja palveluiden käyttöön. Näin ollen ilman oikeudellista sitovuuttakin, käytännesääntöjen ja standardien noudattaminen on merkittävä liiketoiminnallinen etu ja osa hyviä tietoturvallisia käytänteitä. Käytännesäännöt on huomioitava osana tietoturvan sääntelyjärjestelmää, kuten myös standardien noudattaminen osana oikeusnormistoa, jotta lainsäädäntö pysyy teknologianeutraalina ja ajankohtaisena muuttuvassa järjestelmäriippuvaisessa

543 Pöysti 2000: 101.
544 Euroopan unionin neuvosto, Neuvoston päätelmät EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle 22.3.2021: 6.
545 Nieminen 2020: 1084–1085; Korkea-aho 2005: 73–74.

toimintaympäristössä. Hyvien käytänteiden huomioiminen organisaatioiden hyvän tietoturvan sääntelyjärjestelmän eräänlaisena kriteerinä edellyttää myös sitä, että tietoturvasäännösten pitää olla käsitetasolta lähtien hyvien tietoturvallisten käytänteiden mukaisia, jotta lainsäädännön tulkinta helpottuu ja tulkinnallisia ristiriitoja ei synny.

3 TIETOSUOJA JA HYVÄ TIETOTURVATAPA

3.1 Luvun päämäärä

Teknologian kehitys, digitalisaatio ja globalisaatio tuovat uusia haasteita henkilötietojen suojeluun. Henkilötietoja jaetaan ja kerätään enemmän kuin ennen sekä organisaatioiden että yksityisten henkilöiden toimesta, ja tämän lisäksi niitä käytetään laajalti hyväksi. Näin myös todetaan EU:n yleisessä tietosuoja-asetuksessa (2016/679/EU, GDPR).

Internetin kehittymisen myötä, ja sen globaalin luonteen vuoksi, suuri määrä henkilötietoja on siirtynyt internettiin ja niitä siirrellään eri maiden välillä. Joissain tapauksissa tietojen lähettäjä ja vastaanottaja, esimerkiksi sähköpostin välityksellä, eivät välttämättä ole edes tietoisia tietojen liikkumisesta kansallisten rajojen ulkopuolelle.[546] Tämän ilmiön lisäksi on huomioitava, että henkilötietoja säilytetään useammassa järjestelmässä. Tulevaisuudessa tietojen suojaaminen ja tietosuojariskien huomioiminen organisaation jokapäiväisessä toiminnassa tulevat olemaan keskeisessä roolissa etenkin organisaatioiden toimiympäristön muuttuessa, tietovarantojen kasvaessa ja palveluiden digitalisoituessa.

Yleisen tietosuoja-asetuksen myötä organisaatioiden vastuu tietosuojan toteutumisesta on kasvanut entistä suuremmaksi, sillä organisaatioita koskee osoitusvelvollisuus siitä, että ne huomioivat henkilötietojen käsittelyä koskevat yleiset periaatteet ja muut tietosuojalainsäädännön velvoitteet. Tietoturvan parantamisen kannalta tämä on ollut positiivinen edistysaskel, sillä tietosuojan toteutumisen osoitusvelvollisuus kohentaa samalla myös organisaation tietoturvaa ja hyvien tietoturvallisten käytänteiden omaksumista sekä johdon aktiivista sitoutumista tietoturva- ja tietosuojatyöhön.

Lainsäädännön kehittymisen ohella myös organisaatioiden tietosuoja-ajattelussa on tapahtunut asennemuutos. Tietosuojasta on tulossa osa organisaatioiden strategista toimintaa, joka koskettaa organisaatiota kokonaisvaltaisesti. Lisäksi tietosuojatyö ja sen organisointi ovat organisaatioiden operatiivisen toiminnan menestystekijä.[547]

Muuttuva ympäristö sekä uudet palvelut ja toimintatavat luovat mahdollisuuksia toiminnan kehittämiselle sekä uusien palveluiden tarjoamiselle, mutta myös uusia tietoturva- ja tietosuojauhkia. Tämän vuoksi on tärkeää säilyttää kuluttajien sekä organisaation muiden sidosryhmien luottamus siitä, että heidän tietonsa pysyvät

[546] Blume 2001: 32–33.
[547] Andreasson, Koivisto & Ylipartanen 2016: 17.

turvattuina palveluiden siirtyessä entistä enemmän verkkoon. Henkilötietojen suojaamiseksi tarvitaan myös tietoturvatoimenpiteitä.

Puhuttaessa Suomessa oikeudellisesta tietoturvavallisuudesta historia ulottuu vuoteen 1987, jolloin henkilörekisterilaki säädettiin. Tällöin alettiin puhua tietosuojasta, mutta siihen liittyi myös tietoturvallisuuden vaatimus. Henkilörekisterilain onkin nähty olevan meillä Suomessa ensimmäinen modernin tietoturvallisuuden laajempaa käyttöä edellyttänyt laki.[548] Henkilörekisterilain jälkeen säädettiin kansallinen henkilötietolaki, jolla pantiin täytäntöön EU:n henkilötietodirektiivi (1995/46/EY). Informaatioteknologian nopean kehittymisen ja jäsenvaltioiden epäyhtenäisen henkilötietojen suojaa koskevien säädösten ja niiden soveltamisen myötä EU päätyi säätämään kattavan tietosuojakehyksen tietosuoja-asetuksen avulla.[549] Tietosuoja-asetuksen myötä tietoturva ei ole enää ollut samanlaisessa sivuroolissa kuin se oli henkilötietodirektiivissä, mikä kuvastaa tietoturvan merkityksen kasvua ja eurooppalaista asennemuutosta[550].

Tietoturva ja tietosuoja kulkevat käsi kädessä. Siinä missä tietoturvan avulla pyritään suojamaan tiedon luottamuksellisuus, eheys ja käytettävyys (CIA: Confidentiality, Integrity, Availability), tietosuojan tarkoituksena on suojata erityisesti tiedon luottamuksellisuutta[551]. Toisaalta tietosuoja-asetuksen myötä tietosuojan osalta on myös korostettu eheyden ulottuvuutta: tiedon eheyden turvaamiseen kuuluu muun muassa henkilötiedon suojaaminen vahingossa tapahtuvalta tuhoamiselta, hävittämiseltä tai vahingoittumiselta. Vanhentunut tai virheellinen henkilötieto voi aiheuttaa negatiivisia seurauksia rekisteröidylle, esimerkiksi suoria oikeusvaikutuksia tai väärinymmärryksistä aiheutuvaa mielipahaa. Luottamuksellisuuden ja eheyden ulottuvuuksien lisäksi tiedon käytettävyys on tärkeää, sillä henkilötiedon tulee olla käytettävissä (saatavilla) oikea aikaisesti etenkin silloin, kun kyse on kriittisistä järjestelmistä. Rekisteröityjen näkökulmasta esimerkiksi haittaohjelman saastuttama tietojenkäsittely-ympäristö ja siitä johtuva palvelun uudelleen pystyttäminen on seurauksiltaan paljon vakavampi hyvinvointialueen potilastietojärjestelmässä kuin kiinteistövälitysyrityksen asiakastietojärjestelmässä, mikäli luonnollisten henkilöiden tiedot eivät ole käytettävissä oikeaan aikaan.

Tietosuojan avulla pyritään ensisijaisesti suojaamaan yksilöiden henkilötietoja ja yksityisyyttä[552], tietoturvan avulla sen sijaan pyritään suojaamaan henkilötietojen

[548] Saarenpää & Riekkinen 2023: 199.
[549] HE 9/2018 vp: 4.
[550] Saarenpää & Riekkinen 2023: 231.
[551] Sanastokeskus TSK 2004.
[552] Käsitteenä tietosuoja on ristiriitainen, kuten aikaisemmin toisen pääluvun systematiikkaosiossa on todettu. Tämä johtuu siitä, että käsite kuvastaa kaikenlaisten tietojen suojaamista, vaikkakin alun perin tavoitteena on ollut suojata luonnollisia henkilöitä.

lisäksi myös muita salassa pidettäviä tai luottamuksellisia tietoja. Yksityisyys on riippuvainen turvallisuudesta ja kaikki nykyaikaiset tietosuojaperiaatteet sisältävät niin ikään velvollisuuden suojata myös turvallisuutta[553]. Näin ollen, jos tietoturvan taso on puutteellinen, on myös tietosuojan taso puutteellinen. Toisaalta jos tietosuojaa ei olisi tai se olisi vajavaista, niin tietoturva ei olisi tällöin täydellistä.

Tietosuojan näkökulmasta tietoturvalla tarkoitetaan käytännön teknisiä ja organisatorisia toimenpiteitä tietosuojan toteuttamiseksi, joilla pyritään rekisteröidyn etujen, oikeuksien ja yksityisyyden suojaamiseen ja turvaamiseen[554]. Yksityisyyden ja henkilötietojen suoja ovat monella tapaa kuitenkin riippuvaisia tietoturvallisuusratkaisuista[555]. Henkilötietoja on osittain mahdollista suojata tietoturvateknologian avulla, jonka käytön esteenä voivat kuitenkin olla tietämättömyys, osaamattomuus tai suojaamisen kustannukset[556]. Tietosuojalainsäädäntö asettaa vaatimuksia tietoturvalle muun muassa tietojärjestelmien laatuvaatimusten kautta[557]. Tietojärjestelmien huono oikeudellinen tai tietotekninen laatu on usein syynä hallinnollisiin taakkoihin sekä väitteisiin siitä, että tietosuoja vaikeuttaa tiedonkulkua.[558] Tyypilliset väitteet siitä, että tietosuoja- ja tietoturvavaatimukset haittaavat ja hidastavat kehittämistä tai tekemistä, ovat peräisin juuri osaamisen puutteesta. Mikäli henkilökunnan tietosuojaosaaminen on riittävällä tasolla sekä organisaation tietoturvan ja tietosuojan varmentamisprosessit ovat selkeästi kuvattu ja jalkautettu, myös tietosuoja- ja tietoturvavaatimukset tulevat tarpeeksi varhaisessa vaiheessa huomioitua osana kehittämisen, tekemisen ja hankinnan suunnittelua. Tällöin tietosuoja ja tietoturva eivät ole haittaavia tai hidastavia tekijöitä organisaation toiminnassa, vaan luonnollinen osa prosesseja. Esimerkiksi tietosuojariskejä tulisi aina arvioida rekisteröityjen näkökulmasta ennen uusien käsittelytoimien aloittamista, mutta valitettavan usein käytännön työssä tietosuojariskien arviointi tulee kyseeseen liian myöhäisessä vaiheessa käsittelytoimien aloittamisen jälkeen taikka kiireellä juuri ennen järjestelmän tai palvelun käyttöönottoa. Vastakohtaisesti tietoturvan ja tietosuojan varhainen huomiointi auttaa minimoimaan riskejä ja ongelmia, jolloin organisaation palvelut toimivat moitteettomasti, lainmukaisesti ja ne ovat turvallisia. Näin ollen tietoturva ja tietosuoja yhdessä ovat mahdollistajia sekä parhaimmillaan organisaation imagoa ja asiakasmäärää kasvattavia tukitoimintoja. Tässä tutkimuksessa painotetaan tietosuojan huomioimista osana tietoturvaa sekä miten tietoturvan minimivaatimukset suojaavat

553 Cate, Kuner, Lynskey, Millard & Svantesson 2017: 73.
554 Andreasson, Koivisto & Ylipartanen 2013: 14.
555 Pöysti 1999: 455.
556 Pitkänen, Tiilikka & Warma 2013: 8.
557 Tätä aihetta käsitelty lisää esimerkiksi luvussa 4.4 (”Järjestelmien oikeudellisen suunnittelun vaatimukset sääntelyjärjestelmässä”).
558 Saarenpää 2015: 330.

muiden luottamuksellisten tietojen lisäksi erityisesti henkilötietoja ja mahdollistavat turvallisen henkilötietojen käsittelyn organisaatiossa.

Tämä kolmas pääluku keskittyy tietosuojalainsäädännön sisäänrakennetun riskienhallintavelvoitteen tietoturvavaatimuksiin. Tietosuoja-asetus on suoraan sovellettavaa lainsäädäntöä ja velvoittavuutensa kannalta organisaatioita vahvasti sitovaa, jolloin se vaikuttaa suuresti organisaatioiden toimintaan ja tietoturvallisuuden kehittämiseen. Esimerkiksi NIS 2 -direktiiviin verrattuna tietosuoja-asetus on hierarkkisesti etusijalla tulkinnassa. Tästä syystä, ennen kuin siirrytään neljännessä pääluvussa käsittelemään NIS 1 ja NIS 2 -direktiivien tuomia muutoksia ja lainsäädännössä ilmenevää hyvää tietoturvatapaa järjestelmien tietoturvan kannalta, on tärkeää tunnistaa tietosuojalainsäädännön asettamat tietoturvavaatimukset organisaatioille. Huomioitava on se, että yleisessä tietoverkossa tapahtuva tietojenkäsittely on globaalia, jolloin eurooppalainen sääntely ei täysin ratkaise yksilön oikeuksien toteuttamiseen liittyviä ongelmia rajatulla alueella. Tietosuoja-asetuksen suoja kohdistuu jäsenvaltioihin, jolloin EU on muun muassa pyrkinyt varmistamaan tietosuojan toteutumista rajoituksilla henkilötietojen siirrolle sekä muilla turvaavilla järjestelyillä[559]. Tässä luvussa keskeiseksi näkökulmaksi muodostuukin Suomea koskevat tietosuojavaatimukset ja sitä myötä erityisesti vaatimukset, jotka kohdistuvat organisaatioiden tietoturvaan.

Keskeisenä aiheena tässä pääluvussa on tietosuojalainsäädännön hyvä tietoturvatapa tietoturvan sääntelyjärjestelmässä. Vaikuttavimpia tietoturvaa parantavia tietosuoja-asetuksen vaatimuksia ovat muun muassa dokumentointivaatimukset, tietosuojariskien arviointi sekä muut tekniset ja organisatoriset tietoturvatoimenpiteet, minkä takia näitä käsitellään yksityiskohtaisemmin tässä tutkimuksessa. Tarkoituksena on myös selvittää, mitä teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan, sekä vastaako tietoturvan sääntelyjärjestelmässä ilmenevien erilaisten tietoturvatoimenpiteiden vaatimus hyviä tietoturvallisia käytänteitä. Lopuksi käydään läpi organisaatioiden tiettyjä tietoturvatoimenpiteitä, kuten kameravalvontaa ja muuta teknistä valvontaa, joiden osalta tulee huomioida työelämän tietosuojalaki ja työntekijöiden yksityisyys. Organisaation tietosuoja-asiat kattavat myös organisaation sisäiset sidosryhmät, kuten työntekijät. Tarkoituksena ei ole kuitenkaan käydä läpi kaikkia työntekijöiden tietosuojaan liittyviä seikkoja, vaan näkökulmana on ennemminkin tutkimuksen tematiikan mukaisesti organisaation

[559] Esimerkki turvaavista järjestelyistä on Yhdysvaltojen Safe Harbour, jonka kumosi Privacy Shield -järjestely (ks. Voutilainen 2019: 19). Heinäkuussa 2020 Euroopan tuomioistuin totesi kuitenkin Privacy Shield -järjestelyn pätemättömäksi Schrems II-tuomiossaan C-311/18 (ks. Saarenpää & Riekkinen 2023: 27). Nyttemmin komissio on katsonut riittäväksi järjestelyksi EU:n ja Yhdysvaltojen välisen tietosuojakehyksen (DPF – Data Privacy Framework), jonka perusteella siihen sitoutuneet yritykset täyttävät EU:n tietosuojavaatimukset.

tietoturvaa lisäävät käytänteet sekä näissä huomioon otettavat tietosuoja-asiat. Viimeisen alaluvun aiheena on työelämän tietosuoja ja tietoturva, joten lopuksi käsitellään myös henkilöstöturvallisuuden keskeisiä hallinnollisia tietoturvatoimenpiteitä, kuten työntekijöiden luotettavuuden ja osaamisen varmistamista sekä tietoturvavastuita. Näitä tarkastellaan sekä tietosuojalainsäädännön että tietoturvalainsäädännön näkökulmasta.

3.2 Henkilötietojen käsittelyn systematiikkaa

3.2.1 Henkilötieto ja erityinen henkilötieto

Tietosuojan keskeisenä tarkoituksena on suojata yksilöiden henkilötietoja. Näiden tietojen suojaamiseksi on toteutettava tietoturvatoimenpiteitä. Henkilötietoja tulee osata käsitellä myös oikein lainsäädännön hyvän henkilötietojen käsittelytavan tietosuojaperiaatteiden mukaisesti[560]. Käytännön ongelmaksi useissa organisaatioissa kuitenkin muodostuu henkilötietojen tunnistamisen haasteet, mikä puolestaan kertoo organisaation tietosuojan alhaisesta maturiteettitasosta: työntekijät eivät välttämättä osaa tunnistaa käsittelemäänsä tietoa nimenomaan henkilötiedoksi. Täten aluksi on hyvä määritellä, mitä tarkoitetaan henkilötiedolla.

Henkilötieto voi olla yksityiselämän suojan piirissä oleva yksityiselämää koskeva tieto. Yksityiselämää koskevat tiedot ovat aina henkilötietoja, jos ne voidaan yhdistää tiettyä henkilöä koskeviksi. Kaikki henkilötiedot eivät kuitenkaan välttämättä kuulu yksityiselämän suojan alaan.[561] Yksinkertaistettuna esimerkkinä tällaisista henkilötiedoista, jotka eivät kuulu yksityiselämän suojan alaan, ovat nimitietoa sisältävät organisaatiosähköpostiosoitteet. Organisaationäkökulmasta tällaiset henkilötiedot saattavat olla myös niin sanottua julkista henkilötietoa, mikäli ne ovat julkisesti saatavilla. Julkisten henkilötietojen lisäksi organisaatiossa tulee tunnistaa salassa pidettävä henkilötieto ja tällaisen tiedon tietoturvavaatimukset. Esimerkiksi erityiset henkilötiedot, joita käsitellään jäljempänä, vaativat lainmukaisesti enemmän tietoturvatoimenpiteitä kuin ”tavallinen” henkilötieto.

Tietosuoja-asetuksen määritelmän mukaan henkilötiedolla tarkoitetaan kaikkia jo tunnistettuun taikka suorasti tai epäsuorasti tunnistettavissa olevaan *luonnolliseen henkilöön* liittyviä tietoja. Tällaisia tietoja ovat esimerkiksi nimi, henkilötunnus, verkkotunnistetiedot, sijaintitiedot taikka yksilöön liitettävät tunnusomaiset geneettiset, psyykkiset, fyysiset, fysiologiset, taloudelliset, kulttuurilliset tai

[560] Ks. yksityiskohtaisemmin hyvästä henkilötietojen käsittelytavasta ja tietosuojaperiaatteista luvusta 1.5 (”Hyvä tapa tietoturvan sääntelyjärjestelmän elementtinä”).
[561] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 16.

sosiaaliset tekijät. Tieto katsotaan henkilötiedoksi, kun se liittyy henkilöön sisältönsä, tarkoituksensa tai vaikutuksensa vuoksi[562]. Henkilötiedon käsitettä tulkittaessa voidaan myös hyödyntää tietosuojadirektiivin aikaista oikeuskäytäntöä ja -kirjallisuutta, sillä henkilötiedon käsite ei tietosuoja-asetuksessa juurikaan muuttunut[563]. Henkilötiedon määritelmän täyttymisen kynnys on täten varsin matala ja sitä on tulkittava laajasti.

Tapauskohtaisesti riippuu tilanteesta ja asiayhteydestä, riittääkö joku tietty tunniste erottamaan henkilön muista. Esimerkiksi toissijainen tieto, kuten ”mustapukuinen mies”, voi erottaa henkilön muista liikennevaloissa seisovista ihmisistä.[564] Tietosuojatyöryhmän mukaan, henkilötiedon laajaan käsitteeseen liittyviä mahdollisia ongelmia ei tule ratkaista kapealla tulkinnalla, vaan pohtimalla, kuuluuko tilanne ylipäätänsä tietosuojalainsäädännön soveltamisalaan ja onko käsittely tietosuojalainsäädännön asettamissa rajoissa mahdollista[565].

Henkilötietoja voi olla siten monenlaisia. Esimerkiksi tapauksessa **EUT 19.10.2016 C-582/14 Breyer vs. Saksan liittotasavalta** IP-osoitteet katsottiin olevan henkilötietoja:

> *Tapauksessa Breyer kävi useilla Saksan liitovaltion laitosten palvelusivustoilla, joista useimmat näistä sivustoista tallentavat käynnit protokollatietoihin verkkohyökkäyksiltä suojautumista ja hyökkääjien rikosoikeudelliseen vastuuseen saattamista varten. Tallennettuja tietoja olivat muun muassa tietokoneiden staattiset tai dynaamiset IP-osoitteet. Breyer vaati, että Saksan liittotasavaltaa kielletään tallentamasta tai antamasta sivullisen tallennettavaksi Saksan liittovaltion laitosten verkkomediapalveluiden yleisön saatavilla olevilla sivustoilla käynnin päätyttyä Breyerin isäntäjärjestelmän IP-osoitetta, ellei tallentaminen ole tarpeen verkkomediapalvelun käytettävyyden palauttamiseksi häiriön ilmetessä. Pääkysymykseksi nousi, ovatko IP-osoitteet sellaisenaan henkilötietoja, sillä henkilöllisyyttä ei voitu suoraan tunnistaa tallennettujen tietojen perusteella vaan ainoastaan silloin, mikäli internetyhteyden tarjoaja välittää käyttäjän henkilöllisyyttä koskevia tietoja. Ratkaisun mukaan dynaamiset eli tilapäiset IP-osoitteet ovat palveluntarjoajaan nähden henkilötieto, mikäli palveluntarjoajalla on käytettävissään oikeudelliset*

[562] EUT 20.12.2017 C-434/16 Nowak: kohta 35; Voutilainen 2019: 41; Voutilainen 2020: 59; Voutilainen 2023: 69.
[563] Korpisaari & Toikkanen 2020: 461.
[564] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 63–64; Euroopan WP29-tietosuojatyöryhmä WP136: *Lausunto 4/2007 henkilötietojen käsitteestä*, s. 12–13.
[565] Euroopan WP29-tietosuojatyöryhmä WP136: *Lausunto 4/2007 henkilötietojen käsitteestä*, s. 4–6; Korpisaari & Toikkanen 2020: 462.

> *keinot, joiden perusteella se voi tunnistaa henkilön sellaisten lisätietojen avulla, jotka ovat internetyhteyden tarjoajan käytettävissä.*

IP-osoite (Internet Protocol address) on numerosarjasta muodostuva protokolla, joka yksilöi tietoverkkoon liitetyn laitteen[566]. Käytännössä IP-osoitteet auttavat tietojen ja viestinnän siirtämisessä laitteiden välillä, kun IP-paketit kulkevat IP-osoitteesta toiseen. Edellä oleva tapaus koski lähinnä *dynaamisia IP-osoitteita* eli sellaisia, jotka vaihtuvat jokaisen uuden internetyhteyden ottamisen yhteydessä. Aikaisemmassa oikeuskäytännössä **EUT 24.11.2011 C-70/10 Scarlet Extended SA v. SABAM** on todettu *staattisten IP-osoitteiden* eli yksittäiseen laitteeseen sidottujen IP-osoitteiden olevan henkilötietoja[567], sillä käyttäjät on mahdollista tunnistaa täsmällisesti. Tämä tosin koski tilannetta, jossa internetin käyttäjien IP-osoitteiden keräämisen ja tunnistamisen suorittivat ainoastaan internetyhteyden tarjoajat.[568] Edellä mainitusta oikeuskäytännöstä soveltaen myös laitteiden MAC-osoitteet (Media Access Control) ovat henkilötietoa, mikäli henkilö on mahdollista tunnistaa epäsuorasti osoitteen kautta. MAC-osoitteen avulla verkkosovittimella varustetut laitteet on mahdollista yksilöidä verkossa ja siten yhdistää laitteen, esimerkiksi tietokoneen, omistajaan.

EUT:n ratkaisuista voidaan päätellä sekä staattisten että dynaamisten IP-osoitteiden olevan henkilötietoja, mikäli näistä on tunnistettavissa henkilö myös epäsuorasti yhdistelemällä muita tietoja. EUT:n ratkaisujen myötä on tulkittu laajasti, että käytännössä kaikki IP-osoitteet voivat olla henkilötietoja, sillä tietoja käsittelevän tahon tietoon voi periaatteessa milloin tahansa siitä itsestään riippumatta tulla sellaisia tietoja, jotka mahdollistavat IP-osoitteen taustalla olevan henkilön tunnistamisen[569]. Tapauksessa **EUT C-582/14 Breyer vs. Saksan liittotasavalta** oli kiistatonta, ettei dynaaminen IP-osoite ollut itsessään henkilötieto, koska siinä ei käynyt suoraan ilmi, kenen luonnollisen henkilön tietokoneella oli käyty kyseisellä internetsivustolla. Dynaaminen IP-osoite on kuitenkin todettu olevan henkilötieto, mikäli on mahdollista tunnistaa kyseinen henkilö käytettävissä olevien lisätietojen avulla.[570] IP-osoitteen määritteleminen henkilötiedoksi ei ole näin yksiselitteistä.

Onko IP-osoite henkilötietoa vai ei riippuu edellä mainituin perustein siitä, voiko henkilön tunnistaa epäsuoraan yhdistelemällä muita tietoja. Tästä huolimatta käytännön työssä on tulkittu lähes automaattisesti IP-osoitteiden olevan

[566] Myös Voutilainen 2023: 31–32.
[567] Heiskanen 2020: 120.
[568] Myöhemmässä Unionin tuomioistuimen käytännössä IP-osoite on katsottu sekä henkilö- että liikennetiedoksi, ks. esimerkiksi EUT 17.6.2021 C-597/19 M.I.C.M, kohta 113.
[569] Heiskanen 2020: 121. Samaan tulkintaan on myös päätynyt esim. Pesonen 2017, s. 97: Henkilötietoja ovat esimerkiksi IP-osoite.
[570] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 64–65.

henkilötietoja, koska ”milloin tahansa tietoja käsittelevä taho voi saada käsiinsä tietoja”, joita yhdistelemällä IP-osoitetietojen kanssa voi tunnistaa luonnollisen henkilön. Tulkinnan ei kuitenkaan pitäisi olla näin mustavalkoista:

> Ensinnäkin IP-osoitteet ovat yhdistettävissä tietoverkkoon liitettyihin laitteisiin, eli kyseessä voi olla esimerkiksi reitittimen IP-osoite, johon puolestaan on yhdistettävissä useat sitä hyödyntävät, eri laitteet. Tällöin kyseinen IP-osoite ei välttämättä ole henkilöitä yksilöivä, etenkin, jos kyseessä ei ole kotitalouden oma reititin. Kovin yksilöivää ei ole myöskään se, jos käytössä on yhteiskäyttöisiä päätelaitteita.
>
> Toinen huomioitava seikka on se, että luonnollisten henkilöiden tunnistaminen on vaikeutunut VPN-palveluiden käytön kasvun myötä: VPN-palveluiden myötä IP-osoite on mahdollista muuttaa ja reitittää muualle kuin kotimaahan. Monesti ilman VPN-palveluitakin IP-osoitteet ovat varsin epätarkkoja geolokaatioltaan.
>
> Kolmantena huomiona on se, että organisaatioissa on käytössä palveluita, joissa IP-osoitteita ei voi yksinkertaisesti yhdistää luonnollisiin henkilöihin. Näistä esimerkkinä DMARC (Domain-based Message Authentication, Reporting and Conformance), joka on tietoturvapalvelu, jonka avulla organisaatiot voivat suojata verkkotunnuksiaan, esimerkiksi ”@organisaatio.fi” oikeudettomalta käytöltä ja sähköpostien väärentämiseltä. DMARC-raporttien IP-osoitteet ovat alkuperäisen sanomansiirtoagentin (MTA) IP-osoitteita[571].
>
> Toisaalta on huomioitava se, käsitelläänkö IP-osoitetta sähköisen viestinnän palvelulain (917/2014) mukaiseen viestin välittämiseen, jolloin kyseessä on välitystieto. Lain mukaan välitystieto on oikeus- tai luonnolliseen henkilöön yhdistettävissä oleva tieto, jota viestinnän välittäjä käsittelee viestien välittämiseksi[572]. Näin ollen, mikäli välitystietona toimiva IP-osoite on yhdistettävissä luonnolliseen henkilöön, kyseessä on henkilötieto.[573] Ymmärtääkseni palvelut ja järjestelmät käsittelevät IP-osoitteita myös muihin tarkoituksiin kuin viestin välittämiseen. Esimerkiksi juuri

[571] Valtaosa sähköposteista lähetetään sellaisten yleisten MTA:n kautta, jotka toimivat yhdyskäytävinä tai välittäjinä monien yksittäisten lähettäjien sähköposteille eikä tällaisessa yleisessä tapauksessa ilmoitettuja IP-osoitteita voi katsoa henkilötiedoiksi yksinään, koska niitä ei ole kohdistettu tietyille henkilöille. Ks. DMARC 2021.
[572] Ks. HE 221/2013 vp: 95.
[573] Ks. lisää IP-osoitteista välitystietoina luvusta 3.5.4 ("Muu teknisin menetelmin toteutettu valvonta").

sivustojen kävijäseurannan toteuttamiseen[574]. Täten tulisi huomioida IP-osoitteiden käyttötarkoitussidonnaisuus.

Näiden huomioiden pohjalta voidaan todeta, että IP-osoitteen yhdistäminen epäsuorasti luonnolliseen henkilöön ei ole helppoa. Lisäksi asiaa arvioitaessa tulisi kiinnittää huomiota toimialakohtaisiin eroavaisuuksiin: ovatko kaikki rekisterinpitäjäorganisaatiot samanarvoisia sen suhteen, että he voivat saada niin paljon tietoa, jolloin yhdistelemällä näitä tietoja he tunnistaisivat lokeistansa IP-osoitteen perusteella luonnollisen henkilön? Eivät välttämättä, jos vertaa esimerkiksi kävijäseurannan evästeiden IP-osoitteita käsittelevää pientä verkkokauppayritystä versus poliisiorganisaatiota. Toimialakohtaisia eroavaisuuksia arvioitaessa keskeinen tarkasteltava asia on epäsuoran tunnistamisen todennäköisyys muun muassa käytettävissä olevien oikeudellisten keinojen avulla.

Esimerkiksi edellä olevassa tapauksessa **EUT C-582/14 Breyer vs. Saksan liittotasavalta** todettiin, että tilapäiset IP-osoitteet ovat palveluntarjoajaan nähden henkilötieto, mikäli palveluntarjoajalla on käytettävissään oikeudelliset keinot, joiden perusteella se voi tunnistaa henkilön sellaisten lisätietojen avulla, jotka ovat internetyhteyden tarjoajan käytettävissä[575]. EUT:n ratkaisussa painotettiin myös sitä, onko mahdollisuus yhdistää dynaaminen IP-osoite internetyhteyden tarjoajan hallussa oleviin lisätietoihin rekisteröidyn tunnistamiseksi *kohtuullisesti toteutettavissa oleva keino*. Kohtuullisesti toteutettava keino ei ole kyseessä silloin, kun rekisteröidyn tunnistaminen on kielletty laissa tai kun se ei ole käytännössä toteutettavissa esimerkiksi siitä syystä, että se veisi suhteettomasti aikaa ja aiheuttaisi suhteettomasti kustannuksia ja työtä. Tällöin luonnollisen henkilön tunnistamisen riski näyttäytyy käytännössä merkityksettömänä.[576] Kyberhyökkäystilanteessa toimivaltaisen viranomaisen tiedon hankinta rikosoikeudellisen menettelyn käynnistämiseksi on katsottu kohtuullisesti toteuttavissa olevaksi lailliseksi keinoksi[577]. Entä jos kyseessä onkin VPN:llä suojattu IP-osoite, jota viranomainen ei saa haltuunsa? Näinkin on käynyt, esimerkiksi ratkaisussa **KKO 2022:23** virtuaalista erillisverkkoa (VPN) tarjoavaa A Oyj:tä ei velvoitettu antamaan Keskusrikospoliisille A Oyj:n hallussa olevia lokitietoja, jotka olisivat paljastaneet käyttäjän todellisen IP-osoitteen[578]. Todettakoon, että kaikissa yrityksissä tällaisia kohtuullisia tai oikeudellisia keinoja ei ole välttämättä käytettävissä, koska ne

[574] Ks. IP-osoitteiden moninaisia käyttötarkoituksia esim. NordVPN blogi 2021.
[575] EUT 19.10.2016 C-582/14 Breyer, ratkaisun kohta 49.
[576] EUT 19.10.2016 C-582/14 Breyer, ratkaisun kohta 45 ja 46.
[577] EUT 19.10.2016 C-582/14 Breyer, ratkaisun kohta 48.
[578] Ks. lisää KKO:n ratkaisusta luvusta 3.5.4 (”Muu teknisin menetelmin toteutettu valvonta ja välitystiedot”).

> riippuvat myös yrityksen käyttämän palvelun luonteesta sekä IP-osoitteiden käyttötarkoituksesta. Esimerkiksi kaikista IP-osoitteita keräävistä palveluista ei välttämättä ole edes tarkoituksenmukaista aloittaa rikostutkintaa. Tällöin tilapäinen eli dynaaminen IP-osoite ei välttämättä ole yksiselitteisesti yksilöivää henkilötietoa.

Näin ollen IP-osoitteiden tarkastelu henkilötietona vaatii aina toimiala- ja tapauskohtaista arviointia ja tutkintaa, onko luonnollista henkilöä mahdollista kohtuullisesti ja laillisesti tunnistaa epäsuorasti tietoja yhdistelemällä, ja muodostuuko tällöin IP-osoitteista sellainen rekisteri, jossa organisaatio on rekisterinpitäjä. Organisaatioiden tulee tunnistaa palvelunsa, joissa ne käsittelevät henkilötietoa rekisterinpitäjänä, ja palvelun henkilötietotyypit, sillä tämä arvio vaikuttaa myös muihin rekisterinpitäjän velvollisuuksiin, kuten tietosuojan riskiarviointeihin.

Tietosuojalainsäädännössä luonnolliseen henkilöön viittaus on *e contrario* eli vastakohdan pois sulkeva, jolloin yhteisöille ja ryhmille ei ole annettu tietosuojan ulottamaa suojaa. Jos tietosuoja ulottuisi suojelemaan yhteisöjä tai ryhmiä, suojatut kohteet ja ryhmät olisi tullut määritellä ja kuvata. Oikeushenkilöillä ei ole yksityisyyttä, eikä muutenkaan henkilötietoihin rinnastettavia ominaisuuksia, perhettä, elinolosuhteita tai taloutta.[579] Näin ollen tietosuoja-asetuksen suoja ei kohdistu suoranaisesti organisaatioihin, vaan laki määrää velvoitteita organisaatioille suojata yksilöiden henkilötietoja.

Tietosuoja-asetusta ei sovelleta myöskään kuolleiden henkilöiden tietoihin. Asetuksen johdanto-osassa todetaan, että jäsenvaltiot voivat itse säätää kuolleiden henkilöiden henkilötietojen käsittelystä.[580] Tällaista poikkeusta ei kuitenkaan tehty Suomessa, jolloin näyttäisi siltä, että tietosuoja-asetus supistaa vainajien henkilötietojen suojaa[581]. Tältä osin oikeuskulttuurimme muuttui yllättäen, sillä henkilötietojen suoja oli ulottunut kuolleiden henkilöiden tietoihin koko aikaisemman tietosuojalainsäädäntömme ajan[582].

Kuitenkin salassapitosääntely ja salassapitoajat sekä rikoslain 24 luvun 9 §:n vainajan kunniaa suojaava säännös rajoittavat kuolleen henkilön tietojen käsittelyä. Myös perustuslakivaliokunta on todennut, että perustuslain 1.2 §:n säännös ihmisarvon loukkaamattomuudesta ulottaa vaikutuksensa laajemmalle kuin elossa olevien ihmisyksilöiden kohteluun. Näin ollen vainajaa koskeva sääntely ei ole merkityksetöntä tämän yksityisyyden suojaan liittyvien oikeuksien kannalta.[583]

---

[579] Kemppinen 2011: 120–121.
[580] Nyyssölä 2018: 38–39.
[581] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 58–59.
[582] Saarenpää & Riekkinen 2023: 180.
[583] Voutilainen 2019: 89; PeVL 18/2014 vp: 9; PeVL 71/2002 vp: 2; PeVL 19/2008 vp: 2.

Esimerkkinä viranomaisen asiakirjoja koskevan julkisuuslain 31 §:n mukaan henkilötietojen suoja ei katkea henkilön kuolemaan, vaan on voimassa 50 vuotta kuolinhetkestä. Vakiintuneen tulkinnan mukaan arkaluontoisia henkilötietoja käsitellään samojen periaatteiden mukaan kuin muuta salassa pidettävää aineistoa.[584] Henkilötietojen suoja on perusoikeus ja koska pääsääntöisesti perusoikeudet koskevat eläviä luonnollisia henkilöitä, kuolema ei kavenna tätä suojaa ajallisesti[585]. Henkilötiedoiksi ei katsota tietoja, jotka koskevat kuollutta henkilöä, ja ne ovat muodostuneet hänen kuolemansa jälkeen[586]. Koska tietosuoja-asetuksen henkilötietojen suoja ulottuu suorasti tai epäsuorasti tunnistettavissa olevaan luonnolliseen henkilöön, sama suoja ulottuu ikään kuin välillisesti koskemaan myös kuollutta henkilöä ja tämän tietoja, mikäli kuolleen henkilön tiedoista voisi tunnistaa elossa olevan henkilön.

Henkilötietojen säilytysaikoja määriteltäessä tulee ottaa myös huomioon kuolleen henkilön tietojen säilyttämisen tarve kuoleman jälkeen. Esimerkiksi perustuslakivaliokunnan lausunnon mukaan tietojen pysyvän tallentamisen tarvetta voidaan joutua arvioimaan kunkin tiedon osalta myös rekisteröidyn kuoleman jälkeen. Tietojen säilyttämiselle kuoleman jälkeen voi olla perusteena esimerkiksi omaisten oikeuksien toteutuminen, vaikkakin lähtökohtaisesti kuolleen henkilön tiedot siirretään yleisen edun mukaisella perusteella arkistoitavaksi tai tuhotaan, jos arkistoinnille ei ole perusteita.[587] Tähän liittyen huomioitavana esimerkkinä ovat useat digitaalisen palvelun tarjoajat, jotka ovat hyväksymistä vaativissa käyttöehdoissaan maininneet palvelujen säännöistä kuoleman varalta. Muun muassa Facebookissa on mahdollista jättää oma tili ”perinnöksi” valitsemalleen henkilöille, kun vastakohtaisesti esimerkiksi joidenkin muiden digitaalisten palveluiden käyttäjätilit saatetaan käyttöehtojen mukaisesti poistaa tai deaktivoida käyttämättömyyteen liittyvän aikarajan puitteissa.[588]

Organisaation tietojenkäsittelyssä ei ole riittävää ainoastaan tunnistaa, onko kyseessä luonnollista henkilöä koskeva henkilötieto. Jokaisen työntekijän on kyettävä myös tunnistamaan, onko kyseessä nimenomaan tietosuoja-asetuksen mukainen arkaluontoinen, erityinen henkilötieto. Arkaluontoisten henkilötietojen käsittely on ollut lähtökohtaisesti kiellettyä tai rajoitettua jo kansallisessa henkilötietolaissa [589] . Tietosuoja-asetuksen 9 artiklassa henkilötietolain mukaisista

[584] Kemppinen 2011: 123.
[585] Saarenpää 2016a: 220.
[586] Voutilainen 2019: 41.
[587] Voutilainen 2019: 89; PeVL 31/2017 vp: 6.
[588] Shelly 2020: 31–32.
[589] Kumotun henkilötietolain arkaluontoisia henkilötietoja olivat sellaiset tiedot, joista ilmeni henkilön:

1. Rotu tai etninen alkuperä

arkaluontoisista henkilötiedoista käytetään termiä henkilötietojen erityisryhmät tai erityiset henkilötietoryhmät. Erityisten henkilötietoryhmien henkilötietojen käsittely on myös pääsääntöisesti kiellettyä. Asetuksessa tällaisia erityisiin henkilötietoryhmiin kuuluvia arkaluontoisia henkilötietoja ovat henkilön rotu tai etninen alkuperä, seksuaalinen suuntautuneisuus tai käyttäytyminen, uskonnollinen tai filosofinen vakaumus, poliittiset mielipiteet, ammattiliiton jäsenyys tai terveyden tila. Myös geneettisten ja biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten koskeva käsittely on kiellettyä arkaluontoisena, erityisenä henkilötietona. Rikkomuksiin ja rikostuomioihin liittyvistä henkilötietojen käsittelystä on säädetty erikseen asetuksen 10 artiklassa, joten asetuksessa ei katsota näitä henkilötietoja samalla tavalla arkaluontoiseksi kuin henkilötietolaissa katsottiin[590].

Kuitenkin pieniä eroavaisuuksia lukuun ottamatta kumotun henkilötietolain ja tietosuoja-asetuksen arkaluontoiset, erityiset henkilötiedot ovat suurimmaksi osaksi tyypiltään samankaltaisia. Tietosuoja-asetus myös korostaa, että jäsenvaltioille on annettu liikkumavaraa sääntöjen täsmentämisen suhteen erityisten henkilötietojen osalta.

Tietosuoja-asetuksen myötä geneettiset ja biometriset tiedot ovat osana tunnistamista erityistä henkilötietoa, mikä on eräänlainen teknologian kehittymisen tuoma lainsäädännöllinen lisäys. Biometrisia tietoja ovat esimerkiksi kasvokuvat, sormenjäljet, silmän iiris ja ääni[591]. Valokuvat, joista voidaan tunnistaa henkilö, ovat luonnollisestikin henkilötietoa. Asetuksen mukaan kuitenkin valokuvien käsittely biometrisena tietona ei ole automaattisesti erityisten henkilötietojen käsittelyä, paitsi jos niitä käsitellään erityisin teknisin menetelmin mahdollistaen luonnollisen henkilön tunnistamisen tai todentamisen. Esimerkkinä kameravalvonta, jota käytetään henkilön tunnistamista varten (eli se omaisi kasvontunnistustekniikan), on tietosuoja-asetuksen mukaista biometristen tietojen käsittelyä henkilön yksiselitteistä tunnistamista varten. Tietosuoja-asetuksen mukaan geneettisiä tietoja ovat geneettiset ominaisuudet, jotka on saatu luonnollisen henkilön biologisesta näytteestä analysoimalla. Geneettisistä tiedoista on mahdollista saada nimenomaan selville henkilön terveystietoja, jonka vuoksi nämä tiedot ovat

2. Yhteiskunnallinen, poliittinen tai uskonnollinen vakaumus
3. Ammattiliittoon kuuluminen
4. Rikollinen teko, rangaistus tai muu rikoksen seuraamus
5. Terveydentila, sairaus, vammaisuus tai henkilöön kohdistuvat huoltotoimenpiteet
6. Seksuaalinen suuntautuminen tai käyttäytyminen
7. Sosiaalihuollon tarve tai saamat sosiaalihuollon palvelut tai etuudet.

[590] Huomioitava on myös rikosasioiden tietosuojalaki, jossa on rikkomuksiin ja rikostuomioihin liittyvistä henkilötietojen käsittelystä on säädetty erikseen.
[591] Korja 2016b: 139–140.

arkaluontoisia tietoja. Muita perusteluja voi olla, että esimerkiksi oikeuskäytännössä sormenjälkien on katsottu sisältävän luonnollisia henkilöitä koskevia ainutkertaisia tietoja[592].

Erityisten henkilötietojen käsittelykieltoonkin liittyy poikkeuksia. Käsittelykieltoa ei luonnollisestikaan sovelleta, jos rekisteröity on antanut suostumuksensa kyseisten tietojen käsittelyyn tai käsittely koskee rekisteröidyn julkiseksi tekemiä henkilötietoja. Erityisten henkilötietojen käsittelykieltoa ei myöskään sovelleta tietyissä tilanteissa, joissa rekisteröidyn tai rekisterinpitäjän oikeudet tai velvoitteet tulisi toteutua. Esimerkiksi tällaisten tietojen käsittely voi olla tarpeen rekisteröidyn tai rekisterinpitäjän oikeuksien taikka velvoitteiden toteuttamiseksi sosiaalisen suojelun, työoikeuden tai sosiaaliturvan alalla. Onkin tyypillistä, että organisaatioissa työntekijöiden terveystietojen käsittely pohjautuu rekisterinpitäjän lakisääteiseen velvoitteiseen liittyen muun muassa palkan ja muiden etuuksien maksuun. Terveystietojen osalta on huomioitava se, että työnantaja saa käsitellä työntekijän terveystietoja vain, jos työntekijä itse toimittaa ne hänelle (rinnastuu suostumukseen) taikka jos työntekijä on antanut kirjallisen suostumuksen tällaisten tietojen luovuttamiseen työnantajalle[593].

Erityisten henkilötietojen käsittely voi olla myös tarpeen tuomioistuinten lainkäyttötehtävien suorittamiseksi tai oikeusvaateen luomiseksi, esittämiseksi, puolustamiseksi taikka muun muassa lääketieteellisten toimien, hoidon ja palvelun sekä työterveydenhuoltoa koskevien tarkoituksien toteuttamiseksi. Erityisten henkilötietojen käsittelykiellolle saattaa syntyä myös poikkeus, mikäli käsittely suoritetaan uskonnollisen, poliittisen, filosofisen tai ammattiliittotoimintaan liittyvän yhdistyksen, säätiön tai muun voittoa tavoittelemattoman yhteisön laillisen toiminnan yhteydessä, asianmukaisin suojatoimin sekä käsittelyn koskiessa ainoastaan nykyisiä tai entisiä jäseniä taikka henkilöitä, joilla on säännölliset ja tarkoituksenmukaiset yhteydet yhteisöön. Loput poikkeukset erityisten henkilötietojen käsittelyyn koskevat lähinnä erinäisten etujen suojelemista. Tällainen poikkeus käsittelykieltoon syntyy esimerkiksi, mikäli käsittely on tarpeen yleistä etua koskevasta syystä taikka käsittelytarpeen muodostaa yleisen edun mukainen arkistointi taikka tieteellinen, historiallinen tai tilastollinen tutkimustarkoitus. Poikkeus saattaa myös syntyä, mikäli käsittely on välttämätöntä elintärkeiden etujen suojelemiseksi tai käsittely on tarpeen kansanterveyteen liittyvän yleisen edun vuoksi. Tällöinkin

---

[592] Ks. EUT 17.10.2013 C-291/12 Schwarz.

[593] Koskinen & Ullakonoja 2020: 94–95. Tällöinkään työnantaja ei saa käsitellä mitä tahansa terveystietoja työntekijän suostumuksella, vaan ainoastaan esimerkiksi sairausajan palkan tai muiden siihen rinnastettavien etuuksien suorittamiseksi, tai sen selvittämiseksi, onko poissaoloon perusteltu syy. Lisäksi työntekijän pyynnöstä työkykyselvitykset asettavat poikkeuksen terveystietojen käsittelylle, kuin myös muun lainsäädännön, kuten työturvallisuuslain, velvoitteet. (Ibid. s. 94–95)

tulee ottaa huomioon käsittelytarkoituksen oikeasuhteisuus, henkilötietojen suoja sekä erityiset toimenpiteet rekisteröidyn etujen ja perusoikeuksien suojaamiseksi.

Kansallisessa tietosuojalaissa (1050/2018) ei ole tehty lisäyksiä tietosuoja-asetuksen erityisten henkilötietotyyppien suhteen. Lain 6 §:ssä on kuitenkin säädetty erikseen tietyistä tilanteista, jolloin erityisiä henkilötietoryhmiä koskeva käsittely on sallittua. Lisäksi kyseisessä pykälässä on myös täsmennetty, että tällöin tulee toteuttaa asianmukaisia ja erityisiä tietoturvatoimenpiteitä[594] rekisteröidyn suojaamiseksi. Myös rikostuomioihin ja rikkomuksiin liittyvään käsittelyyn on asetettu poikkeuksia kansallisen tietosuojalain 7 §:ssä.

Tietosuoja-asetuksessa on erikseen täsmennetty, että perusoikeuksien ja -vapauksien kannalta erityisiä henkilötietoja on suojeltava tarkasti, koska niiden käsittelyn asiayhteys voi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille. Asiantilaa ilmentää erityisen hyvin ratkaisu **KKO 2014:86**:

> *Erikoislääkäri A oli lukenut puolisonsa sukulaisen B:n potilastietoja potilastietojärjestelmästä, vaikka heidän välillänsä ei ollut potilassuhdetta. Näin ollen tietosuojan edellyttämä käyttötarkoitussidonnaisuus puuttui eikä perustetta henkilötietojen käsittelylle ollut. Potilas B oli myös nimenomaan kieltänyt, että hänen tietojaan ei saa kertoa A:lle. Potilastietojen katselu loukkasi sekä B:n yksityisyyttä että tietosuojaa. KKO totesi, että potilasasiakirjarekisterin tiedot olivat lain nojalla salassa pidettäviä ja että potilastietojen käsittely on mahdollista ainoastaan terveydenhuollon ammattihenkilön osallistuessa kyseisen potilaan hoitoon tai siihen liittyviin muihin tehtäviin. KKO myös painotti, että potilaan oikeus yksityisyyteen on turvattu viime kädessä perustuslain 10 §:ssä. Koska psykiatrisessa hoidossa käsitellään poikkeuksellisen arkaluontoisia potilastietoja, yksityisyyden suojaa koskevat normit saavat erityistä painoa tulkinnassa.*

KKO katsoi ratkaisussaan, että erikoislääkäri A:n tehtäviä ja vastuita ei ollut määritelty kovin täsmällisesti, mutta A:lla oli työtehtäviensä perusteella lähtökohtaisesti oikeus tarkastella poliklinikan toisen lääkärin hoidettavana olevan potilaan potilastietoja hoidon asianmukaisuuden selvittämiseksi. Potilastietojen käyttöoikeus on KKO:n mukaan kuitenkin aina harkittava tapauskohtaisesti huomioon ottaen potilaan oikeus yksityisyyteen. Näin ollen A loukkasi B:n oikeutta yksityisyyteen, koska B oli edellyttänyt, ettei A saanut tietää hänen potilastietojaan. Täten myös virkavelvollisuuden rikkominen oli tältä osin ollut tahallista.[595] Edellä olevan

[594] Näitä tietoturvatoimenpiteitä on käsitelty myöhemmin alaluvussa 3.3.5 (”Muut tietosuojalainsäädännön tietoturvavaatimukset”).
[595] Viljanen 2014: KKO:n ratkaisut kommentein 2014:II.

tapauksen mukaisesti voidaan todeta, että erityisesti arkaluontoisia potilastietoja käsitellessä, yksityisyyden suojaa koskevat normit saavat painoa tulkinnassa ja oikeus yksityisyyteen on viime kädessä turvattu perustuslain 10 §:ssä. Tapaus myös korostaa hyviä tietoturvallisia käytänteitä, joiden mukaan esimerkiksi pääsynhallintaa tulisi toteuttaa vähimpien oikeuksien periaatteen ja *need-to-know*-periaatteen mukaisesti eli esimerkiksi käyttöoikeudet tulisi määritellä sekä oikeuksien ja valtuutuksien tulisi olla tehtävien suorittamiseksi välttämättömiä. Kyseisen tapauksen virkavelvollisuuden rikkomista ei kuitenkaan olisi välttämättä voitu estää ainoastaan järjestelmän pääsynhallintaa koventamalla, sillä tällaisten yksityisyyden loukkausten torjuminen vaatii myös niin sanottua tietoisuuden lisäämistä ja asennekasvatusta. Käytännössä jokaisen henkilökunnan jäsenen roolit, tehtävät ja tietoturvavastuut tulisi määritellä. Myös henkilökunnan kouluttamisella ja tietoisuuden ylläpitämisellä voidaan mahdollisesti ehkäistä sekä tietosuojaan että tietoturvaan liittyviä vahinkoja ja tahallisia tekoja[596].

Tietosuoja-asetuksen myötä henkilörekisteririkos korvattiin tietosuojarikos-nimikkeellä (RL 38 luku 9 §), jolloin rikosoikeudellinen vastuu tulee kyseeseen vain tilanteissa, joissa lainvastainen henkilötietojen käsittely ei ole asetuksessa säädettyjen hallinnollisten seuraamusmaksujen piirissä. Täten tietosuojarikoksen säännös tulee sovellettavaksi ainoastaan silloin, kun henkilön ei voida katsoa toimineen rekisterinpitäjän tai henkilötietojen käsittelijän roolissa. Tästä esimerkkinä on uteliaisuudesta henkilötietojen urkkiminen ilman käsittelyyn liittyvää oikeuttavaa perustetta. Tietosuojarikoksen soveltamisalan määrittäminen on haastavaa, koska tietosuojaa koskevaa EU-oikeudellista ja kansallista lainsäädäntöä on paljon.[597] Siinä missä tietosuoja-asetuksen sanktiot koskevat organisaatioita, tietosuojarikos voi koskea yksittäistä henkilöä. Tällaiset yksittäiset henkilöt voivat esimerkiksi työskennellä organisaatiossa rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa, mutta toimia tietojenkäsittelyyn liittyvien ohjeiden ja sääntöjen vastaisesti, kuten edellä käsitellyssä tapauksessa **KKO 2014:86**. Käsitellyssä tapauksessa on kuitenkin kyse virkavelvollisuuden rikkomisesta, sillä virkavelvollisuuden rikkomisen tai tuottamuksellisen virkavelvollisuuden rikkomisen rikosnimikkeitä on käytetty syytteissä ja katsottu syyksi luetuksi rikokseksi erityisesti silloin, kun teko on vanhentunut henkilörekisteririkoksena, jonka vanhentumisaika oli 2 vuotta nykyisen tietosuojarikoksen tavoin. Virkarikosten vanhentumisaika on 5 vuotta.[598]

[596] Ks. lisää aiheesta luvusta 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).
[597] HE 9/2018 vp: 123–124, 128; Melander & Rautio 2022: 1311.
[598] Voutilainen 2019: 216.

Virkavelvollisuuden rikkomisen tulee olla selvä ja moitittava. Virkavelvollisuuden rikkomisena voidaan muun muassa pitää sitä, kun virkamies ei käyttäydy asemansa ja tehtäviensä edellyttämällä tavalla eikä toimi asianmukaisesti ja viivytyksettä siten kuin virkamieslaeissa on edellytetty. Tapauksen **KKO 2014:86** mukaisesti virkavelvollisuuden rikkominen tulee kyseeseen, kun virkamies laiminlyö tiedon käyttämistä koskevia erityisiä rajoituksia.[599] Tässä tapauksessa rikkomisen osalta kyseessä on muun muassa potilastietojen perusteeton katselu työelämän tietosuojalain 5 §:n vastaisesti[600]. Ratkaisussa **KKO 2014:86** virkavelvollisuuden rikkomisen katsottiin olevan tahallista, mikä vahvisti kantaa, jonka mukaan virkarikoksissa tietoisuus lain sisällöstä asemoituu tahallisuus- ja tuottamuskysymykseksi. Näin ollen myös tahallisuuteen kuuluvan tietoisuuden tulee kohdistua laissa säädettyihin virkavelvollisuuksiin.[601]

Organisaatioissa tulisi henkilötietojen ja erityisten henkilötietojen tunnistamisen ja näihin liittyvän tietoisuuden lisäämisen ohella myös ohjeistaa henkilökuntaa henkilötunnuksien käsittelystä. Tämä on aiheellista, koska henkilötunnus on *riskitieto*, jonka käyttöä on pyrittävä rajoittamaan[602]. Sitä ei saa käyttää minkäänlaisena avainlukuna henkilön tunnistamisessa. Lisäksi esimerkiksi digitaalisten palveluiden suunnittelussa on huomioitava, että henkilötunnuksen käsittely ei ole perustelua pelkästään tietojärjestelmän toiminnallisuuksiin liittyvillä syillä tai siitä syystä, että rekisteröidyn yksilöiminen tai hänen henkilötietojensa käsittely nopeutuisi.[603] Henkilötunnuksesta on tietosuoja-asetuksessa ainoastaan maininta 87 artiklassa, jonka mukaan jäsenvaltiot voivat määritellä tarkemmin henkilötunnuksen käsittelyn edellytyksistä. Täten kansallisen tietosuojalain 29 §:ssä on erikseen säädetty henkilötunnuksen käsittelystä. Pääsääntöisesti henkilötunnusta saa käsitellä rekisteröidyn suostumuksella. Säännöksessä on myös täsmennetty, että henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi, laissa säädetyn tehtävän suorittamiseksi taikka historiallista, tieteellistä tutkimusta tai tilastointia varten. Henkilötunnusta saa käsitellä myös muun muassa vuokraus- ja lainaustoiminnassa, terveydenhuollossa, luotonannossa sekä muita virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa. Lain 29 § on hyvinkin yksityiskohtainen liittyen henkilötunnuksen käsittelyn tilanteisiin. Laissa on myös erikseen mainittu, että henkilötunnusta ei tule merkitä tarpeettomasti henkilörekisterin perusteella laadittuihin tai tulostettuihin asiakirjoihin. Lisäksi rekisteröidyn henkilöllisyyden selvittämiseen ei saa käyttää

[599] Mäenpää 2017: 445; Mäenpää 2016: 462.
[600] Koskinen & Kulla 2019: 270–271.
[601] Kallio & Rikander 2021: 349–350.
[602] Saarenpää & Riekkinen 2023: 239.
[603] Voutilainen 2023: 101–102.

yksinomaan henkilötunnusta tai henkilötunnuksen ja rekisteröidyn nimen yhdistelmää. Henkilötunnusta ei saa käyttää esimerkiksi jäsenrekisterissä, sillä yksilöintiin riittää jäsennumero tai vastaava[604].

Henkilötunnuksen käsittelystä on myös säädetty tunnistus- ja luottamuspalvelulaissa (617/2009, laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista) 6 §:ssä vahvan sähköisen tunnistautumisen osalta. Säännöksen mukaan tunnistuspalvelun tarjoajan ja luottamuspalveluja tarjoavan varmentajan tulee tarkastaa hakijalta tämän henkilötunnus tarkastaessaan hakijan henkilöllisyys. Vahvan sähköisen tunnistautumisen osalta käsittelyperuste ja käyttötarkoitussidonnaisuus perustuu pitkälti tunnistusvälineen käyttäjän ja tunnistuspalvelun tarjoajan väliseen sopimukseen. Lisäksi tunnistukseen luottavalla asiointipalvelulla on sopimus tunnistusvälityspalvelun kanssa. Koska palvelu perustuu sopimuksiin ja käyttäjän käynnistämään asiointiin, henkilötietojen käsittelyperustetta on perusteltua arvioida ensisijaisesti yleisen tietosuoja-asetuksen sopimukseen perustuvan käsittelyperusteen kannalta. Mahdollinen voisi olla myös lakisääteiseen tehtävään liittyvä käsittelyperuste. Henkilötunnuksen käsittely tunnistuspalvelun ja tunnistamiseen tai sähköisiin allekirjoituksiin liittyvän varmennepalvelun yhteydessä on katsottu välttämättömäksi sen takia, että palveluiden toteuttaminen luotettavasti edellyttää henkilöiden varmaa erottamista toisistaan.[605]

Henkilötunnusta ei ole säädetty missään yleislaissa täysin salassa pidettäväksi, mutta sitä on käsiteltävä huolellisesti ja varoen. Tietoverkoissa henkilötunnuksen käsittelyyn on kiinnitetty erityishuomiota osana varovaisuusperiaatetta ja riskiperusteisuutta. Esimerkiksi **apulaisoikeusasiamiehen ratkaisussa 2455/2016** pidettiin perusteltuna sitä, ettei viranomainen pyydä aktiivisesti asiakasta toimittamaan henkilötunnustaan viranomaisen suojaamatonta sähköpostiyhteyttä käyttäen, sillä suojaamattomaan sähköpostiyhteyteen liittyy tietoturvaongelmia. Tähän liittyy myös huolellisuusvelvoite, jonka myötä kaikkien henkilötietojen käsittelyssä on noudattava erityistä huolellisuutta. Tällöin rekisterinpitäjän on ennalta ja oma-aloitteisesti varmistettava, että rekisteröityjen henkilötietojen suoja ei vaarannu käsittelyssä. Näin ollen huolellisuusvelvoitteeseen on katsottu kuuluvaksi, että viranomainen ei voi pyytää asiakasta toimittamaan henkilötietoja tavalla, joka aiheuttaa riskin tietojen joutumisesta asiattomien saataville. Apulaisoikeusasiamiehen ratkaisun mukaan viranomaisen ei tulisi myöskään jättää asiakkaalle sellaista mielikuvaa, että asiakkaan tulisi käyttää suojaamatonta sähköpostia saadakseen asiansa hoidetuksi.[606]

---

[604] Järvinen 2022a: 25.
[605] HE 237/2020 vp: 12–14.
[606] Voutilainen 2019: 133–134, 178–179; EOAK 2455/2016: 4.

Apulaisoikeusasiamiehen tulkinnan mukaan henkilötunnusta ei myöskään saa käsitellä sellaisen syyn takia, jossa tietojärjestelmän ominaisuudet sitä vaativat tai, että tietojen käsittely on henkilötunnuksen avulla helpompaa tai nopeampaa. Esimerkiksi työnantaja ei voi täten käyttää työntekijöidensä henkilötunnuksia järjestelmiensä käyttäjien yksilöintiin, vaan tämä tulee tehdä työnantajan luoman käyttäjätunnuksen tai muun tunnuksen avulla.[607] Henkilötunnusta saa käsitellä lähinnä tapauksissa, joissa yksilöinti on erityisen tärkeää henkilön itsensä kannalta eli ei niinkään käsittelevän organisaation kannalta[608].

Yhteenvetona todettakoon, että organisaation toiminnassa on tärkeää tunnistaa, mikä on henkilötietoa ja onko kyseessä niin sanotusti tavallinen henkilötieto, erityinen henkilötieto vai esimerkiksi riskitietona toimiva henkilötunnus. Lisäksi on huomioitava, että tietosuoja-asetusta ei lähtökohtaisesti sovelleta kuolleisiin henkilöihin, mutta yksityiselämän ja henkilötietojen suoja ulottuvat kuolleen henkilötiedoista suoraan tai epäsuorasti tunnistettaviin muihin luonnollisiin, elossa oleviin henkilöihin. Henkilötietotyyppien tunnistamisen ohella pitää myös pystyä arvioimaan, onko kyseessä julkista vai salassa pidettävää henkilötietoa. Yksityiselämän suojan alaan kuuluvat henkilötiedot ovat tyypillisesti salassa pidettäviä. Vastakohtaisesti julkisia henkilötietoja ovat tiedot, jotka ovat julkisesti saatavilla. Esimerkiksi organisaationäkökulmasta julkisia henkilötietoja ovat yrityksen kotisivuilla olevat työntekijöiden nimi- ja yhteystiedot. Henkilötietojen tunnistaminen vaatii käsittelytoimi- ja järjestelmäkohtaista harkintaa sekä tapauskohtaista arviointia. Henkilötietotyypin ja henkilötietojen luokittelun tunnistamisen kautta määrittyvät tietoturvatoimenpiteet henkilötietojen suojaamiseksi. Esimerkiksi erityisten henkilötietojen, kuten terveystietojen, osalta on täsmennetty tietosuojalain 6 §:ssä vaadittavat erityiset tietoturvatoimenpiteet, koska käsittely voi aiheuttaa huomattavia riskejä yksilöiden oikeuksille ja vapauksille. Tietoturvatoimenpiteiden määrittelyyn liittyy myös olennaisesti se, onko henkilötiedot suoraan vai epäsuorasti tunnistettavissa. Erityisesti epäsuorasti yksilöitävien henkilötietojen tunnistaminen on haasteellista organisaatioissa. Esimerkiksi IP-osoitteet lähes poikkeuksetta luokitellaan henkilötiedoksi organisaatioissa, vaikka asiassa tulisi punnita, onko organisaation tosiasiallisesti mahdollista saada käsiinsä sellaisia tietoja, joita yhdistelemällä IP-osoitteen mahdollisesti takana oleva luonnollinen henkilö olisi tunnistettavissa. Asiaa arvioitaessa tulisi kiinnittää tapauskohtaista huomiota organisaation IP-osoitteita käsittelevän palvelun luonteeseen, IP-osoitteiden käyttötarkoitukseen sekä toimialakohtaisiin eroavaisuuksiin sen osalta, kuinka todennäköisesti organisaatio saisi tietojen yhdistelemiseen käytettäviä lisätietoja olemassa olevien oikeudellisten keinojen avulla. Mikäli IP-osoitteet katsottaisiin henkilötiedoksi, tulee myös arvioida, muodostuuko niistä sellainen

[607] EOAK 1777/4/08; Voutilainen 2019: 180–181.
[608] Järvinen 2022a: 25.

rekisteri, jossa organisaatio on rekisterinpitäjä. Organisaation tulee tunnistaa rekisterinpitäjyytensä, sillä sen myötä määräytyvät muut tietosuojalainsäädännön mukaiset velvollisuudet ja vastuut. Usein kiire tai osaamisen puute johtavat siihen, että organisaatioissa ei tunnisteta riittävällä tasolla henkilötietoja tietojenkäsittelytoimien yhteydessä eikä näin myöskään omaa rekisterinpitäjyyttä. Tällöin tietoturvatoimenpiteet tietojen suojaamiseksi saattavat olla riittämättömällä tasolla[609].

3.2.2 Henkilötietojen käsittely ja henkilörekisteri

Tietosuoja-asetusta sovelletaan artiklojen 2 ja 3 mukaisesti nimenomaan henkilötietojen käsittelyyn. Näin ollen henkilötietojen tunnistamisen ohella on myös olennaista tunnistaa, mikä on henkilötietojen käsittelyä. Esimerkiksi organisaation tietoturvatoimenpiteet saattavat jo itsessään sisältää henkilötietojen käsittelyä. Näistä tietoturvatoimenpiteistä esimerkkinä ovat muun muassa tietynlaiset järjestelmien lokit, pääsynvalvonnan tunnistetiedot ja kameravalvonnan tallenteet.

Huomioitava on, että henkilötietojen käsittelylle pitää aina löytyä peruste laista. Käsittelyksi katsotaan toiminnot, joita kohdistetaan henkilötietoihin taikka henkilötietoja sisältäviin tietojoukkoihin manuaalisesti taikka automaattista tietojenkäsittelyä käyttäen. Koska tietosuoja-asetus on säädetty teknologianeutraalisuuden periaatetta kunnioittaen, tulee sitä sovellettaessa ottaa huomioon, että automaattiseen tietojenkäsittelyyn käytettäviä keinoja tulee tulkita laajasti kattaen kaikki erilaiset teknologiset vaihtoehdot tietokoneista älypuhelimiin sekä muihin älylaitteisiin[610].

Varsinaisia tietojenkäsittelytoimia ovat muun muassa tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, hakua, kyselyä, käyttöä, tietojen yhteensovittamista tai yhdistämistä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, rajoittamista, poistamista tai tuhoamista. Näin ollen tietosuoja-asetuksen mukaan henkilötietojen käsittelyn raja-arvot ylitetään helpostikin, sillä jo haku tai säilyttäminen katsotaan käsittelyksi. Raja-arvojen helppo ylittäminen henkilötietojen käsittelyssä aiheuttavat käytännön työssä ongelmia esimerkiksi lokitietojen keräämisen ja hakemisen sekä varmuuskopioiden säilyttämisen suhteen[611]. Tähän liittyy läheisesti

[609] Riskien mitigoimiseksi organisaation tietosuojan tasoa on mahdollista nostaa ohjeistuksilla, säännöllisellä ja pakollisella koulutuksella sekä tietoisuuden ylläpitämisellä, ks. luku 3.3.1 (”Sääntelyjärjestelmän dokumentaatiovaatimukset”) sekä 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).
[610] Lentzis 2020: 21.
[611] Lokitusta ja varmuuskopiointia on käsitelty mm. luvussa 3.5.4 (”Muu teknisin menetelmin toteutettu valvonta ja välitystiedot”), luvussa 4.4.2 (”Järjestelmien

esimerkiksi käyttötarkoitussidonnaisuuden periaate, jonka mukaan henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten. Tietoja ei saa myöskään käsitellä määriteltyjen laillisten tarkoitusten kanssa yhteen sopimattomalla tavalla myöhemmin, poissulkien kuitenkin yleisen edun mukainen arkistointi taikka tieteellinen, historiallinen tai tilastollinen tutkimustarkoitus. Käyttötarkoitussidonnaisuus ei kiellä käsittelemästä yhtä tarkoitusta varten kerättyjä tietoja myös toista käyttötarkoitusta varten, mikäli se ei ole yhteensopimatonta alkuperäisen käyttötarkoituksen kanssa[612].

Vanhassa henkilötietolaissa ei ollut määritelty erikseen edellä mainituista käsittelytoimista tietojen jäsentämistä, hakua, kyselyä tai rajoittamista. Toisaalta vanhassa henkilötietolaissa oli termi ”muut henkilötietoihin kohdistuvat toimenpiteet”, joten nämä kaikki muut mainitsemattomat käsittelytoimet voidaan katsoa sisältyvän siihen määritelmään. Vanhassa henkilötietolaissa henkilötietojen käsittelyksi katsottiin myös henkilötietojen suojaaminen, mitä sen sijaan ei ole mainittu tietosuoja-asetuksessa. Todennäköisesti suojaaminen katsotaan tietosuoja-asetuksessa itsestäänselvyydeksi, sillä jo pelkästään asetuksen olemassaolon tavoitteena on henkilötietojen suojaamisen edistäminen.

Tietosuoja-asetuksen määrittelemät käsittelytoimet ovat täten varsin kattavat. Tietosuoja-asetus ei kuitenkaan rajoita sitä, mitä työntekijät puhuvat keskenään, sillä henkilötietojen käsittely puhuen ei kuulu tietosuoja-asetuksen soveltamisen piiriin[613]. Tällöin tietoturvan ja hyvien käytäntöjen kannalta huomioon otettavaksi tulevat salassapitosäännökset, salassapitosopimukset ja maalaisjärki. Henkilökunnan tietoturvakoulutuksessa on hyvä täsmentää tietojen käsittelyn suhteen hyviä käytäntöjä luottamuksellisten tietojen puhumisesta (ja myös muunlaisesta tietojen käsittelystä) esimerkiksi julkisissa tiloissa, kulkuneuvoissa taikka kotona etätyötä tehdessä. Huomioitava on, että kaikki luottamuksellinen tieto ei kuulu automaattisesti kaikille kollegoille.

Mikä tahansa jäsenneltyjä henkilötietoja sisältävä tietojoukko muodostaa henkilörekisterin, josta tiedot ovat saatavilla tietyin perustein, esimerkiksi toiminnallisin tai maantieteellisin perustein[614]. Henkilörekisterien osalta suuri haaste liittyy siihen, että henkilörekisteri voi olla osittain tai kokonaan tietoverkoissa, joissa erilaiset toiminnot ovat sulautuneet yhteen. Digitalisoitumisen myötä perinteiset

lokitusvaatimukset tietoturvan sääntelyjärjestelmässä”) ja 4.4.4 (”Varmuuskopioinnin ja toipumisen vaatimukset sääntelyjärjestelmässä”).

[612] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 103.

[613] Nyyssönen 2018: 40, 46.

[614] Ks. myös rikosasioiden tietosuojalaki 1054/2018, jonka 3 §:n mukaan rekisterillä tarkoitetaan jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein ja riippumatta siitä, onko tietojoukko keskitetty, hajautettu taikka toiminnallisin tai maantieteellisin perustein jaettu.

kanavat sulautuvat bittijonoiksi. Asiakirjoista voidaan antaa tietoja tietoverkoissa ja viestinnän kannalta tietoverkoissa on tekstin lisäksi kuvia, videoita ja ääntä.[615] Yksi suuri haaste organisaatioiden tietosuojassa on myös se, että digitalisoitumisen myötä erilaisia mahdollisia digitaalisia tiedon säilytyspaikkoja on niin monia, että voi olla vaikeaa hahmottaa ja tunnistaa kaikki henkilörekisterit. Tämä haaste vaikeuttaa tiedon suojaamista ja oikeanlaista käsittelyä sen koko elinkaaren ajalta. Esimerkiksi työskennellessä (henkilö)tieto saattaa helposti siirtyä sähköpostista pilvisynkronoituihin henkilökohtaisiin työkansioihin, sieltä puolestaan Teamsin jaettuihin työtiloihin ja sieltä mahdollisesti asianhallintajärjestelmään, tiketöintijärjestelmään tai vaikkapa asiakastyötilaan. Näin ollen sama henkilötietoa sisältävä dokumentti saattaa kulkea monen tietojen käsittelypaikan läpi, mutta myös jäädä sinne pidemmäksikin aikaa.

Tietojen käsittelyn monipuolistumisen takia, olisikin tärkeää tunnistaa erityisesti organisaation loogiset rekisterit tai henkilötietovarannot. Loogisella rekisterillä tarkoitetaan tässä yhteydessä henkilörekisteriä, johon luetaan kuuluviksi kaikki ne tiedot, joita käytetään samassa käyttöyhteydessä riippumatta siitä, miten ja mihin ne on tallennettu[616]. Loogisten rekistereiden tunnistaminen on myös tärkeä osa tiedonhallintalain 5 §:n mukaista viranomaisen tiedonhallintamallia, jossa tulee kuvata tiedonhallintayksikön tietovarantoja. Lain mukaan tietovarannolla tarkoitetaan viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettävää tietoaineistoja sisältävää kokonaisuutta, jota käsitellään tietojärjestelmien avulla tai manuaalisesti. Näin ollen lain velvoittamaa tiedonhallintamallia luodessa tulee luoda sellainen malli, jossa loogisten henkilörekistereiden (tai henkilötietovarantojen) ja viranomaisen tietovarantojen yhteensovittaminen huomioidaan.

Käsitteistön ja rekistereiden osalta huomioitava on tässä kohtaa myös tietokannat ja järjestelmät. Rekisterillä ja tietokannalla tarkoitetaan samaa asiaa, mikäli tietokanta sisältää henkilötietoja[617]. Rekisteri voi olla myös järjestelmä. Esimerkiksi joissain tapauksissa lokijärjestelmien lokit katsotaan henkilörekistereiksi[618]. Ratkaisussa **KHO 27.9.2013 taltio 3084** ei ole kuitenkaan katsottu tapahtumalokin muodostavan henkilörekisteriä:

> *Potilaan tutkimuksessa käytetyn laitteen tapahtumaloki sisälsi laitteen toimintaa kuvaavia tietoja, mutta ei luonnollista henkilöä, hänen ominaisuuksiaan tai elinolosuhteita kuvaavia tietoja. Tapahtumalokin tietoja yhdistelemällä potilasrekisterin tietoihin voidaan mahdollisesti saada selville tunnistettavissa olevan potilaan hoitoon liittyviä seikkoja. KHO:n*

[615] Neuvonen 2019: 178–179.
[616] TSV 9.10.2019, dnro. 1689/41/17.
[617] Voutilainen 2019: 40.
[618] Andreasson, Koivisto & Ylipartanen 2013: 81.

> *päätöksessä tulee kuitenkin ilmi, että tapahtumalokin ei silti katsota muodostavan henkilörekisteriä.*

Tapahtumaloki sisältää laitteen toimintaa kuvaavia tietoja. KHO:n ratkaisun perusteella tapahtumalokin ei katsottu olevan henkilörekisteri, vaikka laitteen lokitietoja potilasrekisterin tietoihin yhdistelemällä voitiin mahdollisesti saada selville tunnistettavissa olevan potilaan hoitoon liittyviä seikkoja[619]. Tämä ratkaisu on tosin kumotun henkilötietolain ajoilta, jossa esimerkiksi käsite henkilötieto oli suppeammin määritelty kuin tietosuoja-asetuksessa. Tietosuoja-asetuksessa henkilötiedolla viitataan luonnollista henkilöä koskeviin tietoihin, jotka ovat tunnistettavissa myös epäsuorasti eli välillisesti esimerkiksi yhdistelemällä tietoja. Tietosuoja-asetuksen perusteella rekisteri muodostuu jäsennellyistä henkilötiedoista sisältyvästä tietojoukosta, josta tiedot ovat saatavilla tietyin perustein. Näin ollen, jos tapahtumalokissa olevat tiedot ovat välillisesti katsottuna henkilötietoja ja ne olisivat jäsenneltävissä, olisi tapahtumaloki tietosuoja-asetuksen mukainen rekisteri.

Rekisterimääritelmän ulkopuolelle on jätetty henkilökohtaisiin tai tavanomaisiin yksityisiin tarkoituksiin kerätyt henkilötiedot. Tällaisia ovat esimerkiksi henkilökohtaisten matkapuhelimen henkilöluettelot.[620] Olennaista tässä arvioinnissa on yksityisiin tarkoituksiin tarkoitettu henkilötietojen keräys. Yksityisiin tarkoituksiin tapahtuvia henkilökohtaisia käyttötarkoituksia ovat muun muassa yksityisluontoinen ja tavanomainen sähköpostien käsittely, osoitteiston ylläpitäminen henkilökohtaista kontaktointia varten sekä henkilökohtaisiin tarkoituksiin tai kotitalouden piirissä tapahtuva muut sosiaaliseen verkostoitumiseen tarkoitetut käsittelyt[621]. Oikeuskäytännössä on katsottu muistiinpanojen keräämisen järjestötoiminnan tarkoituksiin jäävän tämän poikkeuksen ulkopuolelle, esimerkiksi ratkaisussa **KHO 2018:171**:

> *Jehovan todistajien keräämät ja muutoin käsittelemät henkilötiedot ovelta ovelle -saarnaamistyössä katsottiin korkeimman hallinto-oikeuden päätöksessä kielletyiksi. Kyseisten tietojen käsittely rikkoo henkilötietojen käsittelyn yleisiä edellytyksiä. Lisäksi saarnaamistyössä tehdyt muistiinpanot voitiin kiistatta pitää henkilötietoina ja joihinkin muistiinpanoihin saattoi sisältyä myös arkaluontoisia henkilötietoja. KHO:n ratkaisun mukaan henkilötietojen kerääminen ja käsittely yksittäisten Jehovan todistaja -jäsenten toimesta ei voitu verrata luonnollisen henkilön suorittamiin yksinomaan henkilökohtaisiin tai niihin verrattaviin*

[619] Pitkänen, Tiilikka & Warma 2013: 47.
[620] Kemppinen 2011: 121.
[621] Voutilainen 2019: 90.

> *tavanomaisiin yksityisiin tarkoituksiinsa tapahtuvaan keräämiseen ja käsittelyyn. Henkilötietoja sisältävistä paperisista ja sähköisistä muistiinpanoista muodostui täten henkilörekisteri tai sen osa. Unionin tuomioistuimen tuomiossa on myös katsottu, että uskonnollista yhdyskuntaa voidaan pitää yhdessä saarnaamistyötä harjoittavien jäsentensä kanssa rekisterinpitäjänä. Koska henkilötietojen käsittely ei perustu esimerkiksi laissa määritellyllä tavalla rekisteröidyn asiakassuhteeseen tai jäsenyyteen, käsittely edellyttää rekisteröidyn yksiselitteisesti antamaa suostumusta.*

Tietosuoja-asetusta sovelletaan lähtökohtaisesti aina automaattisessa henkilötietojen käsittelyssä. Manuaalisessa henkilötietojen käsittelyssä asetusta sovelletaan ainoastaan henkilötietojen muodostaessa rekisterin osan tai, kun henkilötietojen on tarkoitus muodostaa rekisterin osa[622]. Manuaalinen henkilötietojen prosessointi on ihmisten tekemää ilman koneiden käyttöä ja yleensä kyseessä on henkilötietojen käsittelyä paperisten dokumenttien muodossa yksityisten yritysten ja julkisten viranomaisten varmuuskopiointitarkoituksiin[623]. Näin ollen, kuten aikaisemmin on mainittu, esimerkiksi henkilötietojen käsittely puhuen ei kuulu tietosuoja-asetuksen soveltamisen piiriin. Toisaalta rekisterissä olevien tietojen luovuttaminen suullisesti kuuluu tietosuoja-asetuksen soveltamisen alaan.[624] Edellä mainitussa Jehovan todistajia koskevassa tapauksessa henkilötietojen käsittely oli manuaalista, jossa muistiinpanojen kerääminen järjestötoiminnan tarkoitukseen muodosti sen paperisen olomuodon takia henkilörekisterin osan, joka liitetään osaksi sähköistä henkilörekisteriä.

Lopuksi on huomioitava se, että tietosuoja-asetuksen aineellisen soveltamisalan ulkopuolelle on jätetty tiedostot, joita ei ole järjestetty tiettyjen kriteerien mukaan. Tämä johtuu siitä, että henkilötietojen poimimiseksi niistä tarvitaan erittäin korkeaa käsittelyä. **EUT:n ratkaisussa 10.7.2018 C25-17 Jehovan todistajat** on todettu, että rekisteröintijärjestelmän käsite kattaa ”kaikki sellaiset järjestetyt henkilötietojen kokoelmat, joista tiedot ovat saatavilla tietyin perustein, oli kokoelma sitten keskitetty, hajautettu tai maantieteellisin perustein jaettu. Kyseisessä Jehovan todistajien tapauksessa kerätyt henkilötiedot kerättiin ovelta ovelle -toiminnan yhteydessä tietyn maantieteellisen jakauman perusteella ja valmistelemalla myöhempiä vierailuja henkilöiden luokse, joiden kanssa hengellinen keskustelu on aloitettu. Lisäksi rekisteriä pidettiin henkilöistä, jotka eivät halua, että

[622] Nyyssönen 2018: 40, 46.
[623] Lentzis 2020: 21–22. Nykyisin kuitenkin paperisesta tietojen käsittelystä pyritään yhä enemmän luopumaan muun muassa tietoturvasyistä sekä varmuuskopioinnin ja arkistoinnin siirtyessä pilveen.
[624] Nyyssönen 2018: 40, 46.

heidän ovellaan käydään.[625] Tällöin kyseisiin kriteereihin kuului myös nimien ja osoitetietojen lisäksi tieto uskonnollisesta vakaumuksesta, joka on erityinen henkilötieto. Jehovan todistajia koskevassa tapauksessa EUT on tulkinnut rekisterinpitäjän käsitettä laajasti, jotta rekisteröidyn oikeudet voidaan turvata kattavasti ja tehokkaasti[626]. EUT:n tulkinta oli myös linjassa tietosuoja-asetuksen määritelmän kanssa, jonka mukaan rekisteri tarkoittaa jäsenneltyä henkilötietojoukkoa ja josta tiedot ovat saatavilla tietyin perustein.

Yhteenvetona todettakoon, että tietoturvatoimenpiteiden osalta henkilötietojen käsittelyn tunnistaminen on tärkeää, jotta pystytään arvioimaan käsittelyn riskejä sekä toteuttamaan käsittelyssä tehokkaita tietoturvatoimenpiteitä henkilötietojen suojaamiseksi. Käsittelytoimien tunnistaminen siten edesauttaa oikeanlaista tiedon hallintaa ja henkilötietojen käsittelyä. Henkilötietojen käsittelyn tulee olla sopivaa alkuperäisen, laillisen käyttötarkoituksen kanssa. Tietosuojalainsäädännössä määriteltyjen käsittelytoimien tunnistamisen osalta käytännön työssä haasteellista on tunnistaa, että erityisesti säilyttäminen, haut ja kyselyt ovat henkilötietojen käsittelyä. Tämä haaste korostunee tulevaisuudessa palveluiden digitalisoituessa ja tekoälypohjaisten sovellusten käyttöönoton myötä. Esimerkiksi tapauskohtaisesti kielimalleilla tehtävät promptit eli kyselyt saattavat organisaation järjestelmissä laajastikin käsitellä jo olemassa olevaa henkilötietoa lähdedatasta. Tällöin käsittelyssä hämärtyy ensinnäkin se, mihin kaikkialle tekoälyllä on pääsy, mihin tekoälyjärjestelmä kuljettaa (henkilö)tietoa ja minne sitä jää, sekä muodostuuko käsiteltävästä tekoälysovelluksen vastaustuloksesta sellaisia uusia käyttötarkoituksia henkilötiedolle, joka on ristiriidassa alkuperäisen, laillisen käyttötarkoituksen kanssa.

Henkilötietojen käsittely tulisi huomioida moninaisesti erilaisissa organisaation tietoturva- ja tiedonhallintakoulutuksissa eräänlaisena luottamuksellisen tiedon lisäulottuvuutena, johon kohdistuu erityisiä lakivaatimuksia. Huomioitava on myös se, että nykyisessä digitalisoituneessa ympäristössä tietojen käsittely on moninaistunut ja luottamuksellista tietoa käsitellään monessa erilaisessa järjestelmässä ja sitä siirretään sekä organisaation sisällä että organisaation ulkopuolelle. Digitalisoitumisen mahdollistama monipuolinen tietojen käsittely ja henkilötietojen siirto eri järjestelmien välillä aiheuttavat haasteita tiedon hallinnalle ja muun muassa henkilötietojen säilytysaikojen noudattamiselle ja minimikäsittelyn vaatimuksille. Tietoturvan näkökulmasta tiedon omistaja vastaa tiedon luokittelusta sekä tiedonsiirroissaan siitä, että kohdejärjestelmän turvallisuustaso on riittävä ja vastaisi vähintään lähdejärjestelmän turvallisuustasoa. Täten

[625] Lentzis 2020: 21.
[626] Korpisaari & Toikkanen 2020: 465.

henkilötietojoukkojen muodostamien loogisten rekisterikokonaisuuksien tunnistaminen on olennaista, jotta tietoturvatoimenpiteitä osataan toteuttaa oikein ja riittävällä tasolla.

3.2.3 Henkilötietojen käsittelyyn liittyvät roolit

Kaikki organisaatiot käsittelevät henkilötietoja enemmän tai vähemmän, minkä takia jokaisessa organisaatiossa tulee suojata näitä henkilötietoja asianmukaisilla tietoturvatoimenpiteillä. Luonnollinen henkilö, jonka henkilötietoja käsitellään, kutsutaan *rekisteröidyksi*. Esimerkiksi organisaation rekisterinpitäjyyden alla olevia rekisteröityjä ovat tyypillisesti organisaation työntekijät sekä sidosryhmät, kuten asiakkaat ja toimittajat. Näin ollen tietosuojalainsäädännön vaatimukset ulottuvat lähtökohtaisesti kaikkiin organisaatioihin.

Rekisteröityjen henkilötietojen suojaamisen päävastuu on rekisterinpitäjällä. *Rekisterinpitäjä* on luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä muiden kanssa määrittelee henkilötietojen käsittelyn keinot ja tarkoitukset. Mielenkiintoista on, että tietosuoja-asetuksessa *yritys*-käsitteen alla ovat sekä taloudellista toimintaa harjoittavat luonnolliset henkilöt että oikeushenkilöt, jolloin käsite eroaa perinteisestä (liike)yrityksen käsitteestä painottaen enemminkin toiminnan tarkoitusta kuin oikeudellista muotoa[627].

Yleisessä tietosuoja-asetuksessa on eroteltu *henkilötietojen käsittelijä* rekisterinpitäjästä, jonka tehtävänä on käsitellä henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi myös olla rekisterinpitäjän tavoin luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin. Henkilötietojen käsittelijöitä eivät ole rekisterinpitäjään palvelussuhteessa olevat luonnolliset henkilöt, vaan nämä toimivat osana rekisterinpitäjän toimintaa[628]. Henkilötietojen käsittelijöitä ovatkin näin ollen toiset organisaatiot ja niissä työskentelevät henkilöt, jotka käsittelevät henkilötietoja rekisterinpitäjäorganisaation ohjeiden mukaisesti.

Rekisterinpitäjällä on lähtökohtaisesti päävastuu henkilötietojen suojaamiseen liittyvistä tietoturvatoimenpiteiden toteutumisesta. Tietosuoja-asetuksen 28 artiklan mukaan rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely on tietosuoja-asetuksen vaatimuksien mukaista. Näin ollen rekisterinpitäjän on ikään kuin myös varmistettava lukuunsa toimivien henkilötietojen käsittelijöiden tietoturvan

[627] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 87.
[628] Voutilainen 2023: 73.

toteutuminen henkilötietojen suojaamiseksi. Ulkoistuksien ja hankintojen kohdalla tämä toteutuu tehokkaasti muun muassa sopimuksilla, joissa on huomioitu tietosuojaliitteen eli niin sanotun henkilötietojen käsittelysopimuksen lisäksi tietoturvavaatimukset ja palvelutasot riittävällä tasolla. Säännöllisillä auditoinneilla tai arvioinneilla pystytään tarkistamaan, että henkilötietojen käsittelijän prosessit ja tietoturvataso vastaavat sitä, mitä on sovittu.[629]

Rekisteröidyn, rekisterinpitäjän ja henkilötietojen käsittelijän lisäksi tietosuojaasetuksessa on määritelty myös kolmas osapuoli ja vastaanottaja. *Kolmas osapuoli* on luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin kuin rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä tai muu henkilö, jolla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän taikka henkilötietojen käsittelijän välittömän vastuun alaisena. Määritelmä kattaa sellaiset henkilöt, jotka eivät ole rekisterinpitäjän palveluksessa ja jotka eivät kuulu sen määräysvaltaan[630]. Esimerkiksi vahingossa väärään sähköpostiosoitteeseen tulleen viestin yhteydessä henkilötietoa saanut työntekijä olisi tällainen kolmas osapuoli.

Vastaanottajalla tarkoitetaan luonnollista henkilöä, oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja. Vastaanottaja voi olla myös kolmas osapuoli, mutta ei välttämättä. Viranomaiset, jotka vastaanottavat tietoja lainmukaisen tutkimuksen puitteissa, eivät kuitenkaan ole vastaanottajia. Tästä esimerkkinä sähköisen viestinnän palveluista annetun lain 316 §, jonka mukaan liikenne- ja viestintävirastolla sekä tietosuojavaltuutetulla on salassapitosäännösten tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada välitystiedot, sijaintitiedot ja viestit, jos ne ovat tarpeen lain VI-osassa tarkoitettua käsittelyä ja on syytä epäillä tiettyjen, laissa määriteltyjen rikosten tunnusmerkistöjen, kuten tietosuojarikkomuksen, viestintäsalaisuuden loukkauksen tai tietomurron, täyttymistä. Myös toisena esimerkkinä sähköisen viestinnän palvelulain 156 §, jonka mukaan yhteisötilaajalla on oikeus luovuttaa asianomistajana tekemänsä rikosilmoituksen tai tutkintopyynnön yhteydessä poliisille käsiteltäviksi 146–155 §:n mukaisesti saamansa viestintäverkon tai viestintäpalvelun käyttäjän sähköisiä viestejä koskevia välitystietoja. Tällaiset välitystiedot voivat olla muun muassa lähettäjän ja vastaanottajan sähköpostiosoitteet ja viestien aikaleimat, IP-osoitteet silloin kun, niitä käsitellään viestinnän

[629] Rekisterinpitäjän ja henkilötietojen käsittelijän keskinäistä suhdetta ja näiden toimijoiden tietoturvavastuita on käsitelty yksityiskohtaisemmin ulkoistamista ja sopimuksia käsittelevässä kappaleessa 3.3.2 (”Henkilötietojen käsittelyn ja tietoturvan huomioiminen sopimuksissa”).
[630] Oikeuskäytännön mukaan kolmansia osapuolia ovat mm. kyberrikolliset. Ks. EUT 14.12.2023, C-340/21, VB v. Natsionalna agentsia za prihodite, ks. ratkaisun kohta 66.

välittämiseksi, sekä VPN-palveluun tunnistautumisen yhteydessä tallentuvat lokitiedot[631].

Yhteenvetona todettakoon, että kaikki organisaatiot käsittelevät henkilötietoja toiminnassaan. Useat organisaatiot ovat vähintään rekisterinpitäjiä työntekijöidensä henkilötietojen osalta, mutta myös liiketoimintaansa liittyvien asiakas- ja toimittajatietojensa osalta. Lisäksi organisaatiot saattavat toimia henkilötietojen käsittelijän roolissa rekisterinpitäjän lukuun ja ohjeiden mukaisesti. Tämä korostaa tietosuojaan liittyvien roolien tunnistamisen tärkeyttä, sillä roolien määrittelemisen kautta tunnistetaan myös organisaation kohdistuvat vastuut ja velvoitteet tietoturvan osalta. Rekisterinpitäjällä on lähtökohtaisesti päävastuu henkilötietojen suojaamiseen liittyvistä tietoturvatoimenpiteiden toteutumisesta, jolloin rekisterinpitäjän on ikään kuin myös varmistettava lukuunsa toimivien henkilötietojen käsittelijöiden riittävä tietoturvan toteutuminen organisaatiossa. Näin ollen henkilötietojen suojaamiseen liittyvät lainsäädännön tietoturvallisuusvaatimukset ulottuvat kaikkiin organisaatioihin kuten myös osoitusvelvollisuus tietosuojaan liittyvien vaatimusten toteutumisesta. Täten tietosuojalainsäädäntö näyttäytyy kohtuullisena ja oikeudenmukaisena, sillä samat säännöt koskevat kaikkia organisaatioita.

Tietosuojalainsäädännön tietoturvavaatimusten tunnistamisen sekä roolien hahmottamisen haasteet erityisesti henkilötietojen käsittelyn ketjuuntuessa usealle eri toimijalle vaikeuttavat lainsäädännön ymmärrettävyyttä ja tavoitettavuutta erityisesti pienissä sekä alhaisen tietoturvamaturiteetin omaavissa yrityksissä. Näin ollen nykyisessä tietoturvan sääntelyjärjestelmässä olisi tarvetta myös tietoturvan vähimmäissääntelylle kaikkien organisaatioiden osalta, mikä parantaisi henkilötietojen suojaamista kaiken kokoisissa yrityksissä.

3.2.4 Osoitusvelvollisuus

Tietosuoja-asetuksen yksi keskeisimmistä käsitteistä on *osoitusvelvollisuus* (*Accountability*)[632]. Organisaatioiden ei tule ainoastaan noudattaa lakia ja henkilötietojen käsittelyä koskevia yleisiä periaatteita, vaan rekisterinpitäjän on myös pystyttävä aktiivisesti osoittamaan, että tietosuoja-asetuksen vaatimukset toteutuvat organisaatiossa ja organisaatio noudattaa lainsäädäntöä. Osoitusvelvollisuuden periaate toimii organisaatiolle oikeudellisena velvoitteena järjestää todennettava ja järjestelmällinen tietoturvatyö[633].

---

631 KKO 2022:23
632 Osoitusvelvollisuudesta käytetään rinnakkain myös käsitettä tilivelvollisuus.
633 Pöysti 2023: 43.

Osoitusvelvollisuuden yhteydessä on toisinaan puhuttu käännetystä todistustaakasta. Oikeudenkäymiskaaren (4/1734) 17 luvun 3 §:n 1 momentin mukaan rikosasiassa kantajan, eli syyttäjän ja asianomistajan, on näytettävä ne seikat, joihin hänen rangaistusvaatimuksensa perustuu[634]. Lisäksi lain 2 momentin mukaan tuomion, jossa vastaaja tuomitaan syylliseksi, edellytyksenä on, ettei vastaajan syyllisyydestä jää varteenotettavaa epäilyä. Tällöin sana sanaa vastaan -tilanteissa kyse ei ole siitä, kumman osapuolen kertomus tapahtumista on uskottavampi, vaan siitä että, onko syytetyn versio mahdollinen eli sitä ei voida poissulkea. ”Ei voida poissulkea” on todennäköisyysasteeltaan alempi kuin ”syytä epäillä” -kynnys, joka on esitutkinnan käynnistämiskynnys.[635] Tällaiset sana sanaa vastaan -tilanteet ovat kuitenkin harvinaisempia tietoturvaa ja tietosuojaa koskevissa asioissa, koska lähes poikkeuksetta laiminlyönnit tai rikokset ovat todistettavissa tietoteknisesti tai käytännön työn kautta nähtävinä puutteina. Esimerkiksi jos vaatimuksena on tiettyjen seikkojen dokumentointi ja tällainen dokumentaatio puuttuu, se on selkeä laiminlyönti.

Lähtökohtaisesti rekisterinpitäjän voidaan katsoa rikkoneen tietosuoja-asetusta, mikäli hän ei pysty näyttämään noudattaneensa asetusta. Tietosuoja-asetuksen rikkomista koskevat asiat tulevat käsiteltäviksi hallintomenettelyssä ja rikosoikeudenkäynnissä. Hallintomenettelyissä tavoitteena on yleensä puutteellisen asiantilan korjaaminen, jolloin virallisperiaatteen mukaisesti prosessin käynnistänyt viranomainen tulee yksilöimään henkilötietojen käsittelyssä tapahtuneet puutteet. Hallintoprosessia ei todennäköisesti käynnistettäisi, ellei henkilötietojen käsittelyssä ole havaittu puutteita. Rikosoikeudenkäynnissä vallitsee syyttömyysolettama[636], joka on keskeinen ihmisoikeusperiaate eikä tietosuoja-asetuksen osoitusvelvollisuus voi muuttaa tätä lähtökohtaa. Tällöin esimerkiksi, mikäli rekisterinpitäjän edustaja on syytteessä henkilötietojen käsittelyyn liittyen, todistustaakka on yksin syyttäjällä.[637]

Vahingonkorvauskanteissa rekisterinpitäjällä on todistustaakka siitä, että henkilötietoja käsitellään tavalla, jolla varmistetaan niiden asianmukainen turvallisuus. Tällainen todistustaakka on ollut rekisterinpitäjällä EUT:n tulkinnan mukaan

---

634 Säännöstä (OK 17:3) voidaan soveltaa muissakin rikosoikeudellisiksi luettavissa asioissa kuin syyteasiassa (HE 46/2014, s. 48–49). Todistustaakka koskee periaatteessa yhtä lailla rikoksen objektiivisia ja subjektiivisia tunnusmerkistötekijöitä, mutta esimerkiksi tahallisuutta ja tuottamusta arvioitaessa subjektiivisen puolen selvittäminen saattaa olla ongelmallista, mikäli saatavilla ei ole tietoa tekijän tavoitteista tai mieltämisistä (Jokela 2018, s. 680–681). Tekijän tahallisuus joudutaan käytännössä yleensä päättelemään ulkonaisesti ilmenevistä seikoista.

635 Fredman 2021: 734; Rautio & Frände 2020: 159.

636 Todistustaakka koskee kaikista syyksi lukevan tuomion perustavista seikoista, jolloin syyttömyysolettaman perusteella voidaan olettaa, ettei vastaajalla ole velvollisuutta todistaa syyttömyyttään. Ks. HE 46/2014 vp, 48–49.

637 Nyyssölä 2018: 66, 87–88.

silloinkin, kun kyseessä on ollut rekisterinpitäjän alaisuudessa toimineen työntekijän tekemä virhe henkilötietojen käsittelyssä. Toisaalta yhtä lailla tietosuoja-asetuksen 82 artiklaan perustuvan vahingonkorvauskanteen nostajan asiana on osoittaa vahinko, eli esimerkiksi onko asianomaista kärsinyt tapahtumasta. Näin ollen todistustaakka vahingonkorvauksen perusteesta on riita-asioissa vaateen esittäjällä.[638]

Keskeisenä käytännön toimenpiteenä osana organisaation osoitusvelvollisuutta on riittävä dokumentointi[639]. Tästä esimerkkinä on tietosuojapolitiikan ja muiden tietosuojaohjeistuksien luominen, ylläpito ja jalkauttaminen organisaatiossa. Organisaatio voi myös toteennäyttää osoitusvelvollisuuttansa tietotilinpäätöksen avulla[640]. Rekisterinpitäjän osoitusvelvollisuuden toteutumista voidaan lisäksi todistaa kokonaisvaltaisella riskienhallinnalla, jossa tietosuojaan liittyvät riskit on huomioitu kattavasti ja tästä on dokumentaatioevidenssiä[641]. Myös kaikki henkilötietojen tietoturvaloukkaukset tulee dokumentoida, mukaan lukien niihin liittyvät riskiarvioinnit[642]. Kattavan dokumentoinnin lisäksi myös artikloissa 40 ja 42 tarkoitettujen käytännesääntöjen ja hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä osoitusvelvollisuuden toteutumisen todistamiseksi. Näin ollen hyväksyttyjen ja soveltuvien tietoturvastandardien auditointi ja sertifiointi arviointilaitoksen toimesta voivat olla osa osoitusvelvollisuuden todentamista esimerkiksi 32 artiklan mukaisten käsittelyn turvallisuutta koskevien teknisten ja organisatoristen toimenpiteiden osalta. Toisaalta on huomioitava se, että oikeuskäytännössä on myös painotettu, että yksistään asiantuntijalausunnot eivät voi olla riittävä todiste asianmukaisista turvallisuustoimenpiteistä, vaan tietoturvatoimenpiteiden määritys henkilötietojen suojaamiseksi tulee perustua dokumentoituun riskiarviointiin, jota tarvittaessa tuomioistuinten on pystyttävä arvioimaan konkreettisesti[643].

Yhteenvetona voidaan todeta, että tietoturvallisuuden osoitusvelvollisuus henkilötietojen käsittelyssä on moniulotteinen. Kyseessä on aktiivinen osoittaminen henkilötietojen käsittelyn lainmukaisuudesta sen hetken käytännön toiminnassa, mutta myös jälkikäteinen todistustaakka vahingonkorvauskanteen yhteydessä.

---

[638] Ks. EUT 25.1.2024, C-687/21 MediaMarktSaturn ratkaisun kohta 43 ja 68 sekä ratkaisun EUT 14.12.2023, C-340/21 Natsionalna agentsia za prihodite kohta 57.
[639] Tietosuoja-asetuksen tuomia dokumentaatiovaatimuksia on käsitelty seuraavassa alaluvussa 3.3.1 (”Sääntelyjärjestelmän dokumentaatiovaatimukset”).
[640] VAHTI 1/2016: 11, 27, 32.
[641] Tietosuoja-asetuksen tuomia riskienhallintavelvoitteita on käsitelty luvussa 3.3.3 (” Henkilötietojen käsittelyn riskilähtöisyys ja riskiarviointi”).
[642] Henkilötietojen tietoturvaloukkauksista lisää luvussa 3.3.4 (”Tietoturvaloukkauksien ja tietoturvapoikkeamien ilmoittaminen”).
[643] EUT 14.12.2023, C-340/21, VB v. Natsionalna agentsia za prihodite, ks. ratkaisun kohta. 43. Lisää EUT:n ratkaisusta luvussa 3.4.1 (”Tekniset ja organisatoriset toimenpiteet sekä operatiiviset toimenpiteet”).

Tietosuojan osoitusvelvollisuus ei ulotu ainoastaan henkilötietojen käsittelyn vaatimuksiin vaan kokonaisvaltaisesti organisaation tietojen käsittelyn asianmukaisiin tietoturvatoimenpiteisiin, jotka perustuvat dokumentoituun riskien arviointiin ja kokonaisvaltaiseen riskienhallintaan. Nämä tietoturvatoimenpiteet kattavat sekä hallinnollisia että teknisiä tietoturvatoimia, mutta myös fyysisiä suojatoimenpiteitä suhteutettuna uhkaympäristöön sekä käsittelystä syntyviin riskeihin. Tietosuojan osoitusvelvollisuuden toteutumisen aktiivinen edistäminen on merkittävästi parantanut myös organisaatioiden tietoturvatasoa ja tietoturvaan liittyvää dokumentointia, sillä tietosuojalainsäädäntö painottaa hyvin paljon tietoturvaan liittyvää dokumentointia prosessien ja ohjeistuksien kuvaamisen kautta, mutta myös teknisiä tietoturvatoimenpiteitä etenkin erityisten henkilötietojen suojaamiseksi.

3.3 Tietosuojavaatimukset tietoturvan sääntelyjärjestelmässä

3.3.1 Sääntelyjärjestelmän dokumentaatiovaatimukset

Tietosuoja-asetuksen osoitusvelvollisuuden myötä rekisterinpitäjän on pystyttävä aktiivisesti osoittamaan asetuksen mukainen toiminta ja henkilötietojen käsittelyä koskevien yleisten periaatteiden toteutuminen toiminnassaan. Riittävä dokumentointi sekä ohjeistuksien ylläpito on yksi tapa osoittaa organisaation osoitusvelvollisuuden toteutuminen muiden toimien ohella. Dokumentointi on myös tietoturvallisuuden osalta tärkeä käytänne.

Tietosuoja-asetuksen 30 artiklassa on asetettu vaatimus selosteesta käsittelytoimista. Vaatimus koskee lähtökohtaisesti yli 250 työntekijän organisaatioita. Seloste on kuitenkin tehtävä pienemmissäkin organisaatioissa, mikäli organisaation suorittama henkilötietojen käsittely aiheuttaisi todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille, käsittely kohdistuu arkaluontoisiin henkilötietoihin tai rikostuomioita ja rikkomuksia koskeviin henkilötietoihin, taikka käsittely ei ole satunnaista. Käsittelyn satunnaisuuden arviointi saattaa kuitenkin olla hankalaa, sillä jokaisessa organisaatiossa käsitellään henkilötietoja enemmän tai vähemmän. Selosteen tekeminen on tästäkin syystä jo suotavaa ja sitä voidaan myöhemmin käyttää tietosuoja-asetuksen osoitusvelvollisuuden toteennäyttämiseksi.

Vaatimuksen mukaan rekisterinpitäjän ylläpitämään selosteeseen käsittelytoimista on sisällytettävä henkilötietojen käsittelyn tarkoitukset, kuvaus henkilötietoryhmistä ja rekisteröityjen ryhmistä, luovutettujen ja luovutettavien henkilötietojen vastaanottajien ryhmät, tarvittaessa tiedot henkilötietojen siirtämisestä

kolmanteen maahan tai kansainväliselle järjestölle, mahdollisuuksien mukaan eri tietoryhmien suunnitellut poistamisen määräajat, mahdollisuuksien mukaan kuvaus teknisistä ja organisatorista turvatoimista, sekä rekisterinpitäjän tai rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot. **Tietosuojavaltuutetun toimiston 12.7.2017 (dnro. 1081/41/2017) antaman vastauksen** mukaan kumotun henkilötietolain rekisteriselosteen tietosisältö vastaa suureksi osaksi tietosuoja-asetuksen selostetta käsittelytoimista, vaikkakin poikkeuksena on, että tietosuoja-asetuksen mukaisen selosteen ei tarvitse olla jokaisen saatavilla.

> *Tietosuojavaltuutetun toimisto katsoo, että on mahdollista käyttää rekisteriselosteen kaltaista pohjaa noudattaakseen tietosuoja-asetuksen 30 artiklan velvoitetta ylläpitää selostetta käsittelytoimista. Tällöin on huomioitava, että selosteen tietosisältö vastaa tietosuoja-asetuksen vaatimuksia.*

Huomioitava on, että seloste käsittelytoimista eroaa tietosuojaselosteesta, jota myös käytetään organisaatioissa osana osoitusvelvollisuuden todistamista. Tietosuojaselostetta ei ole tietosuoja-asetuksessa määritelty pakollisena dokumenttina, mutta käytännön tasolla rekisterinpitäjäorganisaatiot toteuttavat tietosuojaselosteillaan rekisteröidyn läpinäkyvää informointia henkilötietojen käsittelystä ja rekisteröidyn oikeuksista. Tietosuojaselosteet osana rekisteröityjen informointia ovatkin näin ollen usein julkisia dokumentteja (tai sisäisiä organisaation työntekijöiden ollessa ainoita rekisteröityjä), kun taas käsittelytoimien seloste on lähinnä sisäinen työkalu.

Henkilötietojen käsittelijän ja hänen edustajansa on ylläpidettävä käsittelytoimien selostetta rekisterinpitäjän lukuun suoritettavista käsittelytoimista. Yhtenäistä on se, että rekisterinpitäjän ja henkilötietojen käsittelijän käsittelytoimiselosteen on oltava kirjallinen ja sähköisessä muodossa. Henkilötietojen käsittelijän seloste on kuitenkin hieman suppeampi kuin rekisterinpitäjän pitämä seloste sisältäen seuraavat tiedot: kunkin rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät, tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, mahdollisuuksien mukaan kuvaus teknisistä ja organisatorista turvatoimista, sekä rekisterinpitäjän tai rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot. Mainintaa tietoryhmien suunnitelluista poistamisen määrärajoista ei ole tältä osin asetuksessa mainintaa. Tämä johtunee siitä, että henkilötietojen käsittelijän tekemä tietojenkäsittely on pitkälti sidoksissa

rekisterinpitäjän kanssa tehtyyn sopimukseen[644]: kun sopimus loppuu, myös henkilötietojen käsittelyn lainmukaisuus ja käyttötarkoitussidonnaisuus loppuvat. Yleensä myös sopimuksella on sovittu rekisterinpitäjälle kuuluvien tietojen palauttamisesta tai tuhoamisesta, mikä on myös tietoturvallinen käytäntö.

Rekisterinpitäjän ja henkilötietojen käsittelijän välinen 28 artiklan mukainen sopimus on oltava kirjallinen eli todennettavissa[645]. Kyseisessä sopimuksessa on mainittava, että henkilötietojen käsittelijä käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti. Näin ollen rekisterinpitäjän pitää luoda ja ylläpitää henkilötietojen käsittelyyn liittyviä ohjeistuksia, joita voidaan tarpeen tullen antaa eteenpäin myös kolmansille osapuolille. Tällaisten kirjallisten ohjeiden luominen ja ylläpitäminen on yksi organisatorinen toimenpide, joka velvollisuutena kohdistuu rekisterinpitäjään[646]. Tämä toisaalta vahvistaa entisestään sitä, että tietosuoja-asetuksen mukaiset organisatoriset toimenpiteet ovat luonteeltaan myös yhtäaikaisesti tietoturvatoimenpiteitä, vaikka keskeisenä painotuksena on henkilötietojen käsittely.

Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, loukkaukseen liittyvät seikat, vaikutukset ja toteutetut korjaustoimet, jotta ne olisivat mahdollista tarkistaa myöhemmin esimerkiksi tietosuoja-asetuksessa määritellyn valvontaviranomaisen toimesta (33 artikla). Tämä voi tapahtua esimerkiksi sähköisen tiketöintijärjestelmän avulla, josta pystytään etsimään ja todentamaan myöhemmin tietoturvaloukkauksiin liittyvät tiketit, niiden sisältö sekä loukkauksien vastuuttaminen ja käsittely organisaatiossa. Käytännössä myös henkilötietojen tietoturvaloukkaukseen liittyvä riskienarviointi rekisteröidyn oikeuksien ja vapauksien suhteen tulee myös dokumentoida vähintään joko tikettiin tai muuhun sovittuun paikkaan. Tapahtuma-ajan lokitiedot on säilytettävä osana dokumentaatiota[647].

Tietosuojaa koskevat riskiarviot sekä 35 artiklan mukainen vaikutustenarviointi eli DPIA-arviointi (Data Protection Impact Assessment) on osoitusvelvollisuuden toteennäyttämiseksi tehtävä kirjallisesti[648]. DPIA-arviointi tulee pakolliseksi, kun henkilötietojen käsittely todennäköisesti aiheuttaa luonnollisen henkilön

[644] Tietosuoja-asetuksen 28 artiklan vaatimuksen mukaan henkilötietojen käsittelijän suorittama käsittely on perustuttava sopimukseen tai muun unionin oikeuden taikka jäsenvaltion lainsäädännön mukaiseen oikeudelliseen asiakirjaan suhteessa rekisterinpitäjään.
[645] Lisää sopimuksen sisällöstä alaluvussa 3.3.2 (”Henkilötietojen käsittelyn ja tietoturvan huomioiminen sopimuksissa”).
[646] Voutilainen 2019: 191.
[647] Tietosuojavaltuutetun toimisto 2021a; Korpisaari, Pitkänen & Warma-Lehtinen 2022: 389.
[648] Tietosuojariskien arviointia käsitellään myöhemmin tässä tutkimuksessa luvussa 3.3.3 (”Henkilötietojen käsittelyn riskilähtöisyys ja riskiarviointi”).

oikeuksien ja vapauksien kannalta korkean riskin.[649] Riskiarvioinnin yhteydessä sekä henkilötietojen käsittelyn tarpeellisuutta arvioitaessa saattaa tulla ajankohtaiseksi tarve tehdä henkilötietojen käsittelyyn liittyvä tasapainotesti[650] rekisteröidyn etujen punnitsemiseksi. Mikäli rekisterinpitäjä tekee tällaisen tasapainotestin rekisteröidyn etujen punnitsimiseksi, se olisi suositeltavaa myös dokumentoida osoitusvelvollisuuden täyttämiseksi. Apulaistietosuojavaltuutetun päätöksen mukaan tasapainotestistä ja sen tuloksista tulisi kertoa rekisteröidylle ja selvittää heille, miksi rekisterinpitäjän etu menee mahdollisesti rekisteröidyn etujen edelle.[651]

VAHTI 1/2016 -ohjeessa on kootusti ehdotettu seuraavanlaista dokumentaatiota organisaation tietosuojanhallintajärjestelmän osaksi ottaen huomioon tietysti organisaation koko ja henkilötietojen käsittelytarpeen määrä: tietotilinpäätös[652], dokumentaatio mahdollisista tietoturvaloukkauksista, ohjeet henkilötietoja käsittelevälle henkilöstölle, kuvaukset prosesseista sisäänrakennetun ja oletusarvoisen tietosuojan toteutumiseksi, tietoturvatestauksen tulokset, riskirekisterit riskien omistajien ja toimenpiteiden kera, tietoturvan ja -suojan ohjausryhmien tai muiden foorumien pöytäkirjat, DPIA-arvioinnit hallintakeinoineen, kuvaukset rekisteröityjen oikeuksien takaamiseksi määritellyissä prosesseissa, rekisterien tietovirtakuvaukset, tietosuojaselosteet, tietosuojaroolit ja -vastuut sekä tietosuojapolitiikka. Esimerkkinä edellä mainituista dokumenteista erityisesti tietosuojapolitiikka ylimpänä henkilötietojen käsittelyä ohjaavana ja periaatteita kuvaavana dokumenttina organisaatiossa, on suositeltavaa laatia[653].

Tietoturvan viitekehysten, kuten muun muassa ISO-tietoturvallisuusstandardien mukaan, organisaatioilla tulisi olla johdon hyväksymä tietoturvapolitiikka[654]. Esimerkiksi tietoturvapolitiikan tulisi sisältää vähintään kuvaus tietoturvallisuuden

---

[649] Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 5, 7.
[650] Ks. Korpisaari. Pitkänen & Warma-Lehtinen 2022: 133–135. Oikeutettua etua käytettäessä käsittelyperusteena tulee käsittelyä tarkastella tasapainotestin eli rekisteröidyn etuja koskevan punninnan avulla. Jos rekisteröidyn edut ja oikeudet eivät ole painavampia kuin rekisterinpitäjän intressi henkilötietojen käsittelyyn, henkilötietoja saa käsitellä.
[651] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 140; TSV 4.6.2021, dnro 4900/182/18; Euroopan WP29-tietosuojatyöryhmä WP217: *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, s.* 43.
[652] Tietotilinpäätös on vapaaehtoinen raportti, mutta sitä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden toteuttamisessa. Tietotilinpäätös antaa kokonaiskuvan organisaation tietojenkäsittelyn tilasta ja se kuvaa, miten tietosuojaa koskevat yleiset periaatteet toteutetaan organisaatiossa. Se on tarkoitettu organisaation johdon työkaluksi sekä lisäämään sidosryhmien luottamusta. Ks. VAHTI 1/2016, s. 13.
[653] VAHTI 1/2016: 27.
[654] Katakri 2020 T01-vaatimuksessa linjataan lähinnä organisaation ylimmän johdon hyväksymistä ja dokumentoiduista turvallisuusperiaatteista.

merkityksestä organisaatiossa, turvallisuusperiaatteet, tietoturvallisuusvastuut, tietoturvaa ohjaavat tekijät sekä ylätason kuvaukset tietoturvallisuuden toteuttamistavoista organisaatiossa. Tietoturvapolitiikan sisällöstä on monenlaisia ohjeistuksia eri standardeissa ja VAHTI-ohjeissa ja tietoturvapolitiikka laaditaan usein niin, ettei sitä tarvitse uusia sisällöltään kovin usein[655]. Kuitenkin yleensä tietoturvapolitiikan sisältö olisi hyvä katselmoida vuosittain. Käytännön tasolla tietoturvapolitiikka ja tietosuojapolitiikka on pidetty erillisinä dokumentteina, jotka kuvaavat eri periaatteita, ja ne toteuttavat osoitusvelvollisuutta usein eri näkökulmista. Missään ei ole kuitenkaan ikinä ollut rajausta siitä, etteikö näitä kahta dokumenttia voisi yhdistää. Tietoturva ja tietosuoja ovat kuitenkin yhdessä osa organisaation kokonaisturvallisuutta.

Hyvien käytänteiden mukaisesti tietoturvapolitiikan lisäksi on suositeltavaa ylläpitää myös muuta tietoturvallisuuteen liittyvää dokumentaatiota. Usein suositeltavaa, hyvien käytänteiden mukaista tietoturvadokumentaatiota ovat muun muassa riskienhallinnan dokumentit, tietoturvan vuosikello ja kehittämissuunnitelma, ohjeistus poikkeamatilanteisiin (*”incident response plan”*), jatkuvuus- ja toipumissuunnitelmat sekä mahdollinen valmiussuunnitelma, tietojen käsittely- ja luokitteluohje, käsittelyoikeuksien hallinnointitapaohjeet sekä muut henkilökunnan tietoturvaohjeistukset tietosuojaan liittyvien ohjeistuksien lisäksi. Myös tietoaineistoturvallisuuteen liittyviä hyviä käytänteitä tulisi painottaa osana dokumentointia, eli toimia liittyen tietojen säilyttämiseen, varmistamiseen, palauttamiseen ja tuhoamiseen[656]. Näin tietoaineistoturvallisuus linkittyy myös osaltaan henkilötietojen käsittelyyn. Tietoaineistoturvallisuus katsotaan kuitenkin usein omaksi tietoturvallisuuden osa-alueekseen, ja siihen liittyen voikin kohdistua vaatimuksia niin hallinnollisen, fyysisen kuin teknisen tietoturvallisuuden osa-alueilla[657].

Dokumentoinnin taustalla on usein ajatus riskin pienentämisestä sen osalta, että moni olennainen tieto jäisi vain avainhenkilöiden tietopääomaksi ”nahkakansiin”. Esimerkiksi dokumentoimalla turvallisuuden kannalta keskeiset asiat varmistutaan samalla siitä, että toiminta ei ole henkilöriippuvaista. Näin ollen organisaatiossa tulisi olla ajantasaiset ohjeet (luokiteltujen) tietojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta sekä tietoturvallisuustoimen-

[655] Andreasson & Koivisto 2013: 34.
[656] Hakala, Vainio & Vuorinen 2006: 11.
[657] Katakri 2020:ssa tietoaineistoturvallisuutta koskevat muun muassa vaatimukset T08 – Tietojen luokittelu, F04 – Tiedon käsittely ja säilytys sekä F08 – Tietoaineistoturvallisuus (paperimuotoiset). Myös teknisillä toimenpiteillä toteutetaan tietojen salassapitoa, jolloin esimerkiksi Katakri 2020:ssa huomioitavia vaatimuksia ovat muun muassa I05 – Langaton tiedonsiirto, I15 – Tiedon sähköinen välitys, I18 – Etäkäyttö ja etähallinta sekö I21 – Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen.

piteistä.[658] Toisesta näkökulmasta, esimerkiksi ottaen huomioon tietoturvallisuuden hallintajärjestelmää koskeva ISO/IEC 27001 -standardi, dokumentointi edesauttaa myös tietoturvallisuuden toteennäyttämisessä.

Hyvien tietoturvallisten käytänteiden mukaisesti dokumentaation luominen ja olemassaolo ei ole ainoastaan riittävää, vaan dokumentteja tulisi vastuuhenkilöiden toimesta myös katselmoida ja päivittää säännöllisesti sekä aina muutosten yhteydessä. Tähän hyvään käytäntöön ei tietosuoja-asetus ole varsinaisesti vaatimuksissaan velvoittanut eikä ottanut kantaa. Kuitenkin esimerkiksi tietosuojatyöryhmän lausunnossa on todettu, että päivittämällä DPIA-arviointia hankkeen koko elinkaaren ajalta varmistetaan samalla tietosuojan ja yksityisyyden huomioiminen sekä tuetaan vaatimusten noudattamista[659]. Lisäksi organisaation henkilökunnan tulisi olla tietoisia turvallisuusohjeista ja niiden sijainnista, mikä ei aina toteudu. Käytännössä tätä tietoisuutta voi lisätä tiedottamisella ja kouluttamisella[660].

Todettakoon, että riittävä dokumentointi on yksi keskeinen tapa todentaa organisaation osoitusvelvollisuuden toteutuminen niin tietosuojalainsäädännön näkökulmasta kuin tietoturvatason todentamisen osalta. Tietosuoja-asetuksen dokumentointivaatimukset ovat olleet merkittävä, yhtenäistävä askel kohti hyviä tietoturvallisia käytänteitä, sillä lainsäädännössä ei ole ennen tietosuoja-asetusta korostettu suoraan dokumentoinnin tärkeyttä vastaavalla tavalla. Moni tietosuojalainsäädännön velvoittama dokumentti vastaa myös hyviä tietoturvakäytänteitä, esimerkiksi dokumentoidut (henkilö)tiedon käsittelyohjeet sekä velvollisuudet dokumentoida riskiarviointeja ja poikkeamien hallintaa. Huomioitava on myös NIS 2 -direktiivin voimaan paneva kyberturvallisuuslaki, jonka osalta on ehdotettu kyberturvallisuuden riskienhallinnan toimenpiteinä muun muassa dokumentoituja konfiguraatio- ja ohjelmistopäivityksiä, dokumentoituja omaisuudenhallinnan menettelyitä ja ohjeita, dokumentoituja poikkeamien käsittelyn menettelyitä, rooleja ja vastuita sekä dokumentoituja menettelyitä toiminnan jatkuvuuden ja häiriötilanteista toipumisen suhteen[661]. Toistaiseksi dokumentointivaatimukset ovat kuitenkin tietoturvanäkökulmasta kovin yksinkertaisia tai hajanaisia tietoturvan sääntelyjärjestelmässä, jolloin organisaatioiden tulee nojata enemmän hyviin käytänteisiin ja esimerkiksi viitekehyksissä oleviin tietoturvan dokumentointivaatimuksiin ja suosituksiin. Lainsäädännössä tulisi johdonmukaisemmin huomioida tietoturvadokumentoinnin tärkeys. Säädettäessä tulevaisuudessa

[658] Ks. Katakri 2020 T04-vaatimus.
[659] Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 17.
[660] Ks. luku 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).
[661] HE 57/2024 vp: 163–164, 166–167.

tietoturvallisuuteen liittyvistä dokumentointivelvoitteista, tulisi paremmin huomioida myös dokumentoinnin ajantasaisuuden vaatimukset, mutta myös dokumentoinnin jalkautus esimerkiksi tiedottamalla ja kouluttamalla henkilöstöä.

3.3.2 Henkilötietojen käsittelyn ja tietoturvan huomioiminen sopimuksissa

IT:n ulkoistaminen niin julkisissa kuin yksityisissä organisaatioissa on nykyään hyvin yleistä. Ulkoistamisen muodot voivat vaihdella yksittäisen ohjelmiston tai pilvipalvelun ulkoistamisesta koko IT-palvelun ulkoistamiseen[662]. Monesti myös organisaatiossa olevaa resurssi- tai osaamisvajetta korvataan asiantuntijapalveluiden ostamisella. Ulkoistamisessa ja ylipäätänsä hankinnoissa on tärkeää edellyttää tietynlaista tietoturvatasoa myös kolmansilta osapuolilta osana hallinnollisen tietoturvallisuuden kontrolleja ja riskienhallintaa. Tietoturvavelvoitteet, toiminnan jatkuvuus ja palvelutasot on hyvä huomioida jo sopimustasolla. Hyviin käytänteisiin kuuluu tietoturvaohjeistuksien ja -vaatimusten ulottaminen toimittajiin ja hankintoihin sekä toimittajien tietoturva-auditoinnit, jotta organisaation suojattava omaisuus olisi turvattu toimitusketjusta lähtien ja toimittajasopimuksissa sovitut tietoturva- ja palvelutasot toteutuisivat[663]. Tällöin tietoturvallisuusvaatimukset tulisi olla määriteltynä jo tarjouspyynnössä[664].

Juridisesta näkökulmasta hankinnoissa kiinnitetään erityistä huomiota henkilötietojen ja muiden luottamuksellisten tietojen käsittelyyn. Tietosuojamääräykset eivät aseta esteitä ulkoistamiselle. Pitää vain varmistaa, että vaadittavat sopimusjärjestelyt ja organisatoriset toimenpiteet täyttyvät. Tietosuoja ja luottamuksellisuus ovat esimerkkejä oikeudellisista ongelmista, jotka voidaan ratkaista käytännön teknisillä ja organisatorisilla toimenpiteillä.[665]

Henkilötietojen käsittelijä suorittaa käsittelyä rekisterinpitäjän lukuun. Tietosuoja-asetuksen 28 artiklan mukaan rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka täyttävät yleisen tietosuoja-asetuksen

[662] Esimerkkinä ulkoistetusta pilvipalvelusta on SaaS-palvelu (Software as a Service), joka pyörii toimittajan konesalissa. Vastakohtaisesti voidaan ulkoistaa koko IT-palvelu, esimerkiksi CSOC-valvontapalvelu (kyberturvan valvontapalvelu, Cyber Security Operations Center) tai ulkoistettu konesalipalvelu.
[663] Ks. esimerkiksi ISO/IEC 27001:2020-standardissa liite A 5.19–5.22.
[664] Turvallisuusehdoista tulisi neuvotella jo hankintaprosessin alkupäässä. Huomioitava toki on, että oletusvirhesäännöt ja tuotevastuusäännöt yhdessä vahingonkorvaus- ja markkinointisääntöjen kanssa myös kannustavat muun muassa turvalliseen ohjelmistokehitykseen ja haavoittuvuustietojen paljastamiseen asiakkaille. Ks. Råman 2006b: 295, 334, 336, 420, 425.
[665] Johnssén 2018: 386–387.

vaatimukset toteuttamalla tarvittavat suojatoimet teknisten ja organisatoristen toimien täytäntöönpanemiseksi sekä rekisteröidyn oikeuksien suojelemiseksi.

Henkilötietojen käsittelystä on tehtävä sopimus rekisterinpitäjän ja henkilötietojen käsittelijän välillä. Näin ollen yleisen tietosuoja-asetuksen myötä organisaatioiden on tehtävä kirjalliset sopimukset ulkoisten henkilötietojen käsittelijöiden kanssa, esimerkiksi pilvipalveluiden tarjoajien kanssa. Täten osa tietosuoja-asetuksen vaatimuksista on kohdistettu suoraan rekisterinpitäjille ja henkilötietojen käsittelijöille, kun taas osa vaatimuksista ja velvollisuuksista on velvoitettava sopimuksin osapuolten kesken[666]. Käytännössä palvelua hankittaessa hankintasopimuksen osaksi tulee sisällyttää erillinen tietosuojaliite (*Data Processing Agreement, "DPA"*).

Tietojenkäsittelypalveluiden ulkoistamista on tapahtunut jo ennen tietosuoja-asetuksen voimaantuloa, jolloin henkilötietojen käsittelyyn liittyvistä sopimuksista ei ollut vielä säädetty yksityiskohtaisesti. Henkilötietojen käsittely oli kuitenkin jo henkilötietolain aikoihin rekisterinpitäjän vastuulla ja esimerkiksi tietojenkäsittelypalvelujen ulkoistamiseen liittyvät sopimukset kuuluivat jo ennestään hyviin tietoturvallisiin käytänteisiin. Tämä tulee ilmi muun muassa **tietosuojavaltuutetun päätöksessä 28.2.2017 (dnro. 2450/41/2016 & 2856/41/2012):**

> *Tietosuojavaltuutetun päätöksen mukaan henkilötietoja koskevat tietojenkäsittelypalvelut voidaan ulkoistaa palvelun hankkivan rekisterinpitäjän lukuun, jolloin siitä tehdään sopimus rekisterinpitäjän ja palvelun tuottajan välillä. Tietojenkäsittelyn turvallisuus tulee myös varmistaa riittävin teknisin toimenpitein sekä sopimuksin. Rekisterinpitäjä vastaa, että tietoja käsitellään turvallisesti omassa toiminnassa sekä silloin, kun tietojenkäsittely ulkoistetaan.*

Yleisen tietosuoja-asetuksen 28 artiklassa on määritelty sisältövaatimuksia rekisterinpitäjän ja henkilötietojen käsittelijän väliselle sopimukselle. Rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa on määriteltävä henkilötietojen käsittelyn luonne ja tarkoitus, kohde ja kesto, rekisterinpitäjän velvollisuudet ja oikeudet sekä rekisteröityjen ryhmät ja henkilötietojen tyyppi. Sopimuksessa on myös määriteltävä, että henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti, antaa rekisterinpitäjän saataville kaikki säädettyjen velvollisuuksien noudattamisen osoittamista varten tarpeelliset tiedot, sallii auditoinnit ja osallistuu niihin, sekä toteuttaa 32 artiklassa määritetyt tekniset ja organisatoriset toimenpiteet. Sopimuksessa on myös määriteltävä, että henkilötietojen käsittelijä varmistaa henkilötietojen

[666] Voutilainen 2019: 144.

käsittelyoikeuden omaavien henkilöiden salassapitovelvollisuutta koskevien sitoumuksien olemassaolon tai että heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.

Sopimuksessa tulee lisäksi määritellä, että henkilötietojen käsittelijä auttaa mahdollisuuksien mukaisesti, käsittelytoimen luonne huomioon ottaen, rekisterinpitäjää täyttämän rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat yleisen tietosuoja-asetuksen 3 luvussa säädettyjen rekisteröidyn oikeuksien käyttämistä, esimerkiksi tietojen tarkastamista, oikaisemista ja poistamista. Samankaltaisesti sopimukseen tulee sisällyttää henkilötietojen käsittelijän velvollisuus auttaa rekisterinpitäjää varmistamaan, että teknisiin ja organisatorisiin toimenpiteisiin, tietoturvaloukkauksesta ilmoittamiseen sekä tietosuojaa koskevaan vaikutusten arviointiin (DPIA) liittyviä velvollisuuksia artiklojen 32–36 mukaisesti noudatetaan käsittelyn luonne sekä saatavat tiedot huomioon ottaen. Sopimuksessa on myös rajattava, että henkilötietojen käsittelijä poistaa tai palauttaa kaikki henkilötiedot sekä poistaa jäljennökset käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä, ellei laissa ole erikseen vaadittu henkilötietojen säilytystä.

Tietosuoja-asetuksen mukaan henkilötietojen käsittelijä ei saa käyttää palveluissaan muita henkilötietojen käsittelijöitä ilman rekisterinpitäjän lupaa. Tämä on mainittava myös hankinnan pääsopimuksen tietosuojaliitteessä. Näin ollen henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle riittävän ajoissa suunnitelluista muutoksista muiden henkilötietojen käsittelijöiden eli alikäsittelijöiden osalta, jotta rekisterinpitäjällä on mahdollisuus vastustaa tällaisia muutoksia. Mikäli rekisterinpitäjä on myöntänyt kyseisen ennakkoluvan, toiseen henkilötietojen käsittelijään eli alikäsittelijään sovelletaan sopimuksella samoja tietosuojavelvoitteita kuin rekisterinpitäjän ja alkuperäisen henkilötietojen käsittelijän välisessä sopimuksessa taaten yleisen tietosuoja-asetuksen vaatimukset sekä tekniset ja organisatoriset toimenpiteet. Jos toinen henkilötietojen käsittelijä ei täytä tietosuojavelvoitettaan, esimerkiksi tietoturvan osalta, alkuperäinen henkilötietojen käsittelijä on silti täysimääräisessä vastuussa velvoitteiden suorittamisesta suhteessa rekisterinpitäjään.

Yleisen tietosuoja-asetuksen 29 artiklassa täsmennetään myös se, että rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimivien henkilöiden, joilla on pääsy henkilötietoihin, on käsiteltävä henkilötietoja rekisterinpitäjän ohjeiden mukaisesti. Näin ollen ohjeiden noudattamisesta on velvoitettu suoraan tietosuoja-asetuksessa, mutta myös 28 artiklan mukaisesti sopimusten kautta. Ohjeiden noudattamista koskeva vaatimus sopimusehdoissa on merkityksellinen, koska sopimusehtojen rikkominen johtaa sopimusoikeudellisiin sanktioihin esimerkiksi

vahingonkorvaukseen tai sopimussakkoihin[667]. Täten on erittäin tärkeää, että kyseiset ohjeet on myös kirjallisesti toimitettu henkilötietojen käsittelijälle ja tästä löytyy evidenssiä.

Huomioitava on se, että rekisterinpitäjän lukuun toimiva henkilötietojen käsittelijä ei saa vaikuttaa henkilötietojen käsittelyn tarkoituksen ja keinojen määrittelyyn. Muuten henkilötietojen käsittelijästä tulisi (yhteis)rekisterinpitäjä. Tämä voi tapahtua esimerkiksi, jos henkilötietojen käsittelijä käyttää rekisterinpitäjän antamia tietoja omiin tarkoituksiin.[668] Tietosuojatyöryhmän täsmennyksen mukaan, kun toimitaan jonkun lukuun, palvellaan toisen etuja ikään kuin valtuutuksen alla. Tällöin tietojenkäsittelijän tehtävänä on panna rekisterinpitäjän ohjeet täytäntöön ainakin tietojen käsittelyn tarkoituksen ja keinojen olennaisilta osin. Valtuutuksessa voidaan kuitenkin käyttää harkintavaltaa siltä osin, miten rekisterinpitäjän etuja parhaiten palvellaan esimerkiksi valitsemalla sopivimmat tekniset ja organisatoriset keinot.[669] Mikäli yhteisrekisterinpito tulee kyseeseen, on määriteltävä, miten rekisteröityjen oikeuksien käyttö ja informointivelvollisuus toteutetaan sekä tuotava ilmi rekisterinpitäjien roolit ja suhteet rekisteröityihin nähden. Käytännössä yhteisrekisterinpito on järjestettävä myös kirjallisin sopimuksin, jotta rekisterinpitäjät voivat osoittaa vastuunsa ja velvollisuutensa henkilötietojen käsittelyn osalta.[670]

Esimerkiksi tapauksessa **EUT 5.6.2018 C-210/16 Wirtschaftsakademie Schleswig-Holstein** toisen perustaman alustan hyödyntäminen ilman mahdollisuutta vaikuttaa käyttöehtoihin ei vapauta henkilötietojen suojaa koskevien velvollisuuksien noudattamisesta. Tässä tapauksessa yritys ”Wirtschaftsakademie” tarjosi koulutuspalveluita Facebookissa olevan käyttäjätilin kautta. Tällöin Facebook keräsi tietoja, joita voitiin yhdistää tiettyyn henkilöön ja Wirtschaftsakademie sai tietoja vain anonyymeina. EUT kuitenkin totesi, että sivun hallinnoija Wirtschaftsakademie osallistui henkilötietojen käsittelyn tarkoituksen ja keinojen määrittelemiseen tekemällä käsittelyyn liittyviä valvontoja omien tavoitteidensa mukaisesti. Näin ollen Wirtschaftsakademie oli rekisterinpitäjä yhdessä Facebook Irelandin kanssa eikä yhteisen vastuun syntyminen edellyttänyt, että kaikilla vastuullisilla toimijoilla olisi pääsy henkilötietoihin. Yhteinen vastuu ei välttämättä merkitse henkilötietojen käsittelyyn osallistuvien samanlaista vastuuta.[671] Eri toimijat voivat osallistua henkilötietojen käsittelyyn eri vaiheissa ja eriasteisesti, jolloin kunkin vastuun taso on arvioitava huomioon ottaen kaikki merkitykselliset

[667] Voutilainen 2019: 146–147.
[668] Ivanova 2020: 67.
[669] Euroopan WP29-tietosuojatyöryhmä WP169: *Opinion 1/2010 on the concepts of ”controller” and ”processor”, s.* 25.
[670] Voutilainen 2019: 44–45.
[671] Korpisaari & Toikkanen 2020: 467–468; Lindroos-Hovinheimo 2018: 762.

olosuhteet. Keskeistä kuitenkin mainitussa tapauksessa on perusoikeuksien toteutumisen vaatimus, jonka myötä rekisterinpitäjän käsitteen laaja tulkinta on omiaan vahvistamaan luonnollisten henkilöiden oikeutta henkilötietojen suojaan.[672] Tämän ratkaisun perusteella voidaan myös tietoturvatoimenpiteiden toteuttamisen osalta todeta, että yhteisen vastuun omaavien tahojen ei välttämättä tarvitse toteuttaa samanlaisia tietoturvavastuita ja -toimenpiteitä. Esimerkiksi edellä mainitussa tapauksessa Facebook Irelandilla on erilaiset vastuut tietoturvan osalta alustan tarjoajana, jotta Facebookin käyttö olisi turvallista ja siellä oleva tieto olisi saatavilla ja eheää, sekä luottamuksellista siinä laajuudessa kuin sen käyttäjät haluavat.

Hyvänä tietoturvallisena käytäntönä pidetään tietyn tietoturvatason edellyttämistä hankintasopimuksissa, ja tämä onkin saattanut toteutua useissa organisaatioissa jo ennen tietosuoja-asetuksen voimaantuloa. Hankintojen osalta tietosuojaa koskevien sopimusvaatimusten kehittyminen tietoturvan huomioon ottavalla tavalla on ollut tärkeä edistysaskel organisaatioiden tietoturvan kannalta, vaikkakin näkökulmana on henkilötietojen suojaaminen: sopimukset velvoittavat sopimustahoja toteuttamaan tietoturvatoimenpiteitä. Esimerkiksi tietosuoja-asetuksen 28 artiklan mukaisesti sopimuksessa tai sen liitteessä on kuvattava ne tekniset ja organisatoriset toimenpiteet, joita henkilötietojen käsittelijän on noudatettava rekisterinpitäjän lukuun. Koska rekisterinpitäjän on 28 (1) artiklan mukaisesti varmistettava henkilötietojen käsittelijän kelvollisuus käsitellä henkilötietoja, on nämä teknisiin ja organisatorisiin toimiin liittyvät vaatimukset asetettava jo tarjouspyynnössä.[673] Teknisistä ja organisatorisista toimenpiteistä ei ole lain teknologianeutraalisuuden takia spesifejä vaatimuksia, vaan tässäkin kohtaa asia jää sopimusosapuolten hiottavaksi. Yhtä lailla esimerkiksi tiedonhallintalain 13 §:ssä on asianmukaisesti ja teknologianeutraalisti huomioitu hankintojen tietoturvallisuus. Lain mukaan viranomaisten on varmistettava hankinnoissaan, että tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Järjestelmien ja palveluiden suunnittelun merkitys korostuu lainsäädännön vaatimusten noudattamisen varmistamiseksi myös ulkoistamisen ja hankintojen sekä niihin liittyvien sopimusvaatimusten kohdalla. Luottamuksellisuuden ylläpitäminen ei edellytä pelkästään sopimuksia, vaan se vaatii myös teknisten toimenpiteiden toteuttamista, joilla varmistettaan, että luvattomilla henkilöillä ei ole, eivätkä he ole saaneet pääsyä luottamuksellisiin tietoihin.[674] Hallinnollisten ja fyysisten tietoturvatoimenpiteiden toteuttaminen on yhtä lailla tärkeää.

---

[672] Lindroos-Hovinheimo 2018: 761–762.
[673] Voutilainen 2019: 147.
[674] Johnssén 2018: 389.

Tarvittavat tietoturvallisuustoimenpiteet tulisi määritellä jo hankintojen suunnitteluvaiheessa ennen tarjouspyyntöä. Lisäksi tietojärjestelmän, tietoaineiston ja koko palvelun osalta tulee selvittää jo hankintavaiheessa tietoturvallisuuden toteutuminen kaikissa elinkaaren vaiheissa. Tämä tarkoittaa tietoturvavaatimusten ulottamista palvelun tai tuotteen koko elinkaareen. Vaatimusmäärittely tulisikin olla riskilähtöistä. Niissä tulee myös ottaa huomioon koko alihankintaketju sekä palvelun tuottamisen kansallinen ulottuvuus.[675] Mikäli hankittavassa järjestelmässä tai palvelussa henkilötietoja käsitellään toimittajan tai toimittajan alihankkijan eli henkilötietojen alikäsittelijän toimesta EU/ETA -alueen ulkopuolella, tulee myös huomioida käsittelyn siirtoperuste sekä mahdollisesti arvioida TIA-menettelyllä (*Transfer Impact Assessment*) tapauskohtaisesti tiedonsiirron tietosuoja sekä mahdolliset täydentävät suojatoimet, jos siirtoperuste ei täysin riittäisi takaamaan EU:n vaatimuksien mukaista tietosuojan tasoa.

Huomioitava on, että myös NIS 2 -direktiivi *kannustaa* keskeisiä ja tärkeitä toimijoita huomioimaan sopimusasiat välittömien toimittajiensa ja palvelutarjoajiensa kanssa ja sisällyttämään kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin[676]. Edellä mainitun lisäksi NIS 2 -direktiivin kohdan 85 mukaan keskeisten ja tärkeiden toimijoiden tulisi arvioida ja ottaa huomioon toimittajiensa tuotteiden ja palveluntarjoajiensa palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet ja toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt. Saman tyyppinen vaatimus esiintyy myös tuoreen kyberturvallisuuslain 9 §:n 4 kohdassa, jossa kolmansien osapuolien osalta on todettu, että kyberturvallisuuden riskienhallinnan toimintamallissa ja hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt[677]. Tällainen kolmansien osapuolien tarjoamien tuotteiden ja palvelujen arviointi ja kyberturvallisuuskäytäntöjen huomioon ottaminen voisi käytännön tasolla toteutua esimerkiksi varmistamalla hankinnan tietoturvavaatimuksien toteutuminen jo ennen sopimuksen tekoa markkinavuoropuheluvaiheessa, liittämällä nämä vaatimukset osaksi sopimusta velvoittavaksi sopimusliitteeksi sekä säännöllisesti arvioimalla tai auditoimalla näiden vaatimusten toteutumista. Tietoturvamaturiteetiltaan kehittyneimmissä organisaatioissa yleensä onkin käytössä hankinnan tietoturvavaatimukset, jotka voivat olla koostettuna

[675] Valtiovarainministeriön julkaisuja 2023:57: 8, 16.
[676] Vastaavanlaisesti on todettu myös NIS 2 -direktiivin implementointia koskevassa hallituksen esityksessä 57/2024 vp, ks. s. 93 ja 164.
[677] HE 57/2024 vp: 278.

esimerkiksi Excel-dokumenttiin pohjautuen tiettyyn viitekehykseen, viitekehysten yhdistelmään tai johonkin muuhun hyvien käytänteiden mukaiseen vaatimuskehikkoon[678].

Lain esitöissä on todettu, että säädettyjen vaatimusten kannalta toimija vastaa itse siitä, että se käyttäisi toiminnassaan sellaisia tuotteita ja palveluita, jotka vastaisivat toimijan riskienhallinnan vaatimuksia[679]. Kyseinen toteamus on erittäin laveasti muotoiltu ja siitä on vaikea tulkita, onko kyseessä hankinnan yhteydessä tehtävän riskien arvioinnin hallintatoimenpiteistä nousevat vaatimukset. Kuitenkin NIS 2 -direktiivissä on sanatarkasti mainittu, että toimijoiden on arvioitava edellä mainittuja asioita, kuten toimittajien ja palveluntarjoajien kyberturvallisuuskäytäntöjä, mikä viittaa riskien arviointiin. Osana hallituksen esitystä on todettu, että toimijoiden tulisi ylläpitää toimitusketjusta kuvausta, joka sisältäisi riippuvuudet, haavoittuvuudet, uhat ja riskien vaikutukset[680]. Tämä tukee sitä, että osana dokumentoitua kyberturvallisuuden riskienhallinnan toimintamallia tällaisia toimitusketjujen riskejä olisi tarkoituksenmukaista arvioida. Riskienarvioinnin tunnistettuja riskejä hallittaisiin riskienhallintatoimenpitein, jotka olisivat suotavaa sisällyttää sopimusjärjestelyihin esimerkiksi osana tietoturvavaatimuksia[681].

Tietoturvavaatimusten ulottaminen kolmansien osapuolten sopimuksiin on tärkeää: nykyisessä globalisoituneessa verkkoyhteiskunnassa toimitusketjujen hyödyntäminen tietoturvahyökkäyksissä on sitä helpompaa, mitä useimpia toimijoita on. Hyökkäyksiä, joissa hyväksikäytetään organisaation luottamusta toimittajiinsa ja tavoitteena on saada jalansija eri organisaatioissa toimitusketjun sisällä, kutsutaan toimitusketjuhyökkäyksiksi[682]. Näissä rikolliset nimenomaan yrittävät päästä huomaamattomasti organisaatioiden tietoihin ja järjestelmiin kiinni alihankintaketjujen ja kolmansien osapuolien palvelujen kautta. Erityisesti pitkät arvoketjut luovat uusia haavoittuvuuksia ja mahdollisuuksia väärinkäytöksiin[683]. Myös Eurooppa-neuvosto on painottanut toimittajariippuvuuden välttämistä sekä

[678] Esimerkiksi hankinnoissa voi hyödyntää julkiselle hallinnolle suunnattuja työkaluja, kuten valtiovarainministeriön luomaa hankintaehtotyökalua. Ks. Valtiovarainministeriön julkaisuja 2023:57. Sivuilta löytyy mm. hankintaehtotyökalu, suositusliitteet tietoturvallisuusvaatimuksista sekä suositus tietoturvallisuudesta hankinnoista.
[679] HE 57/2024 vp: 164. Selvyyden vuoksi todetaan, ettei lakiin perustuva riskienhallintavaatimus koskisi alihankkijaa, ellei se itsekin ole toimija, jonka toimintaa sääntely koskee.
[680] HE 57/2024 vp: 93–94.
[681] HE 57/2024 s. 164 mainitaan, että toimijat voisivat *tarvittaessa* pyrkiä hallitsemaan toimitusketjujen kyberturvallisuusriskiä sopimusjärjestelyin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa. Minusta tällainen tapauskohtainen arviointi on haastavaa, minkä takia organisaatiolla tulisi aina olla hankinnoissa vähimmäistietoturvavaatimukset toimittajille. Nämä vaatimukset voisivat huomioida myös toimitusketjuriskit.
[682] Traficomin julkaisuja 21/2022: 2.
[683] Pöysti 2023: 47.

erityisesti tieto- ja viestintätekniikan toimittajien monipuolistamista jäsenvaltioissa, jotta vältettäisiin suurien riippuvuuksien muodostuminen yksittäisistä toimittajista sekä altistuminen näiden mahdollisten häiriöiden seurauksille[684]. Tämä on tärkeä seikka, joka tulisi huomioida myös Suomessa[685]. Esimerkiksi monet kansalliset organisaatiot ovat erittäin riippuvaisia Microsoftin tuotteista ja palveluista, mikä on riskienhallinnan näkökulmasta ongelmallista.

Lopuksi yhteenvetona voidaan todeta seuraavaa: koska NIS 2 -direktiivin osalta kyseessä on enemmänkin kannustaminen kyberturvallisuusriskien hallintatoimenpiteiden huomioimiseen sopimuksissa eikä niinkään suora velvoite, tietoturvan sääntelyjärjestelmässä keskeiset, kaikkia organisaatioita koskevat sopimusvaatimukset tietoturvan osalta nousevat voimassa olevasta tietosuojalainsäädännöstä. Tietosuojalainsäädäntö asettaa minimikriteerit myös tietoturvavaatimuksille hankintasopimuksissa: henkilötietojen käsittelystä on aina tehtävä sopimus rekisterinpitäjän ja henkilötietojen käsittelijän välillä, ja tämän sopimuksen osalta on tietosuoja-asetuksessa asetettu vähimmäisvaatimuksia. Esimerkiksi henkilötietojen käsittelijän tulee toteuttaa 32 artiklassa määritetyt asianmukaiset tekniset ja organisatoriset toimenpiteet. Henkilötietojen käsittelijä ei saa myöskään käyttää muita henkilötietojen käsittelijöitä eli alikäsittelijöitä palveluissaan ilman rekisterinpitäjän lupaa. Tietosuoja-asetuksen myötä tulleet tietoturvavaatimukset henkilötietojen suojaamiseksi sekä muut sisältövaatimukset kirjallisille sopimuksille ovat parantaneet tietoturvan huomioimista osana hankintoja. Vaikka keskeisenä näkökulmana onkin henkilötietojen suojaaminen, tietyn tietoturvatason edellyttäminen ja tietoturvatoimenpiteiden varmistaminen sopimuksella edistävät muidenkin luottamuksellisten tietojen suojaamista parantamalla molempien sopimusosapuolten tietoturvatasoa. Näin ollen tietoturvavaatimusten ulottaminen hankintoihin on tärkeää: hankinnan tietoturvavaatimusten toteutuminen tulisi varmistaa jo ennen sopimuksen tekoa. Lisäksi toimittajakohtaisten tietoturvavaatimusten toteutumista tulisi säännöllisesti arvioida hankinnan elinkaaren ajan toimitusketjuihin liittyvien tietoturvariskien pienentämiseksi.

---

[684] Euroopan unionin neuvosto, Neuvoston päätelmät tieto- ja viestintäteknisen toimitusketjun turvallisuudesta 17.10.2022: 7 ja 13. Neuvosto on myös kannustanut, että EU:n lainsäädäntöön sisällytettäisiin toimittajariippuvuuden ehkäisemiseen liittyvät näkökohdat.

[685] Huomioitava on, että NIS 2 -direktiivin 22 artiklassa on todettu, että NIS-yhteistyöryhmä voi yhdessä Euroopan komission ja ENISAn kanssa tehdä koordinoituja turvallisuusriskiarviointeja tietyistä kriittisistä tieto- ja viestintätekniikan eli TVT-palvelujen, -järjestelmien ja -tuotteiden toimitusketjuista. Näiden riskiarviointien osalta kansallinen valvova viranomainen voi tulevaisuudessa määräyksellä edellyttää toimijoiden ottaa huomioon riskiarvioin tulokset (HE 57/2024 vp, s. 164). Tätä ei suoraan sisällytetty kyberturvallisuuslain 9 §:n 4 kohtaan, kun taas vastaavaa vaatimusta koskevan tiedonhallintalain 18 c §:n 4 kohdassa tämä on huomioitu.

3.3.3 Henkilötietojen käsittelyn riskilähtöisyys ja riskiarviointi

Jo kansallisen henkilötietolain aikoihin lähtökohtana oli se, että rekisterinpitäjän piti arvioida itse tietoturvatasonsa riittävyys ja suorittaa tietynlaista tietojärjestelmien laillisuusvalvontaa tietoturvatason osalta. Tämä johtui syystä, että riittävää tietoturvan tasoa ei ollut kattavasti määritelty säädöstasolla tai oikeustapauksissa. Lopputuloksen katsottiin olevan huono, ja samankaltaisten tietojen suojaamiseen käytettävät menetelmät ja tietoturvataso vaihtelivat organisaatioittain rekisteripitäjäkohtaisesti.[686] Nyttemmin tietosuojalainsäädännön kehityksen myötä henkilötietojen suojaamiseen vaadittavat tietoturvatoimenpiteet ovat yhtenäistyneet etenkin erityisten henkilötietojen suojaamisen, mutta myös esimerkiksi dokumentaatiovaatimusten, osalta. Lisäksi henkilötietojen käsittelyyn liittyvien tietoturvatoimenpiteiden taustalla tulisi olla riskiperustainen arviointi.

Tietosuoja-asetuksen lähtökohtana on riskilähtöisyys, eli valittavien toimenpiteiden ja suojauksen tulee perustua organisaation tekemään riskiarvioon. Riskilähtöisyyden pitäisi ohjata koko organisaation henkilötietojen käsittelyä. Se tulisi ottaa osaksi organisaation kokonaisvaltaista riskienhallintaprosessia, mikä myös osaltaan osoittaisi rekisterinpitäjän osoitusvelvollisuuden toteutumista.[687] Tietosuoja-asetus korostaa riskiperusteista suunnittelua ja henkilötietojen hallintaa, johon liittyy jatkuvaa riskien kartoittamista, arviointia ja reagointia. Tällaisen toiminnan pohjalta tulisi toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet.[688] Kumottuun henkilötietolakiin verrattuna tämä muutos on ollut edistysaskel, sillä riskilähtöisyys parantaa myös organisaatioiden tietoturvaan liittyviä hyviä käytänteitä. Mikäli henkilötiedot eivät ole suojassa, eivät todennäköisesti ole myöskään organisaation muutkaan suojattavat tiedot.

Rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyviä riskejä aina ennen käsittelytoimien aloittamista. Tietosuoja-asetuksen riskilähtöisyys ilmenee muun muassa tietosuoja-asetuksen 35 artiklasta, jossa säädetään tietosuojaa koskevasta vaikutustenarvioinnista eli DPIA-arvioinnista (Data Protection Impact Assessment). Tällä tarkoitetaan menettelyä, jossa arvioidaan henkilötietojen käsittelystä mahdollisesti aiheutuvia riskejä luonnollisten henkilöiden oikeuksiin ja vapauksiin[689]. Oikeuksilla ja vapauksilla tarkoitetaan tässä yhteydessä ensisijaisesti oikeutta yksityisyyteen ja tietosuojaan, mutta niillä voidaan myös tarkoittaa muita perusoikeuksia [690] . Tässä kohtaa huomioitava on, että riskillä ei tarkoiteta

[686] Laaksonen, Nevasalo & Tomula 2006: 45.
[687] Andersson 2018: 6; VAHTI 1/2016: 21.
[688] Voutilainen 2019: 123–124.
[689] Nyyssölä 2018: 269.
[690] Europan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 7.

rekisterinpitäjän havaitsemia henkilötietojen käsittelyyn liittyviä lainvastaisia menettelyjä, vaan tuolloin kyseessä on jo toteutunut riski[691]. Artiklan mukaan rekisterinpitäjä on pääsääntöisesti velvollinen tekemään DPIA-arvioinnin, mikäli henkilötietojen käsittely todennäköisesti aiheuttaisi luonnollisen henkilön oikeuksien ja vapauksien kannalta *korkean riskin*. DPIA:n tarkoitus on auttaa rekisterinpitäjää tietosuojalainsäädännön noudattamisessa, dokumentoinnissa ja osoitusvelvollisuuden[692] täyttämisessä, jolloin tietosuojavastaava on nimenomaan neuvonantajan roolissa.

DPIA-arviointi tulee ajankohtaiseksi erityisesti silloin, kun arvioidaan järjestelmällisesti ja kattavasti luonnollisten henkilöiden ominaisuuksia automaattisen käsittelyn avulla (esimerkiksi profilointi) ja, kun tämä arviointi johtaa luonnollista henkilöä koskeviin oikeusvaikutuksiin tai muuten merkittävällä tavalla vaikuttaviin päätöksiin. DPIA-arviointi tulee myös tehdä, mikäli toiminnassa käsitellään laajamittaisesti erityisiä henkilötietoryhmiä taikka tietoa, joka liittyy rikostuomioihin ja rikkomuksiin, taikka jos järjestelmällisesti ja laajamittaisesti valvotaan yleisölle avointa aluetta. Mikäli henkilötietojen käsittelyssä käytetään uutta teknologiaa, tulee myös DPIA tehdä[693].

Kyseiset käsittelytoimet aiheuttavat todennäköisesti korkean riskin henkilön oikeuksien ja vapauksien kannalta. Luettelo ei ole kuitenkaan tyhjentävä, vaan tietosuojatyöryhmä on listannut myös muita käsittelytoimia, jotka aiheuttavat todennäköisesti korkean riskin mitä useampi kriteeri täyttyy. Tällaiset toimet voivat olla arviointia tai pisteytystä[694], oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia aiheuttavaa automaattista päätöksentekoa, järjestelmällistä valvontaa, arkaluontoisten tai hyvin henkilökohtaisten tietojen käsittelyä, tietojen laajamittaista käsittelyä, heikossa asemassa olevien rekisteröityjen tietojen käsittelyä[695] sekä uusien teknisten tai organisatoristen ratkaisujen innovatiivista käyttöä ja soveltamista. Korkean riskin voivat myös aiheuttaa tietokokonaisuuksien

---

691 Voutilainen 2019: 125.

692 DPIA-arvioinnin osalta on huomioitava, että se on rekisterinpitäjän sisäinen prosessi eli tietosuoja-asetus ei velvoita vaikutustenarvioinnin tulosten julkaisemista tai tiedottamista rekisteröidyille, vaikkakin DPIA:n tekeminen ja julkistaminen voivat lisätä luottamusta rekisterinpitäjän palveluja kohtaan. DPIA-arvioinnin ensisijaisena tarkoituksena on auttaa rekisterinpitäjää tietosuoja-asetuksen noudattamisessa sekä osoitusvelvollisuuden toteennäyttäjänä. Ks. Nyyssölä 2018, s. 270.

693 Tietosuojavaltuutetun toimisto 2023.

694 Arviointi tai pisteytys, joka liittyy rekisteröidyn terveyteen, työsuoritukseen, taloudelliseen tilanteeseen, mieltymyksiin tai kiinnostuksen kohteisiin, sijaintiin tai liikkumiseen taikka luotettavuuteen tai käyttäytymiseen. Ks. Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 10.

695 Esimerkiksi lapset, työntekijät, ikääntyvät ihmiset, potilaat, turvapaikanhakijat sekä muut väestöryhmät.

yhteensovittaminen tai yhdistäminen, kun kyseessä on useampaan eri tarkoitukseen suoritetusta ja/tai eri rekisterinpitäjien suorittamasta käsittelytoimesta. Lisäksi sellaiset käsittelytoimet, jotka estävät rekisteröityjen oikeutta käyttää palvelua, tehdä sopimus tai muuttaa kyseistä oikeuttaan, voivat todennäköisesti aiheuttaa korkean riskin henkilön oikeuksien ja vapauksien kannalta. Lähtökohtaisesti jos edellä mainituista kriteereistä kaksi täyttyy henkilötietojen käsittelyssä, DPIA tulisi tehdä.[696] Organisaation tietoturvanäkökulmasta tällainen korkea riski syntyy etenkin sellaisessa henkilötietojen käsittelyssä, jossa yhdistyy sekä järjestelmällinen valvonta että heikommassa asemassa olevien työntekijöiden henkilötiedot. Esimerkkinä tästä on työpaikalla tehtävä teknisin menetelmin toteutettu tietoturvavalvonta tietojärjestelmissä ja kameravalvonta[697].

Tietosuojavaltuutettu myös painottaa DPIA-arvioinnin tekemistä, kun edellä mainituista käsittelytoimista täyttyy vähintään yksi kriteeri ja se yhdistetään rekisteröidyn informoinnista poikkeamiseen, biometristen tietojen käsittelyyn henkilön yksiselitteistä tunnistamista varten, geneettisten tietojen käsittelyyn sekä sijaintitietojen käsittelyyn. Myös ilmiantojärjestelmien (*whistleblowing*) henkilötietojen käsittelystä on tehtävä DPIA.[698] Näin ollen organisaatioiden tietoturvatoimenpiteitä, jotka voivat aiheuttaa todennäköisesti korkean riskin henkilön oikeuksien ja vapauksien kannalta, ovat esimerkiksi työpaikoilla tapahtuva biometrinen henkilötunnistus organisaation kulunvalvonnan yhteydessä. Biometrisessä tunnistuksessa liitetään perinteisiin tunnistautumismenetelmiin fysiologisia tai käyttäytymiseen liittyviä ominaisuuksia, kuten kasvokuva, silmän iiris, sormenjälki, kädenjälki, käsiala tai ääni, jotka parantavat turvallisuutta ja tekevät tunnistautumisesta vahvan[699].

Kansallisessa tietosuojalaissa tietosuojan vaikutustenarvioinnista on mainittu ainoastaan 6 §:ssä, jonka mukaan erityisiä henkilötietoryhmiä koskevan käsittelyn yhteydessä rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaisia ja erityisiä toimenpiteitä rekisteröidyn oikeuksien suojaamiseksi, kuten esimerkiksi laatia tietosuoja-asetuksen mukainen DPIA-arviointi. Näin ollen esimerkiksi, jos organisaatiossa käsitellään terveystietoja laissa säädetyn tehtävän perusteella, DPIA tulee tehdä. Tämä koskee usein esimerkiksi henkilöstöhallinnon järjestelmiä, joissa saatetaan käsitellä terveystietoja ja sairauspoissaoloja sairausajan palkan tai etuuksien maksua varten sekä sen selvittämiseksi, onko poissaolo ollut perusteltua.

---

[696] Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 10–12.
[697] Ks. myös luku 3.5.4 (”Muu teknisin menetelmin toteutettu valvonta ja välitystiedot”).
[698] Tietosuojavaltuutetun toimisto 2018.
[699] Korja 2016b: 139–140.

Tietosuoja-asetuksen mukaan DPIA-arviointi on toteutettava ennen henkilötietojen käsittelyä ja sen on käsiteltävä suunniteltujen käsittelytoimien vaikutuksia henkilötietojen suojalle. Mikäli tietosuojavastaava on nimitetty organisaatiossa, rekisterinpitäjän tulee kysyä neuvoa tältä DPIA-arviointia tehdessään.

DPIA-arvioinnin tulee sisältää ainakin:

a) arvio rekisteröidyn vapauksiin ja oikeuksiin kohdistuvista riskeistä;

b) järjestelmällinen kuvaus suunnitelluista henkilötietojen käsittelytoimista ja käsittelytarkoituksista;

c) arvio henkilötietojen käsittelyn tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden; sekä

d) kooste suunnitelluista toimenpiteistä riskien hallitsemiseksi, mukaan lukien toimet osoitusvelvollisuuden toteennäyttämiseksi.

Jos riski muuttuu, rekisterinpitäjän tulee uudelleen tarkastella, tapahtuuko henkilötietojen käsittely DPIA-arvioinnin mukaisesti. DPIA-arviointi koskee pääsääntöisesti yhtä tiedonkäsittelytoimea, mutta sitä voidaan käyttää myös useiden sellaisten käsittelytoimien arviointiin, joiden riskit, luonne, laajuus, asiayhteys ja tarkoitus ovat samankaltaisia[700]. Näin ollen tietosuojariskien arviointi on ennemminkin käsittelytoimikohtaista kuin esimerkiksi järjestelmäkohtaista, ellei itse järjestelmässä ole tietyn tyyppistä käsittelyä.

Mikäli DPIA-arviointi osoittaisi, että henkilötietojen käsittely aiheuttaisi aikaisemmin mainitun korkean riskin mitigointitoimenpiteistä riippumatta, rekisterinpitäjän on ennen henkilötietojen käsittelyn aloittamista kuultava ennakolta valvontaviranomaista sekä toimitettava asetuksessa määritellyt tiedot tälle.

Huomioitava on, että kaikissa tapauksissa DPIA:a ei ole tarvetta tehdä. Käytännössä ennen uusia henkilötietojen käsittelytoimien aloittamista tulee tehdä DPIA-tarvearvio. Mikäli aikaisemmin mainitut kriteerit eivät täyttyisi eikä tarvearvio siten indikoisi korkeaa riskiä, ennen henkilötietojen käsittelyn aloittamista tulee tehdä joka tapauksessa perusmuotoinen riskiarviointi.

Perusmuotoinen riskiarvio on perusteltua, sillä rekisterinpitäjällä on silti yleinen velvollisuus toteuttaa toimenpiteitä, joilla hallitaan rekisteröidyn oikeuksiin ja vapauksiin kohdistuvia riskejä. Käytännön tasolla tämä tarkoittaa henkilötietojen

[700] Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 15.

käsittelyyn liittyvien riskien arviointia aina ennen henkilötietojen käsittelyyn ryhtymistä, jotta voitaisiin tunnistaa, milloin tietyntyyppinen käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Riskit on tunnistettava, arvioitava, käsiteltävä ja tarkasteltava säännöllisesti uudelleen.[701] Riskejä tulee arvioida niiden ihmisten näkökulmasta, joiden henkilötiedoista on kysymys, jolloin tietoturvariskin vakavuutta arvioitaessa on huomioitava ihmiselle aiheutuva vahinko[702]. Käytännössä tällainen perusmuotoinen riskiarviointi olisi myös hyvä dokumentoida. Mikäli perusmuotoisen riskiarvioinnin tuloksena on se, että käsittelystä aiheutuu korkea riski henkilön oikeuksille ja vapauksille, DPIA on tehtävä.

Kyseinen tietosuojatyöryhmän ohjeistus vastaa hyvien riskienhallintakäytänteiden mukaista riskienhallintaprosessia. On kuitenkin vaikeaa arvioida täysin, miten organisaatioissa henkilötietojen käsittelyyn liittyvien perusmuotoisten riskien arviointien ja DPIA-arviointien mukaiset riskienhallintatoimet näkyvät organisaatioiden kokonaisriskienhallinnassa. Pienemmissä organisaatioissa henkilötietojen käsittelyyn liittyvät riskiarviot ja DPIA-arviot saattavat muun muassa edistää tietoturvaan liittyvää säännöllistä ja jatkuvaa riskien tunnistamista. Vastakohtaisesti suuremmissa organisaatioissa tällaiset saattavat jäädä esimerkiksi palvelun omistajien ja tietosuojasta vastaavien henkilöiden tietoon valumatta kuitenkaan tietoturvasta vastaaville henkilöille osaksi tietoturvariskienhallintaa ja kokonaisriskienhallintaa.

Huomioitava on myös se, että tietosuojan riskienhallinnassa fokuksessa on riskien vakavuutta arvioitaessa luonnollisten henkilöiden oikeudet ja vapaudet. Vastakohtaisesti organisaatioiden kokonaisriskienhallinnassa keskitytään vakavuuden arvioinnissa muun muassa liiketoiminnan rahalliseen menetykseen, mainehaittaan ja asiakkaiden menettämiseen. Näkökulma on näin ollen eri ja siksi henkilötietojen käsittelyn riskejä voi olla hankalaa synkronoida suoraan sellaisenaan organisaatioiden kokonaisriskienhallintaan.

Tietosuoja-asetus itsessään ei anna mitään tiettyä metodologiaa tai työkaluja, miten riskejä tulisi arvioida tai miten koko DPIA-arviointi tulisi toteuttaa. Erilaiset soft law- ja yhteissääntelymekanismit sekä sertifiointi voivat olla avuksi käytännön toteuttamisessa ja tietosuoja-asetuksen vaatimusten toteennäyttämisessä. Oikeudellisesta näkökulmasta standardien hyväksikäyttöä tietosuoja-asetuksen vaatimusten toteennäyttämiseksi on kuitenkin kritisoitu, sillä standardien lähestymistapa tietosuojan toteuttamiseksi on organisaatiolähtöinen ja tietoturvaluonteinen.

---

[701] Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 7.
[702] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 33.

Esimerkiksi DPIA-arvioinnin koko lähtökohta on arvioida luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä. DPIA-arvioinnin (tai ylipäätänsä tietosuojariskien arvioinnin) *”riski oikeuksille”* -ydinlähestymistapa onkin haastava muun muassa sen suhteen, miten integroida tällainen metodologia itse riskiarvioinnin tekemiseen.[703] On itsestään selvää, että tietosuojalainsäädännön keskeisenä näkökulmana on luonnollisten henkilöiden ihmis- ja perusoikeuksien suojaaminen, kun taas esimerkiksi standardit keskittyvät näkökulmaltaan käytännön toteuttamisratkaisuihin. Edellä esitetty kritiikki on siten sinänsä turhan ankara, sillä standardien tehtävä on nimenomaan olla avuksi käytännön työn toteuttamisessa sekä antaa esimerkkejä, millä tavoin tietosuoja-asetuksen vaatimuksia voisi toteennäyttää tietoturvatoimenpiteillä. Standardien noudattaminen ja niihin liittyvä sertifiointi onkin hyvä tapa todentaa, että tietoturva ja tietosuoja ovat tietyllä standardin määrittämällä tasolla. Näiden työkalujen avulla ei itsessään tehdä DPIA-arviointia, mutta ne voidaan mainita DPIA:ssa osoituksena tietojen turvaamisen vähimmäistasosta ja siihen liittyvistä käytännöistä. Esimerkiksi tietosuojavaltuutetun sivuilta on mahdollista löytää DPIA-pohja Excel-muodossa, jossa tietosuojaperiaatteet-välilehdellä on kohta referenssinä oleville käytännesäännöille ja sertifioinneille[704].

Toinen keskeinen kritiikki kohdistuu ISO/IEC 29134 -standardiin, johon tietosuojatyöryhmä on usein viitannut relevanttina metodologina. ISO/IEC 29134 -standardin tarkoituksena on ollut toimia käytännön ohjeistuksena DPIA-arvioinnin tekemiselle, mutta sille ei tehty ikinä metodologisia muutoksia, vaan näkökulmana säilyi ISO/IEC-standardeille tyypillinen tietoturvallisuuden hallintajärjestelmä (ISMS) -fokus. ISO/IEC 29134 -standardi korostaa myös organisaatiolähtöistä ajattelua, minkä vuoksi on kritisoitu standardin tietosuojan painottamisen jäävän kapeammalle alalle sekä yksilöiden oikeuksien ja vapauksien tunnistamisen epäonnistuvan. Organisaationäkökulman vuoksi saattaa syntyä myös ristiriita DPIA:n luonnollisiin henkilöihin kohdistuvan riskiarvioinnin sekä tietojen käsittelijään kohdistuvien riskien kanssa. ISO/IEC 29134 -standardissa riski tulisi hyvien käytänteiden mukaisesti ensiksi tunnistaa, sitten analysoida ja viimeiseksi arvioida, jolloin päämääräksi jää riskin mitigointi eli pienentäminen. Prosessin aikana organisaation tulee arvioida riskin vaikutustaso sekä riskin todennäköisyys, jossa yleensä riippuen olosuhteista käytetään laadullista tai määrällistä analyysia. Suosituksena kuitenkin on, että mahdollisuuksien mukaan riskien arvioimiseen käytettäisiin yksityiskohtaisempaa kvantitatiivista eli määrällistä analyysia, jossa asetetaan tietyt arvot mahdollisille seurauksille sekä riskien toteutumisen todennäköisyyksille. Näin ollen kyseinen standardi myös pyrkii määrittämään riskin kvantifioimalla sen todennäköisen haitan luonnollisen henkilön oikeuksille.

[703] Christofi, Dewitte, Ducuing & Valcke 2020: 158–159.
[704] Ks. Excel ja ohjeet: Tietosuojavaltuutetun toimisto 2023.

Yksityisyyteen liittyvän riskin kvantifioiminen on nähty ongelmallisena, sillä on vaikeaa, ellei lähes mahdotonta määritellä numeraalisesti potentiaalisia haittoja *”oikeuksille ja vapauksille”,* jotka ovat itsessään aineettomia. Lisäksi ISO-lähestymistavan mukaisesti kvantifioiminen keskittyy yksilöihin kohdistuviin mahdollisiin seurauksiin, kun taas tietosuoja-asetuksessa tietojen suojaamisen kannalta tulee ottaa huomioon myös yhteiskunta-aspekti eli tietojen suojaaminen on tasapainotettava ottaen huomioon myös muut oikeudet ja etuudet oikeasuhteisella tavalla.[705] Kuten aikaisemmin on todettu, standardien tehtävänä on lähinnä käytännön tietoturva- ja tietosuojatyön toteuttamisesimerkkien antaminen tai vähimmäistason todentaminen. Näin ollen standardien luomistyössä on ollut mukana todennäköisesti enemmän tietoturva-asiantuntijoita kuin oikeudellisia osaajia, joten ihmis- ja perusoikeuksien painotus on myös siksi jäänyt vähemmälle. Toki ISO/IEC 29134 -standardi on luotu nimenomaan käytännön esimerkiksi DPIA-arvioinnin tekemiselle, jolloin siinä tulisi yhtä lailla painottaa tietosuojanäkökulmaa sekä tietojen käsittelyn vaikutusta oikeuksille ja vapauksille.

Edellä mainitun kritiikin mukaisesti on totta, että yksityisyydelle sekä muille *”oikeuksiin ja vapauksiin”* kohdistuville mahdollisille haitoille on vaikeaa määritellä numeraalista arvoa riskien arvioinnissa. Tämä kuitenkin kuulostaa suppealta kritiikiltä, kun otetaan huomioon, että se kohdistuu nimenomaan työkaluun, jonka tarkoituksena on auttaa riskien arviointia ja sitä myöten riskeihin reagointia. Organisaatioissa tehtävä riskien arviointityö on nimenomaan asiantuntijoiden arvioihin perustuvaa skenaarioiden punnintaa, eikä esimerkiksi myöskään tietovuodosta tai palvelunestohyökkäyksestä aiheutuvasta organisaation mainehaitasta ole välttämättä helppoa antaa numeraalista arvoa. Täten kritiikki onkin varsin perusteeton, sillä siitä puuttuu näkökulma käytännön työn toteutukseen.

Numeroiden avulla riskit ovat usein helpompi arvottaa tärkeysjärjestykseen ja siten reagoida niihin asianmukaisesti. Siksi myös usein henkilöihin kohdistuvat riskit arvioidaan mahdollisimman kriittisiksi. Henkilöihin kohdistuvia riskejä voivat olla tietosuojariskien lisäksi myös henkilöturvallisuuteen liittyvät riskit, jotka uhkaisivat henkilöiden henkeen tai terveyteen kohdistuvaa turvallisuutta. Useimmiten käytännön työssä arvioidaan numeraalisesti riskin todennäköisyyttä ja riskin vaikutusta[706] esimerkiksi numeroilla 1–4 tai 1–5. Riskin todennäköisyyden numeraalinen arviointi on paljon helpompaa kuin riskin vaikutuksen arvioiminen henkilöiden oikeuksiin ja vapauksiin. Tämän prosessin osalta on kuitenkin ensiksi tunnistettava mahdolliset haitalliset vaikutukset, jonka jälkeen tapauskohtaisesti voisi arvioida vakavuutta. Käytännössä esimerkiksi tason 1 vähäinen vaikutus vastaa hetkellistä päänsärkyä tai ajanhukkaa, tason 3 merkittäviä vaikutuksia voisi

[705] Christofi, Dewitte, Ducuing & Valcke 2020: 152–153, 158–159.
[706] Ks. kuvio 7: Riskien arvioinnin kolme vaihetta.

aiheuttaa perusoikeuksien heikkeneminen, mainehaitta ja taloudelliset tappiot ja viimeisemmän tason kriittinen vaikutus aiheutuisi erittäin vakavista tai jopa lopullisista vaikutuksista, kuten kuolemasta tai pitkäaikaisesta henkisestä kuormituksesta, velkaantumisesta sekä mainehaitasta johtuvasta perhe- tai ystävyyssiteiden katkeamisesta[707]. Joka tapauksessa henkilötietojen käsittelyyn liittyvä vaikutuksen arviointi rekisteröidyn näkökulmasta poikkeaa suurestikin organisaation tyypillisestä riskien vaikutuksien arvioinnista, jolloin kriteereiksi usein asetetaan numeraalisia arvoja tulojen tai asiakkaiden menetykselle, mainehaitan laajuudelle sekä toiminnan keskeytykselle.

Yhteenvetona voidaan todeta, että henkilötietojen käsittelyyn liittyvien tietoturvatoimenpiteiden taustalla tulisi aina olla riskiperustainen arviointi. Rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyviä riskejä aina ennen käsittelytoimien aloittamista. Mikäli henkilötietojen käsittely todennäköisesti aiheuttaisi luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin tai niin sanotut esikriteerit täyttyvät, tulee tehdä tietosuojan vaikutustenarviointi eli DPIA. Täten kaikissa tapauksissa DPIA:a ei ole tarvetta tehdä, jolloin kuitenkin tulee tehdä perusmuotoinen riskiarvio. Tietosuojariskejä arvioidaan aina luonnollisten henkilöiden oikeuksien ja vapauksien kannalta, mikä eroaa muusta organisaation tekemästä riskienarvioinnista: organisaation riskienhallinnan fokuksessa on muun muassa organisaation maine, tulot, jatkuvuus ja asiakastyytyväisyys. Tietosuojariskien hallinta puolestaan keskittyy rekisteröityjen oikeuksien ja vapauksien suojaamiseen organisaation tekemässä henkilötietojen käsittelyssä. Näin ollen tietosuojariskien arviointi on käytännön työssä haastavaa, koska lähes kaikki metodologiat ja hyvät käytänteet keskittyvät organisaationäkökulmaan. Esimerkiksi riskienarvioinnissa numeraalisten arvojen antaminen aineettomiin, *”oikeusiin ja vapauksiin”* kohdistuviin mahdollisiin haittoihin on nähty ongelmalliseksi, mutta se myös ketteröittää tietosuojariskien kriittisyyden tunnistamista, niiden priorisointia ja niihin reagoimista. Standardit sisältävät hyviä esimerkkejä käytännön tietoturvatoimenpiteistä teknologianeutraalin lainsäädännön rinnalla, minkä vuoksi standardeja on myös hyvä hyödyntää esimerkiksi osana tietosuoja-asetuksen riskienhallintavelvoitteiden toteennäyttämistä. Hyvien käytänteiden huomioiminen osana tietoturvan sääntelyjärjestelmää tehostaa myös yksilöiden perusoikeuksien toteutumista. Toinen keskeinen eroavaisuus esimerkiksi tietosuoja- ja tietoturvariskien arviointien osalta on se, että tietosuojariskiarviointi tulisi olla käsittelytoimikohtaista. Tietoturvariskien arvioinnit kohdistuvat usein yksittäisiin järjestelmiin, prosesseihin tai organisaation kokonaisturvallisuuteen, jolloin

[707] CNIL 2018: 4–5; Tietosuojavaltuutetun toimisto 2021b: 32–34.

yksittäisiä käsittelytoimia voi olla haastava erottaa näistä.[708] Eroavaisuuksista huolimatta tietosuoja-asetuksen riskienhallinnan vaatimukset ja riskilähtöisyys ovat kehittäneet organisaatioiden tietoturvatasoa sekä dokumentaatiota.

3.3.4 Tietoturvaloukkauksien ja tietoturvapoikkeamien ilmoittaminen

Tietoturvaloukkauksien määrä sekä tekotapojen monimuotoisuus ovat lisääntyneet teknologian kehittymisen myötä, jolloin organisaatioille on tullut entistä haastavammaksi pitää yllä hyvää imagoa sekä säilyttää asiakkaidensa luottamus. Tietosuojariskien arviointia koskevan velvollisuuden lisäksi tietosuoja-asetuksen riskilähtöisyys tulee myös ilmi osana henkilötietojen tietoturvaloukkauksien dokumentointivelvoitetta ja ilmoitusvelvollisuutta, joita ei ennen tietosuoja-asetusta edellytetty organisaatioilta lainsäädännössä. Tietosuoja-asetuksen 33 artiklan mukaan rekisterinpitäjäorganisaation on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja korjaustoimenpiteet. Tämä on hyvinkin konkreettinen esimerkki tietosuoja-asetuksen asettamasta tietoturvaa parantavasta vaatimuksesta, joka kohdistuu organisaatioiden toimintaan muun muassa kehittämällä turvallisuuspoikkeamien hallintaan liittyviä menettelytapoja. Tietoturvaloukkausten dokumentointi edesauttaa myös niistä oppimista[709].

Henkilötietojen tietoturvaloukkaukset voivat kohdistua tietojen luottamuksellisuuteen, eheyteen tai käytettävyyteen. Käytännössä henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, luovutetaan luvattomaksi tai niihin pääse käsiksi taho, jolla ei ole käsittelyoikeutta. Tällaisia tapahtumia voivat olla esimerkiksi kyberhyökkäys, haittaohjelmatartunta, hakkerointi, varastettu tietokone, hävinnyt tiedonsiirtoväline, tulipalo datakeskuksessa taikka tiliotteen postitus väärälle henkilölle. Käytettävyyden osalta huomioitava on, että mikäli henkilötiedot eivät ole käytettävissä esimerkiksi suunnitellun järjestelmähuollon vuoksi, kyseessä ei ole tietoturvaloukkaus. Suunnittelematon käytettävyyden väliaikainen häviäminen sen sijaan saatetaan katsoa tapauskohtaisesti tietoturvaloukkaukseksi riippuen siitä, onko tietoihin pääsyn häviämisellä merkittäviä seurauksia luonnollisen henkilön oikeuksille ja vapauksille.[710]

---

[708] Ks. lisää organisaation tietoturva- ja tietosuojariskienhallinnasta luvusta 4.2 (” Riskienhallinnan systematiikkaa ja hyvät käytännöt”) ja 4.3 (”Sääntelyjärjestelmän verkko- ja tietojärjestelmien tietoturvariskien hallinta”).
[709] Ks. luku 3.3.1 (”Sääntelyjärjestelmän dokumentaatiovaatimukset”).
[710] Euroopan WP29-tietosuojatyöryhmä WP250: Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, s. 8–9; Tietosuojavaltuutetun toimisto 2019d.

Sama koskee tiedon eheyttä. Jos on huomattu, että esimerkiksi yhden henkilön nimitieto on virheellisesti kirjoitettu, mutta asia on huomattu ajoissa, korjattu ja virheellisestä henkilötiedosta ei ole aiheutunut vaikutuksia luonnollisen henkilön oikeuksille ja vapauksille, ei voida katsoa henkilötietojen tietoturvaloukkauksen tapahtuneen. Kyseessä on kuitenkin tietosuojapoikkeama. Sen sijaan, jos esimerkiksi laskutusdatassa on väärä nimitieto ja lasku ei ole löytänyt perille oikealla henkilölle oikeaan aikaan ja lasku on mennyt perintään, tällöin on kyseessä henkilötietojen tietoturvaloukkaus. Käytettävyyden ja eheyden ulottuvuuksien osalta henkilötietojen tietoturvaloukkauksia arvioitaessa tulee kiinnittää erityishuomiota tapahtuman vaikutuksiin rekisteröidyn kannalta. Sen sijaan luottamuksellisuuden loukkaukset ovat aina henkilötietojen tietoturvaloukkauksia. Olosuhteista riippuen, henkilötietojen tietoturvaloukkaus voi koskea henkilötiedon luottamuksellisuutta, eheyttä ja käytettävyyttä myös yhtäaikaisesti[711].

Myös rekisterinpitäjän ilmoitusvelvollisuutta arvioitaessa kiinnitetään huomiota luonnollisten henkilöiden oikeuksiin ja vapauksiin: onko todennäköistä, että henkilötietojen tietoturvaloukkauksesta aiheutuu riski luonnollisten henkilöiden oikeuksille ja vapauksille?[712] Riskiä ja sen tasoa arvioitaessa on suositeltavaa ottaa huomioon muun muassa tietoturvaloukkauksen tyyppi, henkilötietojen arkaluonteisuus ja määrä, henkilöiden tunnistamisen helppous, henkilöille aiheutuvien seurausten vakavuus, henkilön erityiset ominaisuudet (lapset, vanhukset ym.) sekä rekisterinpitäjän ominaisuudet (esimerkiksi sairaala versus sanomalehden postituslista)[713]. Rekisteröidyn oikeuksilla ja vapauksilla tarkoitetaan esimerkiksi oikeutta yksityisyyteen ja tietosuojaan, mutta myös muita perusoikeuksia, kuten sananvapautta, liikkumisvapautta, ajatuksenvapautta, syrjintäkieltoa, oikeutta vapauteen sekä omatunnon ja uskonnon vapautta[714]. Rekisteröidyn oikeuksia voivat olla myös perusoikeuksien lisäksi tietosuojaoikeudet[715], kuten esimerkiksi oikeus saada pääsy tietoihin tai rajoittaa tietojen käsittelyä.

---

[711] Euroopan tietosuojaneuvoston (EDPB) ohje 9/2022, s. 8.
[712] Tietosuoja-asetuksen 33 artikla, kohta 1.
Tietoturvaloukkauksien ilmoittamisvelvollisuuden kynnys ei rajoitu ainoastaan tilanteisiin, joissa suuri määrä arkaluontoisia tietoja on joutunut ulkopuolisten saataville. Säädös koskee myös arkisia tilanteita työpaikoilla, joissa esimerkiksi joku asiaton on päässyt näkemään työntekijöiden tietoja. Tietoturvaloukkauksilla tarkoitetaan myös vain yhteen henkilöön kohdistuvia loukkauksia. Ks. Nyyssölä 2018, s. 265.
[713] Euroopan WP29-tietosuojatyöryhmä WP250: Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, s. 24–28.
[714] Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 7.; Euroopan WP29-tietosuojatyöryhmä WP218: *Statement on the role of a risk-based approach in data protection legal frameworks*, s. 4.
[715] Erityisesti tietosuoja-asetuksen artiklat 15–22.

Mikäli riskiä luonnollisen henkilön oikeuksille ja vapauksille ei katsota todennäköiseksi henkilötietojen tietoturvaloukkauksen yhteydessä, ei organisaatiolla ole velvollisuutta ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle tai rekisteröidylle. Esimerkiksi tyypillisiä henkilötietojen tietoturvaloukkauksia, joista ei todennäköisesti aiheudu riskiä henkilön oikeuksille ja vapauksille, ovat organisaation työntekijöiden tunnusvuodot, joista ei ole aiheutunut varsinaista tietomurtoa. Tällöin tunnusten hyödyntämisen ja siten tietomurron on estänyt esimerkiksi monivaiheinen tunnistautuminen eli MFA[716] tai organisaation reagointi on muuten ollut nopeaa, ja lokeissa ei ole evidenssiä tunnusten hyödyntämisestä. Tällaisista henkilötietojen tietoturvaloukkauksista on tullut kovin arkipäiväisiä nykyisten, hyvin toteutettujen kalastelukampanjoiden seurauksena.

> Työntekijä erehtyy klikkaamaan kalastelusähköpostin sisältöä ja esimerkiksi linkin kautta avautuneella huijaussivustolla harhautuu syöttämään käyttäjätunnuksensa ja salasanansa huijarille. Käyttäjätunnus ja salasana ovat henkilöön yhdistettävissä olevaa henkilötietoa. Tällöin kyseessä on henkilötietojen tietoturvaloukkaus, kun kyseiset tiedot päätyvät kalastelusivun kautta sellaisen henkilön haltuun, jolle ne eivät kuulu. Mikäli organisaatiossa ehditään kuitenkin tietoturvavalvonnan kautta reagoimaan tähän loukkaukseen tarpeeksi nopeasti eli esimerkiksi lukitsemaan käyttäjän tunnukset ja resetoimaan salasana, rikollinen ei välttämättä ehdi hyödyntämään tunnuksia. Näin ollen tietomurtoa ei tapahdu ja riskiä työntekijän (tai muiden henkilöiden) oikeuksille ja vapauksille ei synny.

Huomioitava kuitenkin on, että henkilötietojen käsittelijöinä toimivien organisaatioiden, on ilmoitettava kaikista henkilötietojen tietoturvaloukkauksista rekisterinpitäjälle, jotta rekisterinpitäjä voi täyttää dokumentointi- ja riskienarviointivelvoitteensa tietosuojalainsäädännön määrittelemällä tavalla. Tietoturvapoikkeamien menettelytavat tulee näin ollen ulottaa myös organisaation toimitusketjuihin[717].

Mikäli kyseessä on rekisterinpitäjä ja ilmoitusvelvollisuutta ei synny, rekisterinpitäjän tulee kuitenkin sisällyttää osaksi henkilötietojen tietoturvaloukkausten dokumentointia riskiarvio luonnollisen henkilön näkökulmasta ja perustelu, miksi

---

[716] MFA eli *Multi-factor Authentication*. Ks. lisää luvusta 4.4.3 (”Pääsynhallintavaatimukset tietoturvan sääntelyjärjestelmässä”).

[717] Turvatoimenpiteiden ja riskinhallinnan tulisi kattaa koko toimitusketju. Asianmukaiset sopimukset (ml. NDA:t eli salassapitosopimukset) ja ohjeet koko toimitusketjun tietoturvapoikkeamien raportointiin voivat olla arvokkaita organisaatiolle, koska ne voivat paljastaa prosessien puutteet ja tarjota mahdollisuuden parantaa toimintaa ja estää vastaavia tapauksia tulevaisuudessa. Esimerkiksi ulkoistetut työntekijät tulisi ohjeistaa ilmoittamaan tietoturvapoikkeamista sovitun prosessin mukaisesti. Ks. Haukilehto 2024, s. 168–169.

valvontaviranomaiselle ei ole päädytty tekemään ilmoitusta[718]. Tämä menettely auttaa rekisterinpitäjää toteuttamaan osoitusvelvollisuuttaan, sillä tietoturvaloukkausten mahdollisten vaikutusten vakavuuden arviointi on rekisterinpitäjän velvollisuus[719]. Usein organisaatioiden tiketöintijärjestelmissä, joissa käsitellään tietoturvapoikkeamia, pystyy hyvin kirjaamaan erilaisia tietoturvaloukkaukseen liittyviä toimenpiteitä ja arviointeja. Valitettavasti käytännön työssä tietosuoja-asetuksen mukaista dokumentointia sinne ei välttämättä tehdä esimerkiksi siitä, mikä on riski rekisteröityjen kannalta ja miksi valvontaviranomaiselle ei ole mahdollisesti päädytty tekemään ilmoitusta. Tämä saattaa johtua tietosuoja-asiantuntemuksen puutteesta tai tietoturvapoikkeamien käsittelyprosessien eriyttämisestä.

Velvollisuus ilmoittaa valvontaviranomaisena toimivalle tietosuojavaltuutetulle (TSV) syntyy, mikäli pelkästään todennäköisyys luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvalle riskille on olemassa. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava mahdollisuuksien mukaan ja ilman aiheetonta viivästystä 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta. Ilmitulo voidaan katsoa tulleen ilmi, kun rekisterinpitäjällä on kohtuullinen varmuus siitä, että on tapahtunut tietoturvapoikkeama, joka on johtanut henkilötietojen vaarantumiseen[720]. Ilmoitus voi olla myös niin sanottu alustava ilmoitus, jolloin myöhemmin lähetetään sitä täydentävä ilmoitus, kun henkilötietojen tietoturvaloukkaukseen liittyvät epäselvät seikat ovat selvinneet. Jos minkäänlaista ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava selvitys tietosuojavaltuutetulle.[721] 72 tunnin aikamääreeseen kuuluu sekä työ- että pyhäpäivät[722]. Henkilötietojen käsittelijällä on puolestaan velvollisuus ilmoittaa ilman aiheetonta viivästystä tietoturvaloukkauksesta rekisterinpitäjälle heti saatuaan tiedon loukkauksesta. Henkilötietojen käsittelijä voi myös sovittaessa ilmoittaa tietoturvaloukkauksesta suoraan tietosuojavaltuutetulle, mutta lopullinen vastuu ilmoituksen tekemisestä on kuitenkin rekisterinpitäjällä.[723]

Velvollisuus ilmoittaa rekisteröidylle syntyy vasta, kun todennäköisyys luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvalle *korkealle* riskille on olemassa sekä mikäli tietyt asetuksessa määritellyt poikkeukset (ks. alla) eivät täyty.[724] Korkea riski henkilön oikeuksille ja vapauksille on olemassa, jos tietoturvaloukkaus voi aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja henkilöille, joiden tietosuojaa on loukattu. Esimerkiksi syrjintä, identiteettivarkaus tai petos,

[718] Euroopan tietosuojaneuvoston (EDPB) ohje 9/2022, s. 26–27.
[719] Tietosuojavaltuutetun toimisto 2019d.
[720] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 385.
[721] Tietosuojavaltuutetun toimisto 2019d.
[722] Nyyssölä 2018: 266.
[723] Tietosuojavaltuutetun toimisto 2019d.
[724] Andersson 2018: 6–7.

taloudelliset menetykset ja maineen vahingoittuminen ovat tällaisia vahinkoja, ja niitä voivat aiheuttaa etenkin erityisten henkilötietojen tietoturvaloukkaus[725]. Tällainen korkea riski luonnollisen henkilön oikeuksiin ja vapauksiin voi myös syntyä esimerkiksi henkilötietojen käyttämisestä petostarkoituksiin tai salassa pidettävien tietojen levitessä laajalle joukolle ihmisiä[726].

Asetuksen 34 artiklan kohta 3 mukaan ilmoitusta rekisteröidylle ei kuitenkaan vaadita, jos jokin seuraavista edellytyksistä täyttyy:

a) rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta;

b) rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että asetuksessa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu;

c) se vaatisi kohtuutonta vaivaa. Tästä esimerkkinä tapaukset, joissa ei tiedetä, keitä rekisteröidyt ovat[727]. Tosin tällaisissa tapauksissa on todennäköisesti käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla.

Täten voidaan todeta, että kynnys ilmoittaa henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle on alhaisempi kuin ilmoittamiskynnys rekisteröidylle[728]. Valvontaviranomainen voi myös vaatia rekisterinpitäjää ilmoittamaan rekisteröidylle henkilötietojen tietoturvaloukkauksesta, jos tämä ei ole sitä tehnyt. Mikäli yksikään edellä mainittujen kohtien a-c asettamista edellytyksistä ei toteudu, rekisterinpitäjä joutuu arvioimaan rekisteröityyn kohdistuvaa ilmoitusvelvollisuutta korkean riskin todennäköisyyden perusteella.

Jos ilmoitus rekisteröidylle kuitenkin tulee tehdä, ilmoitus on tehtävä ilman aiheetonta viivästystä, jotta rekisteröidyllä on mahdollisuus tehdä

[725] Euroopan WP29-tietosuojatyöryhmä WP250: Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, s. 24. Tietoturvaloukkauksen aiheuttamaa korkeaa riskiä arvioitaessa keskitytään eri asioihin kuin DPIA-arvioinnissa, sillä DPIA-arvioinnissa arvioidaan ennemminkin hypoteettista riskiä kuin jo tapahtunutta riskiä tietoturvaloukkauksen yhteydessä.
[726] Voutilainen 2019: 205.
[727] Tietosuojavaltuutetun toimisto 2019d.
[728] Andersson 2018: 6–7.

suojaustoimenpiteitä[729]. Ilmoitukseen pätee tietosuoja-asetuksen 5 ja 12 artiklojen läpinäkyvyyden periaate, jonka mukaan henkilötietojen käsittelyyn liittyvien tietojen ja informoinnin on oltava helposti saatavilla ja ymmärrettävissä sekä lisäksi informointiin on käytettävä selkeää ja yksinkertaista kieltä[730]. Ilmoituksessa on myös kuvattava tietoturvaloukkauksen luonne, seuraukset, organisaation tietosuojavastaavan yhteystiedot lisätietoja varten sekä tietoturvaloukkauksen aiheuttamat toimenpiteet ja tarvittaessa toimenpiteet haittavaikutuksien pienentämiseksi.

Julkista tiedonantoa käytetään, mikäli 34 artiklan mukaisesti rekisteröidyille henkilökohtaisesti ilmoittaminen vaatisi kohtuutonta vaivaa eikä henkilökohtaista ilmoitusta tällöin tehdä. Esimerkiksi **tietosuojavaltuutetun päätöksessä 3.1.2020 (dnro. 60/171/2020)** rekisterinpitäjällä ei ollut riittäviä yhteystietoja käytössään rekisteröidyille ilmoittamista varten:

> *Tietosuojavaltuutettu oli määrännyt rekisterinpitäjän ilmoittamaan tietoturvaloukkauksesta rekisteröidyille. Rekisterinpitäjä oli toimittanut kirjeitse tietosuoja-asetuksen mukaiset ilmoitukset suoraan noin 10 000:lle rekisteröidyille, joiden osalta rekisterinpitäjällä oli ollut riittävät yhteystiedot. Sen sijaan noin 7 000:n rekisteröidyn osalta rekisterinpitäjällä ei ollut riittäviä yhteystietoja ja rekisterinpitäjän mukaan niiden selvittäminen olisi vaatinut kohtuutonta vaivaa, minkä vuoksi rekisterinpitäjä päätyi julkiseen tiedonantoon verkkosivuillaan ja Facebook-sivuillaan. Apulaistietosuojavaltuutettu katsoi tiedonannon olevan pääosin tietosuoja-asetuksen mukainen. Tiedonanto kuitenkin sisälsi kohdan ”asianomaisille on lähetetty tilanteesta lisätietoa henkilökohtaisesti”, vaikka 7 000 rekisteröityä eivät olleet saaneet henkilökohtaista ilmoitusta. Näin ollen apulaistietosuojavaltuutettu antoi rekisterinpitäjälle huomautuksen, koska tämä katsottiin rikkovan muun muassa rekisteröidyn läpinäkyvän informoinnin vaatimusta.*

Näin ollen myös julkisessa tiedonannossa on yhtä lailla noudatettava tietosuoja-asetuksen vaatimuksia ilmoituksen sisältö- ja laatuvaatimuksista. Edellä olevassa tapauksessa 7000 rekisteröityä eivät saaneet henkilökohtaista lisätietoa tapahtuneesta, vaikkakin julkisessa tiedoksiannossa näin ilmaistiin. Tästä syystä he saattoivat virheellisesti saada sellaisen käsitykseen, ettei tietoturvaloukkaus koskenut heitä. Täten tietosuojavaltuutetun päätöksestä voidaan päätellä, että tiedottaminen ei ole tietosuoja-asetuksen 12 artiklan mukaisesti helposti ymmärrettävää, mikäli siitä voi saada virheellisen käsityksen. Läpinäkyvyyden periaatteen mukaisesti

[729] Tietosuojavaltuutetun toimisto 2019d.
[730] Voutilainen 2019: 130.

tietojen ja informoinnin tulisi myös olla helposti saatavilla. Tietosuojavaltuutetun päätöksen mukaan ilmeisesti tiedottaminen yrityksen kotisivuilla ja sosiaalisessa mediassa on tarpeeksi julkista ja siten helposti saatavilla. Päätöksessä ei kuitenkaan ole varsinaisesti otettu kantaa siihen, että kaikki rekisteröidyt eivät välttämättä ole sosiaalisessa mediassa, saati sitten käy säännöllisesti yrityksen kotisivuilla. Ilmoitus tulee lähettää siten, että se mahdollisimman tehokkaasti saavuttaa kaikki tietoturvaloukkauksen piirissä olevat ihmiset, mikä saattaa myös edellyttää useampien viestintävälineiden käyttämistä[731]. Päätöksessä olisi pitänyt ottaa huomioon myös mahdollinen tiedonantovelvoite printtimediassa.

Tietoturvaloukkaus on yksi turvapoikkeamien tyyppi. Kuitenkin kaikki turvapoikkeamat eivät välttämättä ole henkilötietojen tietoturvaloukkauksia, vaikkakin kaikki henkilötietojen tietoturvaloukkaukset ovat puolestaan turvapoikkeamia. Turvapoikkeamat voivat olla sekä hyökkäyksiä ulkoisesta lähteestä että turvallisuusperiaatteiden vastaisesta sisäisestä tietojenkäsittelystä aiheutuvia vaaratilanteita.[732] Henkilötietojen tietoturvaloukkaus koostuu henkilötietojen käsittelystä, joka on aiheutunut vahingossa tai lainvastaisella menettelyllä. Näin ollen mikä tahansa tietoturvaloukkaus ei ole välttämättä juuri tietosuoja-asetuksessa tarkoitettu tietoturvaloukkaus.[733] Muita tietoturvaloukkauksia voivat olla muun muassa sellaiset organisaation ei-henkilötietoja sisältävien tietojen luottamuksellisuutta, eheyttä tai saatavuutta vaarantavat tapahtumat. Tällaisia voivat olla esimerkiksi liikesalaisuuksia sisältävän USB-tikun häviäminen. Reagointi itsessään tällaisiin muihin tietoturvaloukkauksiin voi olla jo prosessina erilainen kuin reagointi varsinaisiin henkilötietojen tietoturvaloukkauksiin, jotka vaativat lain määräysten takia tietynlaiset toimintatavat.

Hyvien tietoturvallisten käytänteiden mukaisesti turvallisuuspoikkeamien käsittelyyn ja hallintaan on oltava menettelytavat. Tämä edellyttää näin ollen myös sitä, että poikkeamien hallinta olisi vastuutettu, dokumentoitu, koulutettu ja harjoiteltu.[734] Edistystä on, että turvallisuuspoikkeamien käsittelystä on säädetty laissa. Tietosuoja-asetuksen myötä turvallisuuspoikkeamien käsittely, hallinta ja dokumentointi ovat kehittyneet myös tietoturvan osa-alueella. Tietosuoja-asetus ei ota

---

731 Korpisaari, Pitkänen & Warma-Lehtinen 2022: 396; Euroopan WP29-tietosuojatyöryhmä WP250: Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, s. 22–23.
732 Euroopan WP29-tietosuojatyöryhmä WP250: Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, s. 7–8.
733 Voutilainen 2019: 203.
734 Katakri 2020 T07 -vaatimuksen mukaan organisaatiolla tulisi olla menettelytavat tietoturvallisuuspoikkeamien käsittelyyn sekä yhteyshenkilöt, joille ilmoitetaan turvallisuuspoikkeamista. Tämä yleensä edellyttää vastuiden määrittelyä, dokumentoitua ohjeistusta, menettelytapojen koulutusta ja harjoittelua, jotka ulottuvat osittain hallinnollisen tietoturvallisuuden vastuualueelle.

kantaa suoranaisesti, minkälaista tekniikkaa tulisi käyttää tietoturvapoikkeamien hallintaan[735]. Tietosuoja-asetus ei myöskään ota kantaa poikkeamatilanteiden kouluttamiseen ja harjoitteluun, mikä ei täysin vastaa hyviä tietoturvakäytänteitä. Poikkeamatilanteiden kouluttaminen ja harjoittelu lisäävät tietoisuutta ja reaktiokykyä poikkeamien varalta, minkä takia tämä on olennainen osa alue turvallisuuspoikkeamien hallinnassa. Tämä korostaa myös poikkeamien asianmukaista dokumentointia ja analysointia, jotta poikkeamien juurisyyt (*"root cause analysis"*) olisi helpommin tunnistettavista sekä poikkeamista oppiminen ja toiminnan parantaminen (*"lessons learned"*) olisi mahdollista.

Tietoturvapoikkeamien ilmoitusvelvollisuudet saattavat olla osittain rinnakkaisia, jolloin organisaatio joutuu tekemään ilmoituksen tietoturvaloukkauksesta useammalle taholle. Esimerkiksi sähköisen viestinnän palveluista annetun lain (917/2014) 275 §:ssä on säädetty teleyrityksen tietoturvapoikkeamien ilmoittamisvelvollisuudesta sekä verkossa toimivan markkinapaikan tarjoajan, hakukonepalvelun tarjoajan sekä pilvipalvelun tarjoajan tietoturvahäiriöiden ilmoittamisvelvollisuudesta. Tähän tulee muutoksia NIS 2 -direktiivin myötä, kun direktiivi implementoidaan kansallisesti kyberturvallisuuslailla[736]. Toisena esimerkkinä toimii sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (703/2023) 90 §, jossa on säädetty tietoturvallisuuteen liittyvien poikkeamien ilmoittamisvelvollisuudesta.

NIS 2 -direktiivin myötä on myös laajemmin säädetty tietoturvapoikkeamien ilmoitusvelvollisuudesta CSIRT-yksiköille, toimivaltaisille viranomaisille tai keskitetyille yhteyspisteille[737]. Ilmoittamisessa korostuu porrastettu lähestymistapa, jotta pystyttäisiin rajaamaan merkittävien poikkeamien leviämistä sekä nopeuttamaan ilmoittamista ja madaltaa kynnystä pyytää apua. Kun keskeinen tai tärkeä toimija tulee tietoiseksi merkittävästä poikkeamasta, sillä on velvollisuus antaa ennakkovaroitus ilman aiheetonta viivästystä tai viimeistään 24 tunnin kuluessa. Tämän jälkeen tulee tehdä varsinainen poikkeamailmoitus ilman aiheetonta viivästystä tai viimeistän 72 tunnin kuluessa siitä, kun toimija on tullut tietoiseksi *merkittävästä poikkeamasta*. Viimeinen vaihe on loppuraportin toimittaminen viimeistään kuukauden kuluttua poikkeamailmoituksesta. NIS 2 -direktiivin ilmoitusvelvollisuudet koskevat nimenomaan merkittäviä poikkeamia, joka on aiheuttanut tai voi aiheuttaa vakavan toimintahäiriön palveluille, taloudellista tappiota

[735] Akatyev, Han, Hwang, Jang, Kim D., Kim J., Park, Shin, & Yu 2018: 97.
[736] HE 57/2024 (s. 38) mukaan sähköisen viestinnän palveluista annetun lain 247 a § ja 275 §:n 2 momentti kumotaan digitaalisen palvelun tarjoajien osalta NIS 2 -direktiivin toimeenpanon johdosta päällekkäisen sääntelyn välttämiseksi.
[737] Myös DORA-säädöksessä (EU 2022/2554/EU, asetus finanssialan digitaalisesta häiriönsietokyvystä) on säädetty tieto- ja viestintätekniikan (TVT) poikkeamien hallinnasta ja etenkin tällaisten laajavaikutteisten poikkeamien raportoinnista NIS 2 -direktiivin mukaiselle CSIRT-yksiköille, toimivaltaisille viranomaisille tai keskitetyille yhteyspisteille.

asianomaiselle toimijalle taikka se vaikuttaa tai voi vaikuttaa luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.[738] NIS 2 -direktiivissä on myös todettu, että poikkeamat vaarantavat monissa tapauksissa henkilötietojen suojan, jolloin toimivaltaisten viranomaisten olisi tehtävä yhteistyötä[739]. Näin ollen vuorovaikutuskohtia saattaa syntyä sekä tietosuoja-asetuksen että muiden tietoturvapoikkeamista sääntelevän lainsäädännön välillä, jolloin on suositeltu pidettävän organisaation menettelyt erillään säädöksien painoalojen mukaisesti ja tehdä poikkeamailmoitukset erikseen kunkin säädöksen vaatimusten mukaisesti toimivaltaiselle viranomaiselle[740]. Suotavaa olisi kuitenkin se, että tietosuoja- ja tietoturvayksiköt tekevät yhteistyötä ja heillä on keskenään sovittu, dokumentoitu ja harjoiteltu toimintapa poikkeamienhallinnalle, vaikka kukin taho lähettäisi poikkeamailmoituksia eri viranomaisille.

NIS 2 -direktiivin toimeenpano kyberturvallisuuslailla tulee kasvattamaan organisaatioiden tietoturvapoikkeamien ilmoitusten määrää, jolloin on syytä tarkastella prosessien toimivuutta sekä voisiko raportointia yhtenäistää organisaation sisällä tietosuojan raportointivelvoitteiden kanssa. Huomioitava on myös se, että tietoturvapoikkeamien ilmoittamisvelvollisuudet poikkeavat suuresti toisistaan, vaikka aikarajoissa onkin yhtäläisyyksiä. Esimerkiksi tietosuojavaltuutetulle tulee ilmoittaa henkilötietojen tietoturvaloukkauksesta, mikäli *riski henkilön oikeuksille ja vapauksille on pelkästään olemassa*. Sen sijaan NIS 2 -direktiivin mukainen turvapoikkeamailmoitus tulee tehdä valvontaviranomaisille vasta merkittävän poikkeaman kohdalla, joka aiheuttaa tai voi aiheuttaa *huomattavaa aineellista tai aineetonta vahinkoa* vaikutuksillaan luonnollisiin henkilöihin. Näin ollen myös NIS 2 -direktiivin mukaisten tietoturvapoikkeamien arvioinnissa tulee huomioida vaikutukset luonnollisiin henkilöihin, mutta tällöin arviointi kohdistuu oikeuksien ja vapauksien sijaan aineellisiin ja aineettomiin vahinkoihin.

---

[738] Ks. lisää NIS 2 -direktiivin kohta 101–102 ja 23 artikla. CER-direktiivissä poikkeamien ilmoitusvastuu on samankaltainen: 33 kohdan ja 15 artiklan mukaisesti kriittisten toimijoiden on lähetettävä ensimmäinen ilmoitus 24 tunnin kuluessa poikkeaman havaitsemisessa ja yksityiskohtainen raportti tarvittaessa viimeistään kuukauden kuluttua tästä. Näin ollen ilmoittamisvelvollisuudesta puuttuu 72 tunnin väli-ilmoitus. NIS 2 -direktiivin ja CER-direktiivin erona on myös poikkeamien ilmoittamisvelvollisuuden osalta se, että NIS 2 -direktiivissä korostetaan poikkeaman merkityksellisyyttä. Molemmissa direktiiveissä tosin poikkeama on määritelty hieman eri tavoin: NIS 2 -direktiivi rajaa näkökulmaltaan poikkeamat verkko- ja tietojärjestelmien tietoturvapoikkeamiin, kun taas CER-direktiivin poikkeamat ovat kaikenlaisia tapahtumia, jotka voivat merkittävästi häiritä tai häiritsevät keskeisen palvelun tarjoamista.

[739] NIS 2 -direktiivin kohta 108.

[740] Ks. Hert, Markopoulou & Papakonstantinou 2019: 10.

Erityisesti *huomattavan aineettoman vahingon* määrittäminen luonnollisen henkilön[741] osalta voi olla vaikeaa. Esimerkiksi **EUT 25.1.2024 C-687/21 MediaMarktSaturn ratkaisun kohdassa 86,** rekisteröidyn pelko siitä, että kolmannet osapuolet käyttävät väärin hänen vuotaneita henkilötietojaan, katsottiin voivan olevan aineetonta vahinkoa.

> Vahingonkorvauslaissa (412/1974) aineettomia henkilövahinkoja ovat kipu, särky sekä muu tilapäiväinen tai pysyvä haitta. Aineetonta henkilövahinkoa voi olla myös psyykkisen tilan häiriintyminen. Psyykkisen henkilövahingon, esimerkiksi järkytystilan tai masennuksen, korvattavuuden edellytyksenä on lääketieteellisin keinoin toteennäyttäminen, jolloin todistamisvelvollisuus tekee asiasta monimutkaisemman. Tällaisen psyykkisen henkilövahingon ilmentymä voi olla vahinkotapahtumasta aiheutunut posttraumaattinen stressireaktio tai pelkotila, joka alkaa hallita ihmisen käyttäytymistä.[742]

> Kärsimys on myös katsottava aineettomaksi vahingoksi. Siinä missä henkilövahingoissa epäedullinen muutos ilmenee henkilön terveydentilassa, kärsimyksessä on kyse negatiivisesta muutoksesta henkilön tunnetilassa. Tällaisia negatiivisia tunnetiloja voivat olla esimerkiksi suru, pelko ja nöyryytys. Tällöin kärsimys ei edellytä aikaisemmin mainittua psyykkisen tilan häiriintymistä: kärsimystä voi kokea ilman, että henkilövahingon kynnys ylittyy tai henkilön terveydentilassa tapahtuu muutoksia. Lisäksi lääketieteellisesti todettavaa muutosta ei tarvita. Kärsimyskorvaus perustuu siihen, että henkilölle loukkauksesta aiheutuva negatiivinen tunnetila on hyvitettävä. On kuitenkin todettu, että kaikki negatiiviset tunnereaktiot eivät ole korvattavia, kuten esimerkiksi elämään normaalisti kuuluvat epämiellyttävät tunnetilat.[743] Kärsimyskorvauksesta on säädetty vahingonkorvauslain 5 luvun 6 §:ssä, jonka mukaan kärsimyksestä voi saada korvausta se, jonka rauhaa tai yksityiselämää on rangaistavaksi säädetyllä teolla loukattu. Yksityiselämää loukkaavan tiedon levittäminen (RL 24 luku 8 §) voi olla tällainen rangaistavaksi säädetty teko yksityiselämän loukkaamisen osalta[744]. Esimerkiksi Vastaamon tapauksessa rikoksen tekijän katsottiin

---

[741] NIS 2 -direktiivissä huomioidaan myös aineettomat vahingot oikeushenkilöille. Käytännössä tällaisia ovat esimerkiksi mainehaitat. Huomioitava on, että todennäköisesti huomattava mainehaitta on sellainen, jolla yleensä loppujen lopuksi on aineellisia vaikutuksia, kuten asiakaskadon myötä taloudellinen tappio.

[742] Ståhlberg & Karhu 2020: 338, 341–345. Ks. myös vahingonkorvauslain 5 luvun 2 §.

[743] Ibid: 338, 350–351.

[744] Huomioitava on se, että perusoikeusmyönteisen tulkinnan myötä yksityiselämän käsitettä ei tule ymmärtää suppeammin kuin mitä se ymmärretään perus- ja ihmisoikeutena. Ks. Ståhlberg & Karhu 2020, s. 353.

> aiheuttaneet suurta kärsimystä tai sen vaaraa taikka erityisen suurta vahinkoa tai sen vaaraa asianomistajille levittäessään yksityiselämää loukkaavia tietoja, jotka olivat terveystietoja[745].

Näin ollen aineetonta vahinkoa voivat olla sekä aineettomat henkilövahingot[746], johon liittyy lääketieteellinen toteennäyttäminen, että kärsimys. **MediaMarktSaturn** -ratkaisussa EUT painotti, että aineettoman vahingon käsitettä on tulkittava laajasti ja perustellut pelkotilat lukeutuvat tietosuoja-asetuksen suojelutavoitteiden piiriin[747].

NIS 2 -direktiivissä kuitenkin korostetaan myös *huomattavan aineettoman vahingon mahdollisuutta*, mikä voi olla todella vaikeaa organisaation määritellä luonnollisen henkilön näkökulmasta. Tietoturvapoikkeamatilanteissa on usein kiire eikä käytännön selvitys- ja raportointityössä ole välttämättä aikaa kovin syvällisesti pohtia, voisiko tietoturvapoikkeamasta aiheutua esimerkiksi aineetonta psyykkistä henkilövahinkoa tai kärsimystä sekä onko tämä aineeton vahinko NIS 2 -direktiivin mukaisesti huomattavaa. Aineettomana henkilövahinkona konkreettinen kipu ja särky voivat vastakohtaisesti olla helpommin arvioitavissa toimialakohtaisesti: esimerkiksi kyberhyökkäyksen lamaannuttaessa sairaalan toiminnan tai liikenteen, voi tästä aiheutua aineettomia henkilövahinkoja (kipua ja särkyä), joista voi myös kumuloitua aineellista vahinkoa[748].

Joka tapauksessa organisaatiot tarvitsevat konkreettisia ohjeita, joita soveltaa hektisissä poikkeamatilanteissa huomattavan aineettoman vahingon arvioimiseksi. NIS 2 -direktiivin mukainen ilmoitus olisi tarkoituksen mukaista aina tehdä sellaisista merkittävistä poikkeamista, joista mahdollisesti koituu tai voi koitua vahingonkorvauslain mukaisesti luonnolliselle henkilölle aineetonta henkilövahinkoa tai kärsimystä. Nämä pitäisi katsoa ilmoitusvelvollisuuden piiriin kuuluvaksi *huomattavaksi aineettomaksi vahingoksi*, koska poikkeamailmoituksella on

---

Yksityiselämää loukkaavan tiedon levittämisen osalta informaatio sinällään on totuudenmukaista, mutta sen levittämiseen ei ole oikeutta. Oikeuttamisperuste voi toki syntyä, jos yksityiselämän tieto koskee julkisuuden henkilöä. Ks. Pesonen 2017, s. 207.

745 Ks. Länsi-Uudenmaan käräjäoikeus 30.4.2024 R 23/3965: 4.

746 Henkilövahinkoa ei ole käsitteenä tarkasti määritelty, ja sen täsmentyminen on jätetty oikeuskäytännön varaan. Ks. Ståhlberg & Karhu 2020, s. 341.

747 EUT 25.1.2024, C-687/21 MediaMarktSaturn, ratkaisun kohta 65, 67 ja 69. Perusteltu pelkotila käytännössä tarkoittaa sitä, että kolmannet osapuolet käyttävät väärin rekisteröityä koskevia henkilötietoja, koska näitä tietoja sisältävä asiakirja on annettu oikeudettomalle kolmannelle osapuolelle, jolla on ollut mahdollisuus ottaa kopioita siitä ennen sen palauttamista (kohta 67). Tapauksessa tuli kuitenkin kohdan 69 mukaan ilmi, että kolmas osapuoli ei ollut tutustunut asiakirjaan tai rekisteröidyn tietoihin, joten pelko ei katsottu olevan perusteltua.

748 Tällaiset aineettomat vahingot aiheuttavat usein hoito- ja tutkimuskuluja, sekä mahdollisesti ansiotulojen menetystä, jolloin niistä koituu aineellista vahinkoa.

myös mahdollista ennaltaehkäistä poikkeaman laajuutta ja siten vaikutuksia luonnollisille henkilölle[749].

Luonnollisten henkilöiden osalta on huomioitava NIS 2 -direktiivin ja tietosuoja-asetuksen yhtenevät ilmoitusvelvollisuudet. Esimerkiksi jos organisaation tietomurron yhteydessä *on mahdollista*, että rikollinen levittää asiakkaiden tietoja yksityiselämää loukkaavalla tavalla (RL 24 luku 8 §), tällöin tulee tietosuojalainsäädännön ilmoitusvelvoitteiden lisäksi tehdä NIS 2 -direktiivin mukainen poikkeamailmoitus, sillä tapahtumasta voisi koitua rekisteröidyille kärsimystä tai psyykkistä henkilövahinkoa.

Lopuksi yhteenvetona voidaan todeta, että tietoturvan sääntelyjärjestelmässä turvapoikkeamien arviointi ja ilmoitusvelvollisuudet ovat haastava kokonaisuus. Henkilötietojen tietoturvaloukkaukset vaativat aina rekisterinpitäjän tekemää, dokumentoitua riskien arviointia siitä, minkä tasoinen riski on kyseessä tai onko edes riskiä olemassa henkilöiden oikeuksille ja vapauksille. Henkilötiedon käytettävyyden ja eheyden ulottuvuuksien osalta riskejä ja ilmoittamisvelvollisuutta arvioitaessa tulee kiinnittää erityishuomiota henkilötietojen tietoturvaloukkauksen vaikutuksiin rekisteröidyn kannalta eli aiheutuuko tapahtumasta vaikutuksia rekisteröidy(i)lle. Sen sijaan luottamuksellisuuden loukkaukset ovat aina henkilötietojen tietoturvaloukkauksia. NIS 2 -direktiivin mukaan soveltamisalaan kuuluvien organisaatioiden tulee turvapoikkeamien kohdalla arvioida myös poikkeaman merkittävyyttä muun muassa luonnollisille henkilöille tai oikeushenkilöille koituvien aineellisten ja aineettomien vahinkojen suhteen, mikä poikkeaa tietosuoja-asetuksen rekisteröityjen *oikeudet ja vapaudet* -näkökulmasta. NIS 2 -direktiivin implementoinnin myötä tietoturvapoikkeamien ilmoitusvelvollisuudet ovat edelleen osittain rinnakkaisia, jolloin organisaatio joutuu tekemään ilmoituksen tietoturvaloukkauksesta useammalle taholle. Ilmoittamisvelvollisuuden osalta tulee huomioida eri säädöksissä määritellyt ilmoituksien aikarajat sekä eri viranomaistahot. Vaikka NIS 2 -direktiivin systematiikka eroaa tietosuoja-asetuksesta, käytännössä huomattavat aineelliset ja aineettomat vahingot hyvin todennäköisesti loukkaavat myös henkilöiden oikeuksia ja vapauksia, kuten esimerkiksi perusoikeuksista oikeutta yksityiselämän ja henkilötietojen suojaan sekä luottamukselliseen viestintään. Tämänkaltainen lainsäädännön kehitys kuvastaa myös sitä, kuinka päällekkäistä sääntelyä esiintyy jopa tietoturva- ja tietosuojalainsäädännön osalta. Tämä vaikeuttaa tietoturvan sääntelyjärjestelmän ymmärrettävyyttä sekä tekee siitä helposti epäyhtenäisen. Suurin haaste piilee käytännön jalkauttamisessa – Kuinka

[749] Ennakoiva lähestymistapa kyberuhkiin on ratkaiseva osa kyberturvallisuusriskien hallintaa, jonka avulla toimivaltaisten viranomaisten olisi pystyttävä estämään tehokkaasti kyberuhkien toteutuminen poikkeamina, jotka voivat aiheuttaa huomattavaa aineellista ja aineetonta vahinkoa (Ks. NIS 2 -direktiivin kohta 105). Tätä varten kyberuhkista ilmoittaminen on erittäin tärkeää.

organisaatiossa luodaan toimivaksi prosessiksi lainsäädännön vaatimukset ja noudatetaan tehokkaasti lakia tietoturvapoikkeamien hallinnan osalta?

Lainsäädännössä tietoturvapoikkeamien ja niihin liittyvien henkilötietojen tietoturvaloukkausten dokumentointi ja ilmoittamisvaatimukset ovat kehittyneet ajan myötä paremmiksi. Hyvien käytänteiden mukaisesti organisaatiolla tulisi olla menettelytavat tietoturvallisuuspoikkeamien käsittelyyn, joka edellyttää vastuiden määrittelyä, ohjeistamista, koulutusta ja harjoittelua. Näihin asioihin lainsäädäntö ei ota suoraan kantaa, ja käytännön työssä näissä myös ilmenee haasteita erityisesti suuremmissa organisaatioissa. Usein tietoturvapoikkeamien havaitsemisen, dokumentoinnin ja hallinnan puutteista kritisoidaan organisaatioiden alhaista riskienhallintakulttuuria, huonoa suhtautumista tietoturvaan, taikka työntekijöiden osaamisen puutetta[750]. Nämä havainnot pitävät paikkansa, mutta ne eivät täysin selitä koko ongelmaa. Toinen keskeinen haaste liittyy suuresti asiantuntijoiden kykyyn luoda toimivia prosesseja ja jalkauttaa niitä läpi koko organisaation. Rivityöntekijöiden tärkein tehtävä on osata tunnistaa tietoturvapoikkeamat ja ilmoittaa niistä eteenpäin luodun prosessin mukaisesti. Erityisesti isommissa organisaatioissa tietoturvan ja tietosuojan substanssiasiantuntijoiden tehtävänä tulisi olla ilmoitettujen poikkeamien analysointi, arviointi ja jatkotoimenpiteiden dokumentointi ja *”lesson learned”* -tyyppinen läpikäynti. Rivityöntekijöille tietoturvapoikkeamien ilmoittaminen ei saa olla liian työlästä, koska se heikentää poikkeamista ilmoittamista[751].

3.3.5 Muut tietosuojalainsäädännön tietoturvavaatimukset

Tietoturvaan liittyviä vaatimuksia löytyy paljonkin tietosuojalainsäädännöstä, sillä laki velvoittaa organisaatioita tekemään tietoturvatoimenpiteitä henkilötietojen suojaamiseksi. Edellä on mainittu tietoturvaa parantavina vaatimuksina muun

[750] Esimerkiksi Haukilehdon väitöstutkimuksessa on todettu, että terveydenhuollon poikkeamaraportointijärjestelmä HaiProssa valtaosaa ilmoitetuista tietoturvapoikkeamista ei ole riskien osalta arvioitu tai poikkeamailmoitukset ovat muuten puutteellisesti täytetty (Ks. esim. Haukilehto 2024, s. 128, 130, 133, 136, 140, 143) . Tämä puute on katsottu kytkeytyvän alhaiseen riskienhallintakulttuuriin sekä heijastelevan myös huonoa suhtautumista tietoturvaan terveydenhuollon organisaatioissa (Haukilehto 2024: 160).

[751] Organisaation on varmistettava, että sillä on selkeä ja käytännöllinen prosessi tietoturvapoikkeamien raportointiin. Jos poikkeamien raportointiin käytetään useita järjestelmiä tai prosesseja, niiden käyttö ja tapaukset, joissa niitä käytettäisiin, on suunniteltava ja ohjeistettava huolellisesti. Useiden järjestelmien tai tapojen käyttäminen tietoturvapoikkeamien raportointiin voi olla työntekijöille hämmentävää ja voi olla vaikeaa selvittää, mitä järjestelmää käytetään tai mitä prosessia noudatetaan. Lisäksi poikkeamien ilmoittamiseen käytettävä ohjelmisto voisi ohjata ilmoittajaa ilmoittamaan kaikki tarvittavat tiedot ja tarkistamaan annettujen tietojen oikeellisuuden automaattisesti – puutteellisilla tiedoilla raportoidut poikkeamailmoitukset vaikeuttavat niiden analysointia ja niistä oppimista. Ks. Haukilehto, s. 166–169.

muassa tietosuoja-asetuksen asettamat dokumentaatiovaatimukset, ulkoistuksiin ja hankintoihin liittyvät sopimukset ja niiden sisältämät tietoturvavaatimukset, henkilötietojen käsittelyn riskiarviointi sekä henkilötietojen tietoturvaloukkauksien dokumentointi- ja ilmoitusvelvollisuus. Näiden lisäksi tietosuoja-asetuksessa painotetaan teknisiä ja organisatorisia tietoturvaan liittyviä toimenpiteitä[752].

Esimerkiksi sisäänrakennetun ja oletusarvoisen tietosuojan vaatimuksen (*"Privacy by Design and Default"*, 25 artikla) mukaan rekisterinpitäjä on tietosuojaperiaatteiden täytäntöönpanoa varten toteutettava tehokkaasti teknisiä ja organisatorisia toimenpiteitä, jotta ne saataisiin sisällytettyä käsittelyn osaksi, ja jotta rekisteröidyn oikeuksia suojattaisiin ja käsittely vastaisi tietosuoja-asetuksen vaatimuksia. Tällöin on suhteellisuusperiaatteen mukaisesti otettava huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn aiheuttamat luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit sekä henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Näin ollen sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa tietosuojaperiaatteiden huomioimista jo käsittelytoimintojen suunnitteluvaiheessa[753] sekä tietosuojan toteutumista oletusarvoisesti organisaation toiminnassa, esimerkiksi rajaamalla käyttöoikeuksia. Tämä on jälleen hyvä esimerkki siitä, kuinka tietosuojaperiaatteilla parannetaan organisaation tietoturvaa: myös tietoturvan tulisi toteutua oletusarvoisesti ja riskiperusteisesti organisaation toiminnassa.

Kansallisessa tietosuojalain (1050/2018) 6 §:ssä on säädetty erikseen kaikkia organisaatioita velvoittavana tietoturvatoimenpiteistä, jotka tulee toteuttaa asianmukaisesti käsitellessä poikkeusperustein[754] erityisiä henkilötietoja. Tällaisia asianmukaisia tietoturvatoimenpiteitä erityisten henkilötietojen, kuten terveystietojen, suojaamiseksi ovat muun muassa:

1) Toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty. Tällaisia toimenpiteitä ovat esimerkiksi järjestelmälokitus. Järjestelmässä tulee tosin sanoen olla eräänlainen käyttöloki (puhutaan myös audit-lokista).[755]

---

[752] Teknisiä ja organisatorisia tietoturvatoimenpiteitä on käsitelty yksityiskohtaisemmin luvussa 3.4 (”Tietoturvan sääntelyjärjestelmän erilaiset tietoturvatoimenpiteet”)
[753] Esimerkiksi järjestelmien tai palveluiden suunnittelussa jo projektin tai hankinnan alkuvaiheessa. Ks. luku 4.4 (”Järjestelmien oikeudellisen suunnittelun vaatimukset sääntelyjärjestelmässä”).
[754] Tietosuojalain 6 §:n 1 momentissa on säädetty erityisiä henkilötietoryhmiä koskevasta sallittavasta käsittelystä. Esimerkiksi sallittavaa käsittelyä on mm. tietojen käsittely, josta säädetään laista tai joka on tarpeen rekisterinpitäjän erityisten oikeuksien ja velvoitteiden noudattamiseksi työoikeuden alalla.
[755] Ks. lisää luvusta 4.4.2 (”Järjestelmien lokitusvaatimukset tietoturvan sääntelyjärjestelmässä”).

2) Toimenpiteet, joilla parannetaan henkilötietoja käsittelevän henkilöstön osaamista. Hyvien käytänteiden mukaisesti tällaisia toimenpiteitä olisivat henkilökunnan ohjeistaminen, tietoturva- ja tietosuojakoulutus sekä osaamisen testaus[756].

3) Rekisterinpitäjän ja käsittelijän sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin. Tästä esimerkkinä riittävä ja asianmukainen pääsyn- ja käyttöoikeuksienhallinta[757].

4) Palveluiden ja järjestelmien tietoturvallisuuden ja vikasietoisuuden takaaminen sekä tietojen palauttamisen takaaminen. Palauttamisen takaamista edesauttaa toipumissuunnittelu ja varmuuskopiointi[758].

5) Menettely tietoturvatoimenpiteiden tehokkuuden arvioimiseksi ja testaamiseksi. Tällainen menettely voisi olla esimerkiksi tietosuoja-asioiden tarkastamisen lisääminen osaksi organisaation sisäisen tarkastuksen suunnitelmaa sekä erityistä henkilötietoa sisältävien järjestelmien sisäiset ja ulkoiset tietoturva-arvioinnit[759].

Muita tietosuojalain 6 §:n 2 momentin velvoittavia toimenpiteitä ovat myös esimerkiksi tietosuojavastaavan nimeäminen, pseudonymisointi[760], henkilötietojen salaaminen, menettelysääntöjen luominen henkilötietojen siirtämiseen ja muuhun tarkoitukseen liittyvään käsittelyyn liittyen, DPIA:n laatiminen sekä muut tekniset, menettelylliset ja organisatoriset toimenpiteet.

Kansallisen tietosuojalain 6 §:n 2 momentin tietoturvatoimenpiteet eivät kuitenkaan ole lain esitöiden mukaan pakollisia ja kattavia, vaan rekisterinpitäjän

---

[756] Ks. lisää luvusta 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).
[757] Ks. lisää luvusta 4.4.3 (”Pääsynhallintavaatimukset tietoturvan sääntelyjärjestelmässä”).
[758] Ks. lisää luvusta 4.4.4 (”Varmuuskopioinnin ja toipumisen vaatimukset sääntelyjärjestelmässä”).
[759] Ks. myös luvut 2.7 (”Tietoturvan sääntelyjärjestelmä ja hyvät käytänteet”) sekä 4.4.5 (”Tietoturvan vähimmäisvaatimukset ja tietoturvatason arviointi”).
[760] Pseudonymisointi on henkilötietojen käsittelemistä tavalla, jolloin tietoja ei voida suoraan yhdistää tiettyyn rekisteröityyn käyttämättä muita lisätietoja (Tietosuojavaltuutetun toimisto 2019b). Pseudonymisointi eroaa anonymisoinnista siten, että pseudonymisoidut henkilötiedot on mahdollista palauttaa henkilötiedoiksi lisätietojen, kuten koodiavaimen, avulla (Korpisaari, Pitkänen & Warma-Lehtinen 2022, s. 72). Tietosuoja-asetuksen johdannon 26 kohdan mukaan pseudonymisoituja henkilötietoja, jotka on mahdollista yhdistää luonnolliseen henkilöön lisätietoja käyttämällä, ovat tietoja, jotka koskettavat tunnistettavaa luonnollista henkilöä. Näin ollen pseudonymisoidut ovat tietosuoja-asetuksen soveltamisalaan lukeutuvia henkilötietoja, kun taas anonymisoidut tiedot jäävät asetuksen soveltamisalan ulkopuolelle. Pseudonymisointia on käsitelty myös luvussa 4.4.1 (”Järjestelmien elinkaarimalli osana oikeudellista suunnittelua”).

harkintaan jää suojatoimenpiteiden riittävyys henkilötietojen käsittelyyn liittyvään riskiin suhteutettuna[761]. Tällöin suojatoimien toteuttamatta jättäminen ei tällaisessa sääntelymallissa voi johtaa seuraamuksiin, minkä vuoksi sääntelymalli on nähty ongelmallisena. Näin ollen tietoturvatoimenpiteet ovat suosituksenomaisia eivätkä ne ole suojatoimia koskien tyhjentäviä. Kritiikin mukaan suojatoimista olisi voitu säätää erikseen erityislainsäädännössä, niin kuin esimerkiksi tiedonhallintalaissa on säädetty tietoturvallisuustoimenpiteistä. Kyseisen kansallisen tietosuojalain 6 §:n suojatoimiluettelolla ei ole merkitystä muusta pakottavasta ja veloittavasta sääntelystä johtuen.[762] Kyseinen kritiikki on ymmärrettävää. On sinänsä erikoista säätää esimerkinomaisesti tietoturvatoimenpiteistä, joiden toteuttamatta jättämisellä ei ole seuraamuksia. Yhtä lailla säännöksessä olisi voitu viitata standardeihin mahdollisena esimerkkinä käytännön toteuttamistavoista. Henkilötietojen käsittelyyn liittyvien tietoturvatoimenpiteiden asianmukaisuus onkin riippuvainen riskiarvioinnista. Rekisterinpitäjällä on tietosuoja-asetuksen 82 artiklaan perustuvan vahingonkorvauskanteen yhteydessä todistustaakka siitä, että sen yleisen tietosuoja-asetuksen 32 artiklan nojalla toteuttamat turvallisuustoimenpiteet ovat asianmukaisia: asianmukaisuutta arvioitaessa kansallisten tuomioistuinten on otettava huomioon käsittelyyn liittyvät riskit ja onko toimenpiteet mukautettu näihin riskeihin[763]. Näin ollen tietosuojalain 6 §:n esimerkinomainen suojatoimiluettelo saa kuitenkin painoarvoa, sillä siinä ilmentyvät tietoturvatoimenpiteet tulisi huomioida osana erityisten henkilötietojen käsittelyyn liittyvää tietosuojan riskiarviointia.

Tietosuojalain 6 §:n 2 momentin tietoturvatoimenpiteet ovat myös erinomainen esimerkki hyvien tietoturvallisten käytänteiden mukaisesta teknologianeutraalista sääntelystä[764], vaikkakin suojatoimiluettelon fokus on erityisten henkilötietojen suojaamisessa. Kyseisen suojatoimiluettelon tietoturvatoimenpiteet ovat tietoturvanäkökulmasta ”perusasioita”, jotka tulisi huomioida organisaatioissa muunlaistenkin tietojen suojaamiseksi. Suojatoimiluettelon tietoturvatoimenpiteistä olisi edistyksellistä säätää vähimmäisvaatimuksina tietoturvan yleislaissa niin, että fokuksena ei olisi ainoastaan henkilötietojen suojaaminen vaan organisaatioiden tietojen turvaaminen ja tietoturvan vähimmäistason ylläpitäminen.

Lopuksi todettakoon, että oikeus kyberturvaan sekä henkilötietojen suojaan tulisi koskea kaikkia yksilöitä, mikä on myös peruste sille, että muitakin tietoja kuin

---

[761] HE 9/2018 vp: 91.
[762] Voutilainen 2019: 174–175, 195; HE 9/2018 vp: 91.
[763] Ks. myös luku 3.4.1 (”Tekniset ja organisatoriset toimenpiteet sekä operatiiviset toimenpiteet”) sekä ratkaisu EUT 14.12.2023, C-340/21, VB v. Natsionalna agentsia za prihodite, kohdat 10–13, 39, 47, 55, 57, 64.
[764] Teknologianeutraalisuuden periaatteen vuoksi teknisiin toteuttamistapoihin ei ole otettu kantaa säädöksessä.

arkaluontoisia, erityisiä henkilötietoja tulee suojata asianmukaisesti kaiken kokoisissa organisaatioissa. Tietosuoja on hyvinkin riippuvainen tietoturvan toteuttamistavoista. Tietosuojalain 6 §:n suojatoimiluettelo on hyvä esimerkki siitä, miten tällaista kaikkia organisaatioita velvoittavaa vähimmäistasosääntelyä voisi toteuttaa tietoturvan yleislaissa. Nykyisellään henkilötietoja suojaavan lainsäädännön hajaantuneiden tietoturvavaatimusten tunnistaminen vaatii tietoturvan sääntelyjärjestelmän kokonaisvaltaista tuntemista, mikä todennäköisesti vähentää säännöksien tavoitettavuutta etenkin maturiteettitasoltaan kypsymättömien organisaatioiden osalta. Tämä aiheuttaa riskiä erityisesti yksilöiden oikeuksien toteutumiselle, mutta mahdollisesti myös yhteiskunnan toimivuudelle sekä organisaatioiden maineelle, taloudelle ja jatkavuudelle. Myös tietoturvan tulisi olla oletusarvoista ja sisäänrakennettua organisaation toiminnassa, prosesseissa ja palveluissa – aivan kuten tietosuojankin.

3.4 Tietoturvan sääntelyjärjestelmän erilaiset tietoturvatoimenpiteet

3.4.1 Tekniset ja organisatoriset toimenpiteet sekä operatiiviset toimenpiteet

Tietosuoja-asetuksessa käytetty käsite ***”tekniset ja organisatoriset toimenpiteet”*** ei ole viimeisen 10 vuoden sisällä kehitetty uusi käsite, sillä se on esiintynyt aikaisemmin esimerkiksi kumotussa henkilötietolaissa (523/1999), jonka mukaan rekisterinpitäjän vastuulla oli toteuttaa kyseiset toimenpiteet henkilötietojen suojaamiseksi. Henkilötietolaissa esiintyvien teknisten ja organisatoristen toimenpiteiden toteuttamisessa oli otettava huomioon käsittelyn merkitys yksityisyyden suojan kannalta, käytettävissä olevat tekniset mahdollisuudet, kustannukset sekä käsiteltävien tietojen laatu, ikä ja määrä. Tällöin rekisterinpitäjän oli määriteltävä tietojen käyttöoikeudet ja käsittelyyn oikeuttavat tavat sekä salasanajärjestelmän avulla tai vastaavin turvajärjestelyin estettävä oikeudettomien henkilöiden pääsy käsittelemään tietoja. Lisäksi rekisterinpitäjän oli suojattava rekisterit niin, että laittomat sisäänpääsy-yritykset laitteistojen ja tietojen osalta aiheuttavat hälytyksen rekisterinpitäjälle sekä mahdollisesti antavat tietoa laittoman yrityksen alkuperästä. Rekisterinpitäjän oli luotava tarpeen mukaan menettelytavat tietojen käsittelyn seuraamiselle sekä tietojen siirto oli varmistettava erityisin toimenpitein niin, että esimerkiksi tietojen siirto ei aiheuta muutoksia tietojen sisällössä eikä tietoja häviä.[765] Näin ollen käsitteen tekniset ja organisatoriset toimenpiteet olivat

[765] HE 96/1998 vp: 66.

tästä näkökulmasta kuitenkin pääosin teknisiä ja keskeistä oli suojata henkilötietoja.

Myös kumotussa NIS 1 -direktiivissä keskeisten palveluiden tarjoajien sekä digitaalisen palvelun tarjoajien velvoitteissa oli yhtenäisesti määritelty, että toimijoiden oli määritettävä ja toteutettava asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet verkko- ja tietojärjestelmiin kohdistuvien turvallisuusriskien hallitsemiseksi ja turvallisuuden toteuttamiseksi. Direktiivi painotti myös sitä, että teknisten ja organisatoristen toimenpiteiden oli suhteutettava verkko- ja tietojärjestelmän kohdistuvaan riskin tasoon nähden huomioon ottaen uusin tekniikka, jottei keskeisten palvelujen tai digitaalisen palvelun tarjoajille aiheutuisi suhteetonta taloudellista ja hallinnollista rasitetta. Direktiivin 51 kohdassa oli myös täsmennetty, että tekniset ja organisatoriset toimenpiteet eivät kuitenkaan saaneet edellyttää tietyn kaupallisen viestintä- ja tietoteknologiatuotteen suunnittelua, valmistamista tai kehittämistä tietyllä tavalla. Lisäksi digitaalisen palvelun tarjoajien oli otettava huomioon teknisissä ja organisatorissa toimenpiteissään uusimman tekniikan lisäksi myös järjestelmien ja tilojen turvallisuus, poikkeamien käsittely, liiketoiminnan jatkuvuus, kansainvälisten standardien noudattaminen sekä seuranta, tarkastukset ja testaukset.

NIS 1 -direktiivissä ei määritelty tarkemmin, mitä teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan tai mikä on tällaisten tietoturvatoimenpiteiden vähimmäistaso. Toimenpiteiden sisältö jätettiin avoimeksi, jotta toimenpidepäätös voisi suhteuttaa riskin tasoon nähden. Lainsäädännön esitöissä on myös täsmennetty, että riskienhallinnalla tarkoitetaan asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tietojärjestelmien ja viestintäverkkojen kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat a) tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka; b) tarjottujen tai niiden välityksellä saatavien palvelujen luottamuksellisuuden, eheyden, saatavuuden tai aitouden[766]. Tämäkään määritelmä ei avaa teknisten ja organisatoristen toimenpiteiden sisältöä sen tarkemmin, mutta itse toimenpiteiden tarkoituksena on suojata tietojärjestelmiä ja viestintäverkkoja. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen sekä niiden testaaminen tai auditointi, tunnettujen tietoturvallisuusstandardien noudattaminen[767] sekä tiedon suojaus- ja salaustuotteiden käyttö[768].

NIS 1 -direktiiviä ja tietosuoja-asetusta valmisteltiin samoin aikoihin, joten olisi voinut olettaa, että NIS 1 -direktiivissä esiintyvät tekniset ja organisatoriset

[766] HE 192/2017 vp: 65, 68, 70–74, 76–77, 79.
[767] Kuten esimerkiksi ISO/ IEC 27001:2013 tietoturvallisuuden hallintajärjestelmää koskeva standardi.
[768] HE 192/2017 vp: 65, 68, 70–74, 76–77, 79.

toimenpiteet olisivat olleet samankaltaisia kuin tietosuoja-asetuksessa. Huomioitava myös on, että alkuperäinen NIS 1 -direktiivi ei viitannut tietosuoja-asetukseen suoranaisesti, vaan esimerkiksi NIS 1 -direktiivin 2 artiklassa oli viittaus vanhaan henkilötietodirektiiviin (1995/46/EY), vaikka tietosuoja-asetus oli jo tuolloin julkaistu[769]. Näin ollen näissä kahdessa säädöksessä esiintyvä käsite *”tekniset ja organisatoriset toimenpiteet”* on lähtökohtaisesti pitänyt käsitellä erillään jo niiden historian, mutta myös näkökulman vuoksi.

Tietosuoja-asetuksen mukaan rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joiden avulla tietosuoja-asetuksen velvoittama osoitusvelvollisuus pystytään näyttämään toteen ja rekisterinpitäjä pystyy myös varmistamaan, että yleistä tietosuoja-asetusta noudatetaan organisaation henkilötietojen käsittelyssä. Asetuksen mukaan osoitusvelvollisuus pystytään muun muassa näyttämään toteen riittävällä dokumentaatiolla sekä kokonaisvaltaisella riskienhallinnan toteutumisella. Täten voidaan päätellä, että riittävä dokumentointi ja riskienhallinnan toteutuminen kuuluvat teknisiin ja organisatorisiin toimenpiteisiin.

Tietosuoja-asetuksen 24 (1) artiklan mukaan teknisiä ja organisatorisia toimenpiteitä arvioitaessa, tarkistaessa ja päivittäessä on otettava huomioon luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit sekä henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Teknisten ja organisatoristen toimenpiteiden tarkoituksena on 25 (2) artiklan mukaan myös varmistaa, että oletusarvoisesti käsitellään vain tarpeellisia henkilötietoja koskien muun muassa kerättyjen henkilötietojen määriä, säilytysaikaa ja saatavilla oloa sekä käsittelyn laajuutta. Tietosuoja-asetuksen teknisten ja organisatoristen toimenpiteiden tarkoituksena on etenkin varmistaa, ettei henkilötietoja saateta oletusarvoisesti rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

Tietosuoja-asetuksen 24 ja 25 artiklat koskevat ainoastaan rekisterinpitäjän vastuuta. Tietosuoja-asetuksen 32 artikla ulottaa puolestaan teknisten ja organisatoristen toimenpiteiden velvollisuuden myös henkilötietojen käsittelijään. Rekisterinpitäjän ja henkilötietojen käsittelijän on 32 artiklan mukaan toteutettava todennäköisyydeltään ja vakavuudeltaan vaihtelevan riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Tällaisia teknisiä ja organisatorisia toimenpiteitä ovat yleisen tietosuoja-asetuksen 32 artiklan mukaan:

[769] Hert, Markopoulou & Papakonstantinou 2019: 9.

a) henkilötietojen pseudonymisointi[770] ja salaus,

b) kyky taata palveluiden sekä henkilötietoja käsittelevien järjestelmien luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus,

c) teknisen tai fyysisen vian sattuessa kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin, sekä

d) säännöllisen menettelyn omaksuminen teknisten ja organisatoristen toimenpiteiden tehokkuuden arvioimiseksi ja testaamiseksi.[771]

Kyseinen luettelo ei määrittele kovinkaan tarkasti spesifejä toimia turvallisuustason varmistamiseksi, vaan tämä jää rekisterinpitäjän päätettäväksi. Voisi sanoa, että kyseessä on enemminkin tavoitteet, joihin rekisterinpitäjän pitää pyrkiä erilaisilla toimilla.[772] Erityisiä teknisiä toimenpiteitä voivat olla lokitus, henkilötietojen salaaminen ja tietojen palauttaminen varmuuskopioista, kun taas organisatorisia toimenpiteitä voivat olla esimerkiksi vaikutustenarviointi, menettelysäännöt, henkilökunnan koulutus, testaus ja itsearviointi[773]. Tietosuoja-asetuksen vaatimuksista johdettuna organisatorisia toimenpiteitä ovat myös erilaisten dokumenttien laatiminen ja ylläpitäminen[774]. Lisäksi organisatorisiin toimenpiteisiin on katsottu kuuluvaksi suunnitella, miten organisaatio tiedottaa henkilötietojen käsittelystä eri tilanteissa sekä miten toimitaan, kun henkilötietoja ei voida käsitellä tietojärjestelmissä[775]. Jälkimmäinen vaatimus on pitkälti yhdistettävissä organisaation jatkuvuus- ja toipumissuunnitteluun. Joka tapauksessa tietosuoja-asetuksen tekniset ja organisatoriset toimenpiteet huomioivat paremmin myös organisatoriset toimenpiteet kuin esimerkiksi kumottu henkilötietolaki.

Tietosuoja-asetuksen 24 (2) artiklassa myös mainitaan, että teknisiin ja organisatorisiin toimenpiteisiin kuuluu silloin, kun se on oikeasuhteista, että rekisterinpitäjä panee täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet. Tietosuoja-asetuksessa ei avata sen enempää, mitä näillä toimintaperiaatteilla (*data protection policies*) tarkoitetaan, mutta ne katsotaan monitulkintaisesti olevan osana säädettyä osoitusvelvollisuuden toteutumista. Toimintaperiaatteita syntyy, kun rekisterinpitäjä suunnittelee teknisiä ja organisatorisia toimenpiteitä.

---

[770] Pseudonymisointi on henkilötietojen käsittelemistä tavalla, jolloin tietoja ei voida suoraan yhdistää tiettyyn rekisteröityyn käyttämättä muita lisätietoja. Ks. Tietosuojavaltuutetun toimisto 2019b.
[771] Näitä toimia on myös käsitelty sisällöltään tarkemmin edellisessä alaluvussa osana kansallisen tietosuojalain 6 §:n erityisiä henkilötietoryhmiä suojaavia tietoturvatoimenpiteitä, ks. luku 3.3.5 (”Muut tietosuojalainsäädännön tietoturvavaatimukset”).
[772] Nyyssölä 2018: 244.
[773] Korpisaari, Pitkänen & Warma-Lehtinen 2018: 161.
[774] Ks. luku 3.3.1 ”Sääntelyjärjestelmän dokumentaatiovaatimukset”.
[775] Voutilainen 2019: 193.

Täten periaatteet voivat liittyä esimerkiksi henkilötietojen keräämiseen, käsittelyn valvontaa tai raportointiin, jolloin ne avaavat osaltaan, miten organisaatio on suunnitellut toimivansa tietosuoja-asetuksen mukaisesti.[776] Toimintaperiaatteet käsitteenä ei ole kovin käytetty käytännön toiminnassa, vaan voisi ennemminkin puhua organisaation sisäisistä henkilötietojen käsittelyyn liittyvistä ohjeistuksista ja linjauksista.

Asetuksen mukaan myös käytännesääntöjen ja sertifiointimekanismin noudattamista voidaan pitää yhtenä tekijänä asetuksen vaatimusten noudattamisen toteennäyttämiseksi teknisten ja organisatoristen toimenpiteiden osalta. Käytännössä tietosuoja-asetuksen teknisten ja organisatoristen tietoturvallisuustoimenpiteiden suunnittelu ja toteutus jää osittain kansallisen erityislainsäädännön, alan käytäntöjen ja käytännesääntöjen sekä rekisterinpitäjien ja henkilötietojen käsittelijöiden riskiperusteisen suunnittelutoimenpiteiden varaan[777]. Henkilötietojen käsittelyn turvallisuuden ja osoitusvelvollisuuden todentamisen näkökulmasta onkin hyvä, jos organisaatio pystyy todentamaan, että sen tuottamat palvelut ja prosessit noudattavat hyviä käytänteitä ja tietoturvallisuuden käytännesääntöjä[778].

Tietosuoja-asetuksessa on korostettu turvallisuustason varmistamiseksi *asianmukaisia* teknisiä ja organisatorisia toimenpiteitä, joita toteuttaessa on otettava huomioon *uusin tekniikka* ja kustannukset. Lähtökohtaisesti asianmukaisen turvallisuustason vaatimus tuomitsee organisaatioita, jotka ovat laiminlyöneet velvollisuutensa pitää asiakkaidensa tiedot turvassa. Asiantuntijoiden standardien mukaan asianmukaisuuden vaatimus ei kuitenkaan edistä parannuksia organisaatioiden tietoturvassa eikä täytä edes turvallisuuden vähimmäistasoa. Onkin kritisoitu, että tällainen epämääräinen käsite voi aiheuttaa huolimattomuutta, tehottomuutta ja huonoa turvallisuuden omaksumista organisaatioissa, mikä voi johtaa jatkuviin ja vakaviin tietoturvaloukkauksiin. *Uusin tekniikka* -käsite on puolestaan tunnettu oikeudellinen termi, jonka käytöllä on pyritty toteuttamaan lainsäädännön teknologianeutraalisuutta. Tätäkin käsitettä on kritisoitu monimutkaiseksi ja epämääräiseksi, joka mahdollistaa tulkinnanvaraisuudesta johtuvan huolimattomuuden.[779] Käsitteet *asianmukainen* ja *uusin tekniikka* toistuivat myös NIS 1 -direktiivissä. NIS 2 -direktiivissä painotus on asianmukaisuuden lisäksi oikeasuhteisuudessa – uusin tekniikka on jätetty pois.

Edellä mainitun kritiikin osalta on totta, että *asianmukaisuuden* vaatimus lainsäädännössä ei välttämättä suoraan paranna organisaatioiden tietoturvaa tai aseta

[776] Ibid: 127.
[777] Ibid: 196–197.
[778] Ks. lisää 2.7 (”Tietoturvan sääntelyjärjestelmä ja hyvät käytänteet”) ja 4.4.5 (”Tietoturvan vähimmäisvaatimukset ja tietoturvatason arviointi”).
[779] Akatyev, Han, Hwang, Jang, Kim D., Kim J., Park, Shin, & Yu 2018: 95–96.

sille vähimmäistasoa. Se kuitenkin antaa teknologianeutraalisti harkintavaltaa vastuullisille toimijoille päättää riskiperusteisesti tarvittavista tietoturvatoimista ja tietoturvallisuuden tasosta. Näin ollen voidaan päätellä, että asianmukaisuudesta säädettäessä ei ole ollut edes tarkoitus säätää samaan aikaan tietoturvan vähimmäistasosta. Huomioitava on myös se, että dokumentoitavalla riskienarvioinnilla, jossa pyrkimyksenä on kattavasti tunnistaa organisaatioon ja sen järjestelmiin kohdistuvia uhkia, on mahdollista parantaa tietoturvaa tunnistamalla heikkouksia.

Yhtä lailla *uusin tekniikka* -käsitettä on kritisoitu epämääräiseksi, joka voi aiheuttaa tulkinnanvaraisuudellaan huolimattomuutta. Tämä kritisointi on melko perusteetonta, sillä on tärkeää huomioida uudet tekniset mahdollisuudet niin tietoturvatoimenpiteitä suunniteltaessa käytännössä kuin lainsäädännön tasolla. Teknologian ottaessa harppauksia eteenpäin, aiheesta on kuitenkin lähes mahdotonta säätää yksityiskohtaisesti, minkä vuoksi tarvitaan juuri tällaista teknologianeutraalia ja normatiivisiin käsitteisiin perustuvaa sääntelyä, joka samalla lisää toimijoiden vastuuta seurata teknologian muutoksia ja arvioida niiden tarpeellisuutta omassa toiminnassaan.

Kaiken kaikkiaan *asianmukaisten teknisten ja organisatoristen toimenpiteiden* -vaatimus on kuitenkin haastava juuri sen monimerkityksellisyyden takia. Esimerkiksi jonkun asiantuntijan mielestä asianmukainen, kohtuullinen ja uusimman tekniikan huomioiva, turvallisuustasoa varmistava toimenpide voi olla riittävä, kun taas jonkun toisen mielestä ei. Näin on ainakin siihen asti, kunnes jokin asia menee pieleen ja syntyy turvallisuuspoikkeama. Tietoturvallisuuden osalta tulisi pyrkiä ennalta ehkäisemään poikkeamia, ei reagoimaan niihin vasta tapahtumahetkellä. Siksi tarvitaan riskien arviointia ja hallintaa. Riskienhallinta on ollut myös nykyisen tietosuoja- ja tietoturvalainsäädännön kehityksen fokuksessa. Asianmukaisia toimenpiteitä arvioitaessa ja niistä päätettäessä tuleekin perusteissa tukeutua riskien arvioinnin tuloksiin. Tällaiseen lopputulokseen on tultu myös **EUT:n ratkaisussa 14.12.2023, C-340/21 VB v. Natsionalna agentsia za prihodite**[780]:

> *Tapauksessa viranomaisorganisaationa ja rekisterinpitäjänä toimivan NAP:n tietojärjestelmään oli päästy luvattomasti ja kyseisen kyberhyökkäyksen seurauksena saatuja henkilötietoja oli julkaistu internetissä yli 6 miljoonan luonnollisen henkilön osalta. Pääasian kantaja vaati korvauksia henkisestä kärsimyksestä, joka kantajan mukaan oli seurausta siitä, että rekisterinpitäjä ei ollut muun muassa varmistanut henkilötietojen*

[780] Ratkaisun kohdat 10–13, 39, 47, 55, 57, 64.

> *asianmukaista turvallisuutta (5 artiklan 1 f-kohta), toteuttanut 24 artiklan asianmukaisia teknisiä ja organisatorisia toimenpiteitä eikä ollut noudattanut 25 artiklan mukaisia sisään rakennetun ja oletusarvoisen tietosuojan vaatimuksia. Kantajalle muodostui henkistä kärsimystä pelosta siitä, että ilman hänen suostumustaan julkistettuja, häntä koskevia henkilötietoja voidaan käyttää tulevaisuudessa väärin tai että häntä kiristetään, häntä vastaan hyökätään tai hänet jopa kaapataan. Ratkaisussa EUT painotti asianmukaisuuden osalta sitä, että kansallisten tuomioistuinten on arvioitava konkreettisesti rekisterinpitäjän kyseisen artiklan perusteella toteuttamien teknisten ja organisatoristen toimenpiteiden asianmukaisuutta ottaen huomioon kyseessä olevaan käsittelyyn liittyvät riskit ja arvioiden, onko näiden toimenpiteiden luonne, sisältö ja täytäntöönpano mukautettu näihin riskeihin. Kolmansien osapuolien pääsy luvattomasti järjestelmään ei sellaisenaan riitä toteamiseen sen osalta, että rekisterinpitäjän toteuttamat tekniset ja organisatoriset toimenpiteet eivät olleet asianmukaisia 24 ja 32 artiklassa tarkoitetussa merkityksessä. Lisäksi rekisterinpitäjällä on tietosuoja-asetuksen 82 artiklaan perustuvan vahingonkorvauskanteen yhteydessä todistustaakka siitä, että sen yleisen tietosuoja-asetuksen 32 artiklan nojalla toteuttamat turvallisuustoimenpiteet ovat asianmukaisia. Kuitenkin asiantuntijalausunto ei voi olla systemaattisesti tarvittava ja riittävä todiste rekisterinpitäjän tämän artiklan nojalla toteuttamien turvallisuustoimenpiteiden asianmukaisuuden arvioimiseksi.*

EUT:n ratkaisu on merkittävä asianmukaisia tietoturvatoimenpiteitä arvioitaessa, sillä se lisää organisaatioiden riskienhallinnan vastuuta. Merkittävä linjaus on myös se, että yksistään asiantuntijalausunnot eivät voi olla riittävä todiste asianmukaisista turvallisuustoimenpiteistä. Tämä tarkoittaa käytännössä sitä, että kolmannen osapuolen tekemät auditointiraportit tai arviointilausunnot palvelusta tai järjestelmästä eivät ole riittäviä evidenssejä asianmukaisesta tietoturvatasosta. Käytännön työssä tällaisia tietoturva-arviointeja tai -auditointeja on saatettu yksistään pitää riittävinä. Näin ollen tietoturvatoimenpiteiden määritys henkilötietojen suojaamiseksi tulee perustua dokumentoituun riskiarviointiin, jota tarvittaessa tuomioistuinten on pystyttävä arvioimaan konkreettisesti[781]. Riskiarvioinnissa tulee huomioida myös käsittelystä mahdollisesti aiheutuvat henkilötietojen tietoturvaloukkaukset ja niiden mahdolliset vaikutukset luonnollisten henkilöiden oikeuksiin ja vapauksiin, jotta asianmukaiset tietoturvatoimenpiteet pystytään

[781] Ks. ratkaisun kohta. 43. Kansallisen tuomioistuimen on voitava arvioida rekisterinpitäjän suorittamaa monitahoista arviointia ja näin tehdessään varmistaa, että rekisterinpitäjän toteuttamat toimenpiteet soveltuvat tällaisen turvallisuustason varmistamiseen.

määritellä[782]. Asianmukaiset toimenpiteet ja tarvittavat suojatoimet palvelevat samaa tarkoitusta eli rekisteröityjen oikeuksien suojaamista sekä sen varmistamista, että rekisteröityjen henkilötietojen suojaaminen sisällytetään osaksi käsittelyä[783]. Asianmukaisuuden ja tietoturvatoimenpiteiden määrittämisen tukena tarvitaan riskien arvioinnin tuloksia.

Tietosuoja-asetuksessa teknisten ja organisatoristen toimenpiteiden päämääränä on ensisijaisesti henkilötietojen ja yksityisyyden suojaaminen. Alkuperäisessä NIS 1 -direktiivissä ensisijainen päämäärä oli verkko- ja tietojärjestelmien turvallisuusriskien hallitseminen sekä palveluiden jatkuvuuden takaaminen. Huomioitava on se, että myös teledirektiivin (2018/1972/EU) V osiossa on säädelty yleisten sähköisten viestintäverkkojen tai yleisten saatavilla olevien sähköisten viestintäpalveluiden tarjoajien velvollisuudesta toteuttaa tarvittavat ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen verkkojen ja palvelujen turvallisuuteen kohdistuvia riskejä. Näin ollen esimerkiksi NIS 1 -direktiiviin verraten teledirektiivin turvallisuussääntelyn keskiössä on ollut yleiset sähköiset viestintäverkot ja yleisesti saatavilla olevat sähköiset viestintäverkot. Teledirektiivissä on myös painotettu, että teknisillä ja organisatorisilla toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso huomioon ottaen myös uusin tekniikka. Lisäksi direktiiviä tulkittaessa voidaan päätellä, että teknisiä ja organisatorisia toimenpiteitä voivat olla salaustoimenpiteet sekä sellaiset toimenpiteet, jotka ehkäisevät ja minimoivat turvapoikkeamista aiheutuvia vaikutuksia käyttäjille sekä muille verkoille ja palveluille.

Alkuperäisen NIS 1 -direktiivin kumoavassa NIS 2 -direktiivissä teknisiä ja organisatorisia toimenpiteitä on yllättävän vähän painotettu. Artiklan 21 mukaan keskeisten ja tärkeiden toimijoiden on toteutettava asianmukaiset ja oikeasuhteiset ***tekniset, operatiiviset ja organisatoriset toimenpiteet*** hallitakseen riskejä, joita niiden toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu, ja estääkseen tai minimoidakseen poikkeamien vaikutuksen palvelujensa vastaanottajiin ja muihin palveluihin. Artiklan toisen kohdan mukaan toimenpiteisiin on sisällytettävä vähintään riskianalyyseja ja tietojärjestelmien turvallisuuspolitiikkoja, poikkeamien käsittelyä, toiminnan jatkuvuuden hallintaa, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisitilanteiden hallintaa. Toimenpiteisiin on myös sisällytettävä toimitusketjun turvallisuuden huomioimista, verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuutta mukaan lukien haavoittuvuuksien käsittely ja julkistaminen, toimintaperiaatteet ja menettelyt kyberturvallisuusriskien hallintatoimenpiteiden tehokkuuden arviointiin, perustason kyberhygienia

[782] Ratkaisun kohta 42.
[783] Euroopan tietosuojaneuvoston (EDPB) ohje 4/2019, s. 6.

käytännöt ja kyberturvallisuuskoulutus, salaustekniikoiden käyttöä koskevat toimintaperiaatteet ja menettelyt, henkilöstöturvallisuutta, pääsynhallintaperiaatteita ja omaisuudenhallintaa sekä tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.

Näin ollen NIS 2 -direktiivissä löytyy toteutustasolla enemmän konkretiaa. Käsitteistöön on kuitenkin jälleen lainsäädäntöuudistuksen myötä tullut muutoksia, kun operatiivisuuden ulottuvuus on lisätty osaksi tietoturvatoimenpiteitä. Operatiivisuutta ei ole sen tarkemmin täsmennetty käsitteenä direktiivissä[784]. Lisäksi käsitteen osalta ei tule selkeästi ilmi, miten operatiiviset toimenpiteet olennaisesti eroavat teknisistä ja organisatorista toimenpiteistä. Kuitenkin yleiskielessä operatiivisuus viittaa organisaatioissa esimerkiksi jokapäiväiseen ja varsinaiseen käytännön työhön. Tältä näkökannalta operatiiviset toimenpiteet olisivat tietoturvan osalta sellaisia, joissa tietoturvaa toteutetaan jokapäiväisessä työssä. Tällöin vastakohtaisesti ei-operatiiviset tekniset ja organisatoriset toimenpiteet olisivat esimerkiksi ennaltaehkäiseviä, kehittäviä tai jopa kertaluontoisia toimenpiteitä. Operatiivisten toimenpiteiden lisäys tietoturvatoimenpiteiden käsitteistöön on varsin huono ja tehoton tästä näkökulmasta, koska aikaisemman tulkinnan mukaan myös teknisten ja organisatoristen toimenpiteiden tarkoitus on ollut muun muassa turvallisuuden toteuttaminen, poikkeamien käsittely sekä oletusarvoinen (henkilö)tietojen suojaaminen jokapäiväisessä toiminnassa.

Yhteenvetona todettakoon, että edellä käsiteltyjen säädöksien perusteella teknisten ja organisatoristen toimenpiteiden käsitteen sisältö ei ole ollut kovin yksiselitteinen sen osalta, minkälaisia tietoturvatoimenpiteitä teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan. Toteuttamisvaihtoehdot vaihtelevat säädöskohtaisesti kunkin säädöksen painotuksen mukaan, ja lisäksi teknologianeutraalisuuden periaate tuo paljon tulkinnanvaraisuutta toimenpiteiden toteuttamistavoille. Esimerkiksi NIS 1 -direktiivissä teknisten ja organisatoristen toimenpiteiden sisältö jätettiin avoimeksi, jotta toimenpidepäätös voisi suhteuttaa riskin tasoon nähden. Myös tietosuoja-asetus painottaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä, jolloin tietoturvatoimenpiteiden tulisi lähtökohtaisesti pohjautua mahdollisten hyvien käytännesääntöjen ja standardien lisäksi dokumentoituun riskiarviointiin, jotta asianmukaisuutta olisi ylipäätänsä mahdollista arvioida.

---

[784] Hallituksen esityksessä 57/2024 ei ole myöskään operatiivisen toimenpiteen ulottuvuutta käsitelty esimerkiksi kyberturvallisuuslain 2 §:n määritelmissä. Tiedonhallintalain 4a-lukuun se tulee myös mukaan sellaisenaan, eli tiedonhallintalaissa on käytössä 4a-luvussa *”tekniset, operatiiviset ja organisatoriset kyberturvallisuuden riskienhallintatoimenpiteet”*, mutta muutoin tiedonhallintalaissa käytetään tietoturvallisuustoimenpiteistä hallinnollisten, toiminnallisten ja teknisten toimenpiteiden määritelmää.

Tekniset ja organisatoriset toimenpiteet ei ole käsitteenä jalkautunut niin hyvin kansalliseen lainsäädäntöön ja käytäntöihin (lukuun ottamatta tietosuojalainsäädäntöä ja -ohjeistuksia), koska se ei ole hyvien tietoturvakäytänteiden mukainen. Käytännön tasolla tietoturvan toimenpiteet jakautuvat hallinnollisiin, fyysisiin ja teknisiin toimenpiteisiin[785]. NIS 2 -direktiivin mukaiset tekniset, organisatoriset ja operatiiviset toimenpiteet lisäävät sisällöltään konkretiaa vähimmäisvaatimuksillaan, mutta ne kohdistuvat vain tiettyihin toimijoihin kriittisillä toimialoilla. Lisäksi NIS 2 -direktiivissä esiintyvä ”operatiiviset toimenpiteet” ilmenee varsin merkityksettömänä lisänä teknisten ja organisatoristen toimenpiteiden käsitteessä.

Kaikki nämä havainnot tekevät tietoturvan sääntelyjärjestelmästä haastavan ymmärrettävyydeltään ja tavoitettavuudeltaan. Vaadittavasta tietoturvan vähimmäistasosta ei ole säädetty kaikkia organisaatioita velvoittaen, jolloin asianmukaisten tietoturvatoimenpiteiden määrittely pitäisi perustua lainsäädännön mukaan organisaation tekemään, dokumentoituun riskiarvioon. Tämä heikentää erityisesti yksilöiden perusoikeuksien toteutumista, koska käytännön työssä etenkin tietoturvatasoltaan epäkypsemmissä organisaatioissa tällainen tietoturvatoimenpiteiden suhteuttaminen riskiarvioon ei välttämättä toteudu.

3.4.2 Hallinnolliset ja tekniset toimenpiteet

Aikaisemmin käsitelty teknisten ja organisatoristen toimenpiteiden käsite on kansallisessa lainsäädännössä esiintynyt lähinnä tietosuojalainsäädännössä. Kansallisessa lainsäädännössä on kuitenkin kuvailtu tietoturvaan liittyviä toimenpiteitä myös muunlaisin käsittein vuosien saatossa, ja niiden sisältämissä merkityksissä on ollut eroja etenkin tietoturvallisuuden osa-alueiden painotuksessa. Esimerkiksi yksityisyyden suojasta televiestinnästä ja teletoiminnan tietoturvasta annetussa laissa (565/1999) tietoturvakäsitteen määritelmän yhteydessä käytettiin käsitettä ***”hallinnollisin ja teknisin toimenpitein”***. Tämä laki kumottiin ja nykyään tilalla on laki sähköisen viestinnän palveluista (917/2014), jossa myös esiintyy käsite hallinnolliset ja tekniset toimet. Sähköisen viestinnän palveluista annetun lain mukaan tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tietojen olevan vain niiden käyttöön oikeutettujen saatavilla, ja että tietoja ei voi muuttaa muut kuin siihen oikeutetut, sekä tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Huomion arvoista on myös se, että laissa sähköisen viestinnän palveluista on 272 §:ssä säädetty toimenpiteistä tietoturvan toteuttamiseksi, johon esimerkiksi viestinnän välittäjän roolissa toimiva työnantaja voi ryhtyä tietoturvasta huolehtimiseksi. Tällaisia (tietoturva)toimia

[785] Ks. lisää tietoturvan elementeistä luvusta 2.2.1 (”Tietoturva”).

ovat viestin sisältöä koskeva automaattinen selvittäminen, viestien välittämisen ja vastaanottamisen automaattinen estäminen tai rajoittaminen, tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattinen poistaminen viesteistä sekä muut edellä tarkoitettuihin rinnastettavat teknisluonteiset toimenpiteet. Toimenpiteiden tulee toteuttaa huolellisesti ja käyttäjiä mahdollisuuksien mukaan informoiden sekä toimenpiteiden on oltava välttämättömiä viestin vastaanottajan viestintämahdollisuuksien taikka verkko- tai viestintäpalveluiden turvaamiseksi[786]. Edellä mainitut toimenpiteet tietoturvan toteuttamiseksi ovat lähinnä teknisiä. Täten itsessään hallinnollisia ja teknisiä toimenpiteitä ei ole avattu sen yksityiskohtaisemmin kyseisessä laissa.

Tietoturvasta huolehtimiseksi hallinnolliset ja tekniset toimet voivat kohdistua toiminnan turvallisuuteen, tietoaineistoturvallisuuteen, tietoliikenneturvallisuuteen sekä laitteisto- ja ohjelmistoturvallisuuteen[787]. Toiminnan turvallisuudella tässä yhteydessä tarkoitetaan kirjallisten ohjeiden ylläpitämistä esimerkiksi tietoturvallisuusvaatimusten toteuttamisesta, oman tietoturvatason säännöllisestä seuraamisesta, miten suojataan laitteet ja tiedostot luvatonta pääsyä ja käyttöä vastaan sekä miten varmistetaan tietoturvavaatimusten toteutuminen alihankkijoiden kohdalla. Toiminnan turvallisuudella tarkoitetaan myös tietoturvatapahtumien havaitsemista valvomalla asiakirjoja, verkkoja, laitteistoja ja palveluita sekä ylläpitämällä järjestelmärekisteriä, josta näkyy, kenellä on järjestelmän käyttäjätunnuksia ja minkälaisilla käyttöoikeuksilla.[788] Toiminnan turvallisuuden osalta kirjallisten ohjeistusten ylläpito omaa hallinnollisen tietoturvan vivahteen, vaikka muuten kyseiset hallinnolliset ja tekniset toimet ovat varsin teknisiä toteuttamistavoiltaan etenkin tietoaineistoturvallisuuden, tietoliikenneturvallisuuden sekä laitteisto- ja ohjelmistoturvallisuuden osalta. Myös fyysisen tietoturvallisuuden näkökanta jää uupumaan.

Hallinnollisia ja teknisiä tietoturvatoimia voivat olla myös esimerkiksi laitteiden ja järjestelmien pääsynvalvonta, tietojen ja järjestelmien luvattoman käytön esto ja käyttöoikeuksien määrittely, käsittelytapahtumien kirjaaminen, tietoliikenteen alkuperävalvonta ja reititysvalvonta, tietoliikenteen häirinnän valvonta ja sen estäminen, ylläpitotoimien asianmukainen järjestäminen sekä järjestelmien ja tietojen suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta (esimerkiksi haittaohjelmilta)[789]. Täten tämän täsmennyksen pohjalta hallinnolliset ja tekniset toimenpiteet keskittyvät ennemminkin teknisen tietoturvallisuuden osa-alueeseen jättäen hallinnollisen ja fyysisen tietoturvallisuuden käsittelyn kovin suppeaksi,

[786] HE 125/2003 vp: 71–73; Hoikka, Neuvonen & Rautiainen 2016: 511–512.
[787] HE 125/2003 vp: 70; PeVL 9/2004 vp: 8.
[788] Helopuro, Perttula & Ristola 2009: 23–24.
[789] HE 221/2013 vp: 91.

mikä ei myöskään vastaa hyviä tietoturvallisia käytänteitä. Määritelmä ilmentää tällöin myös vanhanaikaista lähestymistä tietoturvaan, sillä se jättää ”hallinnollisten” sekä teknisten turvatoimien toteuttamisvastuun käytännössä IT-henkilöstön vastuulle.

Sähköisen viestinnän palveluista annetun lain käsite *hallinnollisista ja teknisistä toimenpiteistä* on säilynyt ennallaan siitäkin huolimatta, että EU:ssa säädettiin *teknisistä ja organisatorista* toimenpiteistä yleisessä tietosuoja-asetuksessa ja alkuperäisessä NIS 1 -direktiivissä. Sähköisen viestinnän palveluista annetun lain määritelmiin ei ole myöskään tulossa muutosta NIS 2 -direktiivin implementoimista koskevan hallituksen esityksen HE 57/2024 mukaan. Tällöin hallinnolliset ja tekniset toimenpiteet säilyvät kyseisessä laissa ja NIS 2 -direktiivin mukainen käsite *teknisistä, operatiivisista ja organisatorisista toimenpiteistä* implementoidaan kansalliseen kyberturvallisuuslakiin. Näin ollen tietoturvan sääntelyjärjestelmän peruskäsitteistö tietoturvatoimenpiteiden osalta pysyy hajanaisena ja siten vaikeasti ymmärrettävänä. Lopuksi kuitenkin todettakoon, että itse hallinnolliset ja tekniset toimenpiteet käsitteenä kuvaa paremmin tietoturvatoimenpiteiden osa-alueita (hallinnollinen, tekninen ja fyysinen tietoturvallisuus) kuin tekniset ja organisatoriset toimenpiteet käsitteenä.

3.4.3 Viranomaisen hallinnolliset, tekniset ja toiminnalliset toimenpiteet

Viranomaisen tietoturvan vähimmäisvaatimuksia kuvaavassa tiedonhallintalaissa (906/2019) määritellään käsitteenä ***”tietoturvallisuustoimenpide”***, jolla tarkoitetaan tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden varmistamista ***hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä***. Näin ollen tiedonhallintalaista jätettiin suoraan pois käsite tekniset ja organisatoriset toimenpiteet, vaikkakin teknisten ja organisatoristen toimenpiteiden käsitettä oli juuri samoihin aikoihin painotettu osana EU:n uusia säädöksiä eli tietosuoja-asetusta ja NIS 1 -direktiiviä. Huomioitava on myös se, että tiedonhallintalain käsitteessä ei suoraan hyödynnetty sähköisen viestinnän palveluista annetun lain hallinnollisten ja teknisten toimenpiteiden käsitettä, vaan tiedonhallintalaissa kyseistä käsitettä laajennettiin uudella ulottuvuudella eli toiminnallisuudella.

Hallinnollisilla toimenpiteillä tarkoitetaan tässä yhteydessä tietoaineistojen hallinnoinnin järjestämistä siten, että tietoaineistoja käsitellään turvallisella ja viranomaisten toimintaa sekä julkisuusperiaatetta palvelevalla tavalla. Teknisillä toimenpiteillä tarkoitetaan teknisiä menettelyitä, joilla varmistetaan tietoaineistojen luottamuksellisuus, eheys ja saatavuus sopivilla ja riittävillä teknisillä ratkaisuilla. Toiminnallisilla toimenpiteillä tarkoitetaan menettelyitä, joilla viranomaisen

toiminnassa varmistetaan tietoaineistojen turvallinen käsittely. Näillä hallinnollisilla, teknisillä ja toiminnallisilla toimenpiteillä eli tietoturvallisuustoimenpiteillä tarkoitetaan esimerkiksi toiminnan turvallisuuden, tietoaineistoturvallisuuden, fyysisen turvallisuuden, tietoliikenne-, laitteisto- ja ohjelmistoturvallisuuden varmistavia toimenpiteitä, jotka on suhteutettava uhkien vakavuuteen, kustannuksiin ja tekniseen kehitystasoon.[790] On todettu, että tiedonhallintalaissa on käytetty tietosuoja-asetuksen kansallista liikkumavaraa, joten siinä säädetyillä tietoturvatoimenpiteillä määritellään tietosuoja-asetuksessa tarkoitettuja teknisiä ja organisatorisia toimenpiteistä henkilötietojen suojaamiseksi[791].

Hyvien tietoturvallisten käytänteiden näkökulmasta tietoturvallisuustoimenpiteen määritelmä on paljon laajempi kuin aikaisemmin käsitelty hallinnollisten ja teknisten toimenpiteiden määritelmä, sillä se ottaa muun muassa fyysisen turvallisuuden huomioon. Se on myös yksinkertaisemmin muotoiltu kuin teknisten ja organisatoristen toimenpiteiden määritelmä. Tosin toiminnallisten toimenpiteiden eriyttäminen hallinnollisista toimenpiteistä on tarpeetonta, sillä molempien toimien tavoitteena on alun perinkin tietoaineistojen turvallinen käsittely. Tietoaineistojen turvallista käsittelyä varmistetaan kaikilla tietoturvallisuuden osa-alueilla eli hallinnollisilla, teknisillä ja fyysisillä tietoturvatoimenpiteillä. Näin ollen toiminnallisten toimenpiteiden lisäys lainsäädäntöön ei loppujen lopuksi ole kovin relevantti muutos, vaan se enneminkin sekoittaa jo olemassa olevaa käsiteviidakkoa.

Yhteenvetona todettakoon, että viranomaisen tietohallintalaissa käytetty *tietoturvallisuustoimenpiteet* -käsite on hyvä lisäys tietoturvan sääntelyjärjestelmän käsitteistöön, koska se kuvaa yksinkertaisesti ja tiivistetysti kaiken tarpeellisen: tietoturvatoimenpiteillä suojataan organisaation luottamuksellisia tietoja sekä näiden luottamuksellisuutta, eheyttä ja saatavuutta. Kyseistä käsitettä on myös konkretisoitu tietoturvan osa-alueilla, jotka tosin eivät vastaa hyviä käytänteitä, sillä osa-alueissa ei ole mukana fyysisiä toimenpiteitä vaan toiminnalliset toimenpiteet. Toiminnalliset toimenpiteet lisäyksenä ei tuo lisäarvoa käsitteen määrittelyyn ja se tekee tietoturvan sääntelyjärjestelmän käsitteistöstä monimutkaisemman.

3.4.4 Tietoturvatoimenpiteiden käsitteistön yhdenmukaisuus

Kerrattakoon, että tämänhetkisen voimassa olevan lainsäädännön myötä kaikki neljä käsitettä ovat käytössä tietoturvan sääntelyjärjestelmässä:

[790] HE 284/2018 vp: 65–66.
[791] HE 284/2018 vp:149; Voutilainen 2020: 211–212; Voutilainen 2023: 276.

1) Tekniset ja organisatoriset toimenpiteet – muun muassa teledirektiivi ja tietosuojalainsäädäntö.

2) Hallinnolliset ja tekniset toimenpiteet – laki sähköisen viestinnän palveluista (917/2014).

3) Hallinnolliset, toiminnalliset ja tekniset toimenpiteet eli tietoturvallisuustoimenpiteet – viranomaisen tiedonhallintalaki (906/2019).

4) Tekniset, operatiiviset ja organisatoriset toimenpiteet eli kyberturvallisuusriskien hallintatoimenpiteet – NIS 2 -direktiivi ja sen implementoiva kansallinen kyberturvallisuuslaki. Myös tiedonhallintalain uudessa 4a-luvun 18 c §:ssä tullaan käyttämään tätä määritelmää[792].

EU-lainsäädäntöuudistuksien päämääränä on ollut usein tietoturvaa koskevan lainsäädännön yhtenäistäminen unionissa. Kansallisen tietoturvalainsäädännön yhtenäistämiseksi ja hyvän tietoturvatavan kehittämiseksi tulisi ottaa käyttöön tietoturvan sääntelyjärjestelmän käsitteistöön vain yksi vaihtoehto. Se, että käytössä olisi yksi käsite, ei estäisi kuitenkaan käsitteen sisällön määrittelemistä monipuolisemmin sekä laajempaa tietoturvan ulottuvuuksien huomioimista. Tämä ei tarkoita tarkkojen teknisten vaatimuksien lisäämistä, vaan enemminkin lainsäädännön teknologianeutraalisuus sekä hyvät tietoturvakäytänteet huomioon ottaen toimenpide-ehdotusten yhtenäistämistä säädösten ja lain esitöiden pohjalta.

Nykyisessä tietoturvan sääntelyjärjestelmässä ilmenevät eri käsitteet eri säädöksissä tekevät tietoturvalainsäädännöstä epäjohdonmukaista ja epäyhtenäistä sekä hankaloittavat sen ymmärrettävyyttä. Mainittujen käsitteiden määrittelyssä ei ole nojauduttu tarpeeksi hyviin käytänteisiin tai alan sanastoon, jota tietoturva-ammattilaiset käyttävät päivittäisessä työssään. Miksi lainsäätäjät haluavat kehittää jotain uutta käsitettä, jos tietoturvan käytännesäännöissä yleisesti puhutaan tietoturvatoimenpiteistä ja tietoturvan ulottuvuuksina ovat hallinnollinen, fyysinen ja tekninen tietoturva? Yksi syy voi olla kapea englannin kielen kääntäminen, jossa ei ole huomioitu alan sanastoa. Esimerkiksi englanninkielinen tietosuoja-asetus on huomioinut tietoturvan ulottuvuuksista hallinnollisen tietoturvan osa-alueen: tietoturvan osa-alueista hallinnollisen tietoturvan kontrollit eli *”organizational controls”* vastaavat samalla tasolla englanniksi tietosuoja-asetuksen toimenpiteitä *”organizational measures”*. Valitettavasti tietosuoja-asetuksen suomenkielisessä käännöksessä tietoturvaan liittyvää alan käsitteistöä ei ole huomioitu vaan hallinnollisen (tietoturva)toimenpiteen sijaan on käännetty suoraan suomeksi organisatoriset toimenpiteet. Taustalla vaikuttaa todennäköisesti myös kumotun

[792] HE 57/2024 vp: 301–302, 336.

henkilötietolain (523/1999) historia, sillä kyseisessä säädöksessä käytettiin käsitteenä organisatorista toimenpidettä. Näin ollen historiallisista seikoista johtuen kansallisessa tietosuojalainsäädännössä ei ole huomioitu hyviä tietoturvakäytänteitä käsitteistön osalta. Se ei kuitenkaan tarkoita sitä, etteikö tulevaisuudessa asiaa voisi korjata ja käsitteistöä yhtenäistää kansallisessa tietoturvan sääntelyjärjestelmässä. Esimerkiksi NIS 1 ja 2 -direktiiveissä yhtenä keskeisenä käsitteenä on *verkko- ja tietojärjestelmä*, mutta kansallisella tasolla on päädytty eriävään käsitteeseen ja pitäydytty esimerkiksi kyberturvallisuuslain osalta käsitteessä *viestintäverkko- ja tietojärjestelmä*[793].

Hyvässä tietoturvan sääntelyjärjestelmässä yleinen ja yhdenmukainen käytettävä käsite voisi vallan hyvin olla *”tietoturvatoimenpiteet”,* joka EU-yhtenäisyyden lisäämiseksi tarkemmin määriteltynä sisältäisi hallinnolliset (*organizational*) ja tekniset toimenpiteet. Vieläkin parempi olisi, jos tietoturvatoimenpiteen käsitettä lähennettäisiin enemmän käytännön työn kanssa, jolloin ”*tietoturvatoimenpiteet”* yksinkertaisemmin määriteltynä sisältäisi hallinnolliset, fyysiset ja tekniset toimenpiteet.[794]

Tietoturvatoimenpidekäsitteen määrittelyssä tulisi tukeutua tietosuoja-asetuksen kattavaan teknisten ja organisatoristen toimenpiteiden määritelmään, mutta näkökulmana ei olisi ainoastaan henkilötietojen suojaaminen vaan kokonaisuudessaan organisaatioiden liikesalaisuuksien sekä muiden luottamuksellisten tietojen suojaaminen. Tietoturvatoimenpidekäsitteen sisältöön voisi toimenpiteinä lukeutua esimerkiksi riittävä dokumentointi[795], tietoturvariskien hallinta, kyky taata palveluiden, laitteiden sekä järjestelmien luottamuksellisuus[796], eheys, käytettävyys ja vikasietoisuus, kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin (varmuuskopiointi), fyysisen turvallisuuden huomioiminen luottamuksellisten tietojen suojaamiseksi, henkilökunnan ohjeistus, koulutus, testaus, henkilökunnan roolien ja vastuiden määrittely sekä mahdollisesti tunnettujen tietoturvallisuusstandardien noudattaminen ja tietoturvatoimenpiteiden tehokkuuden arvioiminen säännöllisesti esimerkiksi auditoimalla. Tietoturvatoimenpiteet tulisi suhteuttaa organisaation verkkojen, järjestelmien, palveluiden, toimitilojen (ja etätyön) tietoturvallisuuteen ja jatkuvuuteen kohdistuvan riskin tasoon nähden

793 HE 57/2024 vp: 144–145.
794 Ks. myös vastaavaa pohdintaa luvusta 2.2.1 (”Tietoturva”).
795 Muun muassa huomioon ottaen minimissään tietosuoja-asetuksen dokumentointivaatimukset, jatkuvuus- ja toipumissuunnittelu sekä tarvittavat henkilökunnan tietoturvaohjeistukset.
796 Esimerkiksi tietosuojalain 6 §:stä johdettuna asianmukaiset, riskiperusteiset toimenpiteet, joilla estetään pääsy luottamuksellisiin tietoihin ja joilla on jälkeenpäin mahdollista varmistaa, kenen toimesta luottamuksellisia tietoja on muokattu, siirretty, poistettu tai katseltu.

huomioon ottaen uusin tekniikka. Yhtä lailla nämä voisivat olla tietoturvan yleislaissa kaikkia organisaatioita velvoittavia tietoturvan vähimmäisvaatimuksia.

Eräänä kritiikkinä tiedonhallintalain tietoturvallisuustoimenpiteet käsitteelle on esitetty, että edeltäjiensä tavoin tiedonhallintalain määritelmästä puuttuu maininta oikeudellisista toimista tietoturvan toteuttamisessa eli lainsäätäjä on unohtanut itse itsensä[797]. Koska säädös tähtää tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen viranomaisorganisaatiossa, on epäselvää, miten oikeudelliset toimet tietoturvallisuustoimenpiteinä parantaisivat organisaatioiden tietoturvatasoa esimerkiksi proaktiivisesti. Lähinnä tällainen ”oikeudellinen”, proaktiivinen tietoturvallisuustoimenpide voisi olla *compliance*-tyyppinen toiminta eli toimiminen lakien ja sidosryhmävaatimusten mukaisesti. Tähän tyypillisesti liittyy myös organisaatiossa tehtävä sisäinen (tietoturva)tarkastus, itsearvioinnit ja kolmannen osapuolten tekemät auditoinnit ja tarkastukset. Tällainen toiminta kuuluu käytännön tasolla yleensä hallinnollisen tietoturvallisuuden osa-alueelle. Huomioitava on myös se, että tiedonhallintalaissa on vahva viranomaispainotus lain soveltamisen osalta. Oikeudelliset toimet osana hallinnollisia tietoturvatoimenpiteitä tulisi ottaa huomioon yleisen tietoturvalainsäädännön tasolla kattavammin. Tällaisen *compliance*-tyyppisten vähimmäisvaatimuksien hyvänä esimerkkinä toimii kansallisen tietosuojalain 6 §:n 2 momentissa ilmaistu menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Yhteenvetona todettakoon, että organisaatioiden tietoturvan sääntelyjärjestelmässä tietoturvatoimenpiteitä kuvaavat käsitteet ja niihin liittyvät täsmennykset ovat moninaisia eivätkä ne ole täysin hyvien käytänteiden mukaisia. Esimerkiksi *hallinnolliset, toiminnalliset ja tekniset toimenpiteet* sekä t*ekniset, operatiiviset ja organisatoriset toimenpiteet* -käsitteet jäävät toiminnallisten ja operatiivisten toimenpiteiden osalta riittämättömästi kuvatuiksi eivätkä ne vastaa hyviä käytänteitä. Myös organisatoriset toimenpiteet käsitteenä ei ole hyvien käytänteiden mukainen, mutta se on vakiintunut erityisesti tietosuojalainsäädäntöön ja -ohjeistuksiin. Yksinkertaisimmillaan käytännön työssä tietoa suojataan hallinnollisilla, fyysisillä ja teknisillä tietoturvatoimenpiteillä. Näin ollen nykyisessä tietoturvan sääntelyjärjestelmässä ilmenevät eri käsitteet tekevät tietoturvalainsäädännöstä epäjohdonmukaista ja epäyhtenäistä, jolloin se on myös vaikeammin ymmärrettävää. Käsitteistön kehitys on ollut jatkuvasti parempaan suuntaan kansallisella tasolla esimerkiksi tiedonhallintalain myötä, jossa käytetään ylätason käsitettä *tietoturvallisuustoimenpiteet* kuvaamaan eri toimenpiteitä tiedon suojaamiseksi.

---

[797] Saarenpää & Riekkinen 2023: 201.

Lainsäädännön käsitteitä määriteltäessä ja kuvatessa tulisi tukeutua käytännesääntöihin ja alan sanastoon, jotta säädökset olisivat johdonmukaisia, tavoitettavia ja ymmärrettäviä, ja jotta kuilu käytännön työn ja lainsäädännön välillä ei kasvaisi suureksi. Organisaatioiden hyvässä tietoturvan sääntelyjärjestelmässä hyvien käytänteiden mukainen käsite olisi ”*tietoturvatoimenpiteet*”, ja se huomioisi kaikki kolme tietoturvan osa-aluetta eli hallinnolliset, fyysiset ja tekniset toimenpiteet. Käsitteen määrittelyssä voisi tukeutua erityisesti tietosuoja-asetuksessa ilmeneviin tietoturvatoimenpiteisiin (teknisten ja organisatoristen toimenpiteiden määritelmään), mutta näkökulmana olisi laajemmin luottamuksellisten tietojen suojaaminen. Lisäksi tietoturvatoimenpiteet tulisi suhteuttaa organisaation verkkojen, järjestelmien, palveluiden ja toimitilojen tietoturvallisuuteen ja jatkuvuuteen kohdistuvan riskin tasoon nähden huomioon ottaen uusin tekniikka.

3.5 Työelämän tietosuoja ja tietoturva osana tietoturvan sääntelyjärjestelmää

3.5.1 Yleistä työelämän tietosuojalainsäädännön tietoturvavaatimuksista

Tietoturvatoimenpiteitä suunnitellessaan ja toteuttaessaan organisaatioiden tulee huomioida myös työntekijöidensä tietosuoja organisaation keskeisinä rekisteröityinä sekä työntekijöiden henkilötietoihin liittyvät käsittelysäännöt.

Suomen lainsäädännössä työntekijöiden henkilötietojen käsittelyä sekä yksityisyyttä sääntelee laki yksityisyyden suojasta työelämässä (YksTL 759/2004) eli työelämän tietosuojalaki. Työelämän tietosuojalakia sovelletaan työntekijän lisäksi virkamiehiin, virkasuhteessa oleviin henkilöihin sekä soveltuvin osin myös työnhakijaan. Työnhakijan, työntekijän ja virkamiehen yksityisyyden suojaan kuuluu mahdollisimman suuri oikeus tietää ja päättää omien henkilötietojensa käsittelystä ja sisällöstä sekä oikeus tulla arvioiduksi oikeiden tietojen perusteella[798]. Työelämän tietosuojalain noudattamista valvovat työsuojeluviranomaiset yhdessä tietosuojavaltuutetun kanssa. Työnantajan tai tämän edustajan rikkoessa tai toimiessa vastoin tiettyjä työelämän tietosuojalain säännöksiä joko tahallaan tai törkeästä huolimattomuudesta on tuomittava sakkoon, jollei teosta muualla laissa säädetä ankarampaa rangaistusta. Huomioitava kyseisen säädöksen osalta on se, että riskilähtöisyys ei ole työelämän tietosuojalain ohjaavana tekijänä toisin kuin se on tietosuoja-asetuksessa eikä yleinen tietosuoja-asetus ole velvoittanut jäsenvaltioita tekemään muutoksia työntekijöiden henkilötietojen käsittelyä koskevaan

[798] Koskinen & Ullakonoja 2020: 91–92.

lainsäädäntöön. Yleisen tietosuoja-asetuksen 88 artiklassa on mainittu, että jäsenvaltiot voivat antaa lainsäädännössä tai työehtosopimuksien kautta yksityiskohtaisempia sääntöjä koskien työntekijöiden henkilötietojen käsittelyä.

Työelämän tietosuojalain tarkoituksena on suojata yksityisyyttä työelämässä työnantajan direktio-oikeudesta huolimatta. Direktio-oikeus on johdettu työsopimuslaista, eli työtä tehdään työnantajan johdon ja valvonnan alaisena, jolloin näin ollen työnantajalla on oikeus muun muassa valvoa työntekijää, määritellä tietojärjestelmiensä ja sähköpostinsa käyttö sekä määrätä työnteon aika, paikka ja suoritustapa[799]. Perusoikeuksia on kuitenkin kunnioitettava työpaikallakin, eli työnantajalla ei ole näin ollen yleistoimivaltaa[800]. Kuitenkin työsopimuslain lojaliteettivelvoitteen mukaan työntekijän on tehtävä työnsä huolellisesti noudattaen niitä määräyksiä, joita työnantaja antaa toimivaltansa mukaisesti työn suorittamisesta[801]. Lojaliteettivelvollisuus on käyttäytymisvelvollisuutta[802]. Tähän liittyy myös tietoturvallisesti toimiminen työssä sekä maalaisjärjen että tietoturvaohjeiden mukaisesti työskennellen.

Työntekijöiden henkilötietoja koskee tarpeellisuusvaatimus, aivan kuten perinteisiä rekisteröityjen henkilötietojakin. Tarpeellisuusvaatimus on ehdoton, eli siitä ei voida poiketa edes työntekijän suostumuksella. Työelämän tietosuojalain 3 §:n mukaan työnantaja saa käsitellä vain välittömästi työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen, johtuvat työtehtävien erityisluonteesta taikka liittyvät työntekijöille tarjoamiin etuuksiin. Tarpeellisia tietoja ovat esimerkiksi työtehtävien suorittamiseen, työntekijän valintaan, työolosuhteisiin, työ- ja virkaehtosopimusten määräysten noudattamiseen liittyvät tiedot sekä työtehtävien erityisluonteeseen liittyvät tiedot, mutta myös mahdollisesti tiedot, jotka koskevat työnantajan tarjoamia etuuksia[803]. Tarpeellisuusvaatimuksella on pyritty varmistamaan työntekijöiden

---

[799] Innanen & Saarimäki 2012: 155. Työntekijälle puolestaan työsopimus perustaa oikeuden saada palkkaa tai muuta vastiketta siitä, että hän on tehnyt työsopimuksen edellyttämää työtään (Koskinen & Ullakonoja 2020, s. 17). Tietoturvavastuiden ja tietoturvaohjeiden mukaisesti toimimisen velvoittavuuden ulottaminen työsopimuksiin on tärkeää, ks. lisää työsuhteen salassapitovelvoitteista luvusta 3.5.6 (”Henkilöstöturvallisuus: työntekijöiden luotettavuus ja tiedon salassapito”) sekä työntekijöiden tietoturvavastuiden ulottamisesta työsopimuksiin luvusta 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).

[800] Saarenpää 2015: 380.

[801] Työsopimuslain 3. luvun 1 §:n mukaan työntekijän on tehtävä työnsä huolellisesti sekä noudattaa niitä määräyksiä, joita työnantaja antaa toimivaltansa mukaisesti työn suorittamisesta. Lisäksi työntekijän on toiminnassaan vältettävä kaikkea, mikä on ristiriidassa hänen asemassaan olevalta työntekijältä kohtuuden mukaan vaadittavan menettelyn kanssa.

[802] Pesonen 2017: 261.

[803] Koskinen & Ullakonoja 2020: 94.

ja työnhakijoiden riittävä yksityisyyden suojan taso[804]. Vaikkakin työelämän tietosuojalaissa korostetaan, että kerättyjen henkilötietojen on oltava *välittömästi* työntekijän työsuhteen kannalta tarpeellisia, tietosuoja-asetuksessa puhutaan vain pelkästä tarpeellisuudesta. Täten on tulkittu, että nämä käsitteet ovat saman sisältöisiä, sillä tietosuoja-asetuksen keskeisiä periaatteita ei voida muuttaa kansallisella lainsäädännöllä. Näin ollen tällaisen tulkinnan mukaan kansalliset säännökset voivat olla yksityiskohtaisempia, mutta ei tiukempia.[805] Edellä oleva tulkinta on kuitenkin kritiikille altis. Tietosuoja-asetuksen 88 artiklan mukaan jäsenvaltiot voivat antaa yksityiskohtaisempia säännöksiä koskien työntekijöiden henkilötietojen käsittelyä. Ei ole kuitenkaan yksiselitteistä tulkintaa siitä, missä määrin tietosuoja-asetuksen 88 artikla oikeuttaa korottamaan rekisteröidyn suojaa verrattuna asetukseen ja miltä osin säännökset voivat olla tiukempia kuin asetuksen säännökset. Työelämään liittyy kuitenkin erityisiä tilanteita, jotka poikkeavat muusta tietojen käsittelystä, jolloin työelämän tietosuojalaki voidaan artiklan 88 ja erityisiä henkilötietoja koskevan 9 artiklan nojalla pitää pääosin sellaisenaan.[806] Työntekijät ovat lähtökohtaisesti katsottu olevan heikossa asemassa olevia rekisteröityjä[807]. Lisäksi työelämän tietosuojalain nimenomainen tarkoitus on antaa parempaa suojaa työntekijöille. Edellä olevat seikat huomioon ottaen on vähintäänkin perusteltua, että yksityiskohtaisempi säännös voi olla yhtä lailla tässä kontekstissa tiukempi. Usein yksityiskohtaisempi sääntely luonnollisesti johtaa tiukempaan sääntelyyn.

Työntekijöiden henkilötietojen keräämiseen liittyy myös muita vaatimuksia kuin tarpeellisuusvaatimus. Työelämässä henkilötietojen ja yksityisyyden suojaa on rakennettu tiedollisen itsemääräämisoikeuden varaan, jolloin esimerkiksi työelämässä käsiteltävien henkilötietojen tulee pääsääntöisesti olla joko työntekijän työnantajalle toimittamia tai joiden hankkimisesta työnantajan on informoitava työntekijää[808]. Näin ollen lain mukaan henkilötiedot on ensinnäkin kerättävä ensisijaisesti työntekijältä itseltään. Mikäli näin ei tapahdu, työntekijältä on hankittava suostumus tietojen keräämiseen. Tähänkin liittyy poikkeus: työntekijän suostumusta ei tarvita, jos viranomainen luovuttaa tietoja työnantajalle työelämän tietosuojalaissa säädetyn tehtävän suorittamiseksi taikka, kun työnantaja hankkii henkilöluottotietoja työntekijän luotettavuuden selvittämiseksi. Tällöinkin

[804] Alapuranen 2020: 80–81; HE 75/2000 vp: 3.
[805] Nyyssölä 2018: 36.
[806] HE 97/2018 vp: 9.
[807] Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 12.
[808] Neuvonen 2014: 66–67.

työnantajan on ilmoitettava työntekijälle etukäteen tietojen hankkimisesta luotettavuuden selvittämistä varten.[809]

Organisaation hyviä tietoturvallisia toimitapoja suunniteltaessa ja toteuttaessa tulee ottaa joillakin osa-alueilla myös huomioon työntekijöiden tietosuojalainsäädäntö ja sen vaatimukset. Esimerkiksi mikäli fyysinen tietoturvallisuus on huomioitu organisaation toiminnassa riittävällä tasolla, etenkin suuremmissa organisaatioissa monitasoinen fyysinen turvallisuus sisältää mitä todennäköisemmin tilojen valvonnan kameravalvonnalla ja kulunvalvonnalla. Työntekijöihin kohdistuva työasemien ja internetin käytön valvonta osana teknisen tietoturvallisuuden toteuttamista on myös seikka, jossa tulee ottaa huomioon työntekijöiden yksityisyys ja henkilötietojen käsittely. **Tietosuojavaltuutetun lausunnon 4.9.2015 (dnro. 1661/41/2014)** mukaisesti valvonnan toteuttamisessa tulee ottaa huomioon erityisesti työelämän tietosuojalain 3 §:n tarpeellisuusvaatimus:

> *Kiinteistöjen kulunvalvonnan osalta kyseeseen voivat tulla organisaation tietoturvallisuuteen, asiakaspalveluun ja muuhun turvallisuuteen liittyvät asianmukaiset henkilötietojen käsittelyn tarkoitukset. Valvonnan toteuttamisessa tulee ottaa huomioon erityisesti työelämän tietosuojalain tarpeellisuusvaatimus sekä työntekijöille on tiedotettava valvonnan tarkoituksesta, käytettävistä menetelmistä sekä käyttöönotosta.*

Esimerkiksi kameravalvonnan käyttö työpaikalla lisää tietoturvallisuutta ja se voi olla tunnistettu riskien arvioinnissa tarpeelliseksi riskien mitigointikeinoksi. Samalle se kuitenkin rajoittaa työntekijöiden yksityisyyttä, minkä vuoksi sen käytöstä on säädelty erikseen työelämän tietosuojalaissa.

Työelämän tietosuojalain soveltamisalaa koskevan 2 §:n mukaan laissa säädetään teknisestä valvonnasta työpaikalla, mutta teknistä valvontaa tai teknisin menetelmin toteutettavaa valvontaa ei ole käsitteenä määritelty kyseisessä lainsäädännössä. Esimerkkinä on kuitenkin mainittu lain 21 §:n mukaisesti kameravalvonta ja kulunvalvonta.[810] Huomioitava on, että työelämän tietosuojalain 21 §:ssä käytetään nimenomaan ilmaisua *”teknisin menetelmin toteutettu valvonta”* erotuksena ilmaisusta *”tekninen valvonta”*, joka on poliisille kuuluva oikeus poliisilain (872/2011) 4 luvun sekä pakkokeinolain (806/2011) 2 luvun mukaisesti[811].

Yhteenvetona todettakoon, että työelämän tietosuojalaki on merkittävä laki suunniteltaessa ja toteuttaessa organisaation järjestelmällistä, teknisin menetelmin toteutettua (tietoturva)valvontaa: työntekijät ovat keskeisiä organisaation

[809] HE 97/2018 vp: 18, 25.
[810] Alapuranen 2020: 102–103; Nyblin 2009: 23.
[811] PeVL 10/2004 vp: 6; Nyblin 2008: 542.

rekisteröityjä. Tietosuojan näkökulmasta työntekijät ovat myös heikossa asemassa ja tällöin työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, eikä tästä voi joustaa edes työntekijän suostumuksella. Lisäksi henkilötiedot on lähtökohtaisesti kerättävä ensisijaisesti työntekijältä itseltään, mutta mikäli näin ei tapahdu, työntekijältä on hankittava suostumus tietojen keräämiseen. Työnantajan direktio-oikeudesta huolimatta työntekijöillä on oikeus yksityisyyteen eli yksityiselämän suojaan, henkilötietojen suojaan sekä viestinnän luottamuksellisuuteen. Työnantajalla on kuitenkin muun muassa oikeus ohjeistaa ja valvoa työntekijöitä sekä määritellä työnantajan omaisuuden käyttö esimerkiksi tietojärjestelmien, laitteiden ja työnantajalle kuuluvien sähköpostien osalta. Tämä saattaa osaltaan heikentää luottamuksellisen viestinnän suojaa, mutta myös työntekijöiden sananvapautta[812]. Tietosuoja- ja tietoturvariskien pienentämiseksi työnantajan olisi hyvä painottaa, että työnantajan tarjoamat työvälineet on tarkoitettu lähtökohtaisesti vain työn tekemiseen. Työntekijän lojaliteettivelvoitteen myötä työntekijän on tehtävä työnsä huolellisesti noudattaen työnantajan määräyksiä ja ohjeistuksia, johon lukeutuu myös tietoturvallisesti toimiminen tietoturvaohjeiden mukaisesti[813]. Huomioitava on, että työsuhteen päättymisen myötä moni laillinen käsittelyperuste työntekijän henkilötiedoille päättyy.

3.5.2 Kameravalvonta

Fyysinen tietoturvallisuus on yksi osa-alue osa organisaatioiden tietoturvaa. Kameravalvonta on yksi fyysistä tietoturvallisuutta parantava suojakontrolli. Tietoturvan sääntelyjärjestelmässä kameravalvonnan osalta keskeisin säädös on työelämän tietosuojalaki ja erityisesti sen luku 5, jossa on koottuna yksityiskohtaiset säännökset liittyen kameravalvontaan työpaikalla[814].

Työelämän tietosuojalain 16 §:n mukaan työnantaja saa käyttää kameravalvontaa tiloissaan työntekijöiden ja muiden tiloissa oleskelevien henkilöiden turvallisuuden varmistamiseksi, omaisuuden suojaamiseksi tai tuotantoprosessien asianmukaisen toiminnan valvomiseksi sekä turvallisuuteen, omaisuuteen tai tuotantoprosessiin kohdistuvien vaaratilanteiden ennaltaehkäisemiseksi tai selvittämiseksi. Tämä käytännössä kattaa tietoturvaperusteisen kameravalvonnan, jolla suojataan

[812] Ks. 2.5.3 (”Yksityisyys: yksityiselämän, henkilötietojen ja viestin suoja”) sekä 2.5.4 (”Sananvapaus ja tietoturva”).
[813] Vastaavaa on todettu myös luvussa 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”): jokaisen työntekijän tulee noudattaa työssään tietoturvaohjeita sekä tunnistaa tietoturvavastuunsa.
[814] Huomioitava on myös, että kameravalvontaan liittyy suoraan ja epäsuorasti myös muita säädöksiä, kuten yhteistoimintalaki (1333/2021), työturvallisuuslaki (738/2002), laki yksityisistä turvallisuuspalveluista (1085/2015), tietosuojalaki (1050/2018) ja rikoslaki (39/1889). Näistä säädöksistä ks. tarkemmin: Paasonen & Luomala 2021 – Kameravalvonta tutkimus ja sääntelykohteena.

organisaation fyysisissä tiloissa olevaa omaisuutta sekä vahingontekoa, joka vaikuttaisi organisaation kyberturvallisuuteen.

Kameravalvonnalla tarkoitetaan jatkuvasti kuvaa välittävän tai kuvaa tallentavan teknisen laitteen käyttöön perustuvaa valvontaa. Tähän liittyy sekä kuvaaminen että katseleminen, jolloin myös internettiin tai puhelimiin liitettyjen toimintojen kautta välittyvät näköiskuvat henkilöstä luetaan työelämän tietosuojain 16 §:n piiriin. Säännös rajaa ulkopuolelle työntekijän kuuntelun teknisellä laitteella, sillä rikoslain salakuuntelua koskevat tunnusmerkistöt kattavat työelämän. Jos kuvaamiseen tai katseluun liittyy ääntä, salakuuntelua koskevan rikoslain säännöksen (RL 24 luku 5 §) lisäksi sovelletaan työelämän tietosuojalain 16 §:ä.[815] Työelämän tietosuojalaki määrittelee sallitun kameravalvonnan rajat työpaikalla, jolloin se rajaa ulos myös rikoslain mukaisen salakatseluun liittyvän kameravalvonnan työpaikalla[816]. Täsmennettäköön: mikäli valvontakameralla kuvaaminen täyttää salakatselurikoksen tunnusmerkistön, tapaukseen sovelletaan kuitenkin sitä. Salakatselua koskeva rangaistussäännös ja tietosuojarikos eivät myöskään sulje toisiaan pois. Työelämän tietosuojalain kameravalvontaa koskeva sääntely täsmentää, mutta ei syrjäytä salakatselun tunnusmerkistöä. Työelämän tietosuojalain 16–17 ja 21 §:ssä tarkoitetulla tavalla oikein suunniteltu, käyttöönotettu ja toteutettu kameravalvonta on sallittua.[817] Esimerkiksi salakatseluun (RL 24 luku 6 §) voisi vastakohtaisesti syyllistyä, jos organisaation työtiloissa ei ole noudatettu työelämän tietosuojalain säännöksiä ja oikeudettomasti kuvataan tai katsellaan teknisellä laitteella ei-julkisissa tiloissa[818] oleskelevaa henkilöä tämän yksityisyyttä loukaten.

Kameravalvonnan avulla työntekijöistä kerättävät kuvat ja ääni ovat tietosuoja-asetuksessa ja työelämän tietosuojalaissa tarkoitettuja henkilötietoja, jotka yleensä muodostavat henkilörekisterin. Työnantaja toimii yleensä tämän henkilörekisterin rekisterinpitäjänä, tosin henkilötietojen käsittely ja kameravalvonta on voitu ulkoistaa.[819] Myös reaaliaikainen kuvayhteys on henkilötietojen käsittelyä, sillä se merkitsee yhtäältä joko tietotekniselle alustalle kiinnittämistä ja siten tallentamista tai vaihtoehtoisesti tietojen käyttöä. Tietosuojavaltuutettu on tosin ollut tulkinnoissaan varovainen ja todennut vain tallentavan kameravalvonnan olevan henkilötietojen käsittelyä ja, että säilytysajalla ei ole vaikutusta. Euroopan

[815] HE 162/2003 vp: 48–49.
[816] Nyblin 2009: 34; HE 162/2003 vp: 33, 49.
[817] Frände, Korkka-Knuts & Wahlberg 2023: 435, 438. Valvontakameralla tapahtuvaa salakatselua on esimerkiksi toimistorakennuksen sisäänkäyntiä valvova valvontakamerajärjestelmä, jonka käyttö suuntautuu samanaikaisesti vastapäisen asuintalon huoneiston ikkunoihin (Frände, Korkka-Knuts & Wahlberg 2023, s. 438).
[818] Kuten esimerkiksi rikoslain 24 luvun 3 §:n mukaisesti virastossa, liikehuoneistossa, toimistossa, kokoustilassa, tuotantolaitoksessa taikka muussa vastaavassa huoneistossa tai rakennuksessa.
[819] Alapuranen 2020: 118–119.

tietosuojaneuvoston ohjeissakaan ei todeta suoraan reaaliaikaisen valvonnan olevan henkilötietojen käsittelyä, mutta ohjeissa on täsmennetty, että tallentavan ja reaaliaikaisen valvonnan välisen valinnan pitäisi perustua tavoiteltuun tarkoitukseen.[820] Tietosuoja-asetuksen mukaisesti henkilötietojen käsittelyksi katsotaan esimerkiksi tietojen käyttö ja siirtäminen. Reaaliaikaisessa kameravalvonnassa henkilön kuva yleensä esimerkiksi siirretään teknisesti valvontakamerasta[821] tallentimelle ja siitä suojattua nettiyhteyttä pitkin saataville valvomomonitoriin, jossa poikkeuksia lukuun ottamatta vartijan tai muun relevantin työntekijän tulisi seurata tätä reaaliaikaista kuvaa[822]. Tällainen video- tai bittivirran siirtäminen on viimeistään silloin henkilötiedon käsittelyä, kun kuva muodostuu valvomomonitoriin (tai jos se on siirretty tallentimelle ennen valvomomonitoria). Tätä tietoa voidaan käyttää muun muassa henkilön käyttäytymisen arvioinnissa. Näin ollen myös reaaliaikainen kameravalvonta on sen mahdollistamien henkilötietojen käsittelyä.

Pääsääntöisesti kameravalvontaa ei saa käyttää tietyn työntekijän tai työntekijäryhmän tarkkailuun, jolloin esimerkiksi kameravalvonnan käyttö on kiellettyä työntekijöiden henkilökohtaisissa työhuoneissa taikka kohdentaen tiettyyn työpisteeseen. Oleellista lain tulkinnan kannalta on, että näissä työskentelypisteissä työskentelee tietty työntekijä taikka tietyt työntekijät. Myös pukeutumistilojen, käymälöiden ja muiden henkilöstötilojen kameravalvonta ei ole sallittua. Tähänkin liittyy kuitenkin poikkeus. Työelämän tietosuojalain 16 § 2 momentin mukaisesti työnantaja voi kohdentaa kameravalvonnan tiettyyn työpisteeseen, jos tarkkailu on välttämätöntä a) työntekijän työhön liittyvän ilmeisen väkivallan uhkan tai hänen turvallisuudelleen tai terveydelleen ilmeisen haitan tai vaaran ehkäisemiseksi; b) omaisuuteen kohdistuvien rikosten ehkäisemiseksi ja selvittämiseksi, jos työntekijän olennaisena tehtävänä on käsitellä merkittävää arvo- tai laatuomaisuutta; taikka c) työntekijän etujen ja oikeuksien varmistamiseksi ja kameravalvonta perustuu tällöin tarkkailun kohteeksi tulevan pyyntöön. Työntekijän pyyntöön perustuva c-kohdan valvonta on lakkautettava, jos työntekijä sitä esittää. Mikäli työnantajalla on kuitenkin lakkauttamispyynnöstä huolimatta edelleen tarve toteuttaa kameravalvontaa, on tämä mahdollista kohdentaa tiettyyn työpisteeseen

[820] Saarenpää & Riekkinen 2023: 268–269; Euroopan tietosuojaneuvoston (EDPB) ohje 3/2019: 11.
[821] Valvontakameroita on yleensä kahden tyyppistä: Analogisia kameroita ja IP-kameroita. Analoginen kamera siirtää kuvan analogisena videovirtana koaksiaalikaapelia pitkin tallenninlaitteelle tai tarkkailumonitorille. IP-kamera muuttaa kuvainformaation digitaaliseksi bittivirraksi, jonka avulla kuva siirtyy tietoverkkoa pitkin tallenninlaitteelle. Kuvan digitalisointia varten IP-kamerassa on mm. erilaisia ohjelmia kuvan pakkaamista ja katselemista varten. Ks. Sallinen 2010, s. 20.
[822] Lisää kameratyyppien ja tallentimien eroista sekä esimerkkejä teknisten toteutusten havaintokuvista, ks. myös Sallinen 2010, s. 22–25.

a tai b-kohtien edellytysten täyttyessä.[823] Tällöin tulee olla kuitenkin erityisen tarkka työelämän tietosuojalain 16 § 2 momentin tosiasiallisten poikkeusedellytysten täyttymisen suhteen. Esimerkiksi jos sisällöllisenä perusteena käyttää edellä mainitun a-kohdan työntekijöiden työhön liittyvää ilmeistä väkivallan uhkaa, mutta tällaista ei todellisuudessa ole ollut, vaan kohdennettuja valvontakameroita on käytetty mahdollisten irtisanomisperusteiden itsenäiseksi selvittämiseksi, työnantaja rikkoo työelämän tietosuojalain säännöksiä[824]. Näin ollen salakatselun tunnusmerkistö täyttyy, mikäli kuvaaminen ja tallentaminen on tapahtunut työntekijöiden yksityisyyttä loukaten eikä työelämän tietosuojalain säännöksiä ole noudatettu. Pitkäaikaista sekä tiettyyn henkilöön tai tiettyihin henkilöihin kohdistuvaa kameravalvontaa työpaikalla voidaan pitää avoimestikin toteutettuna henkilöiden yksityisyyttä loukkaavana.[825]

Työelämän tietosuojalain 17 §:n mukaan työnantajan tulee kiinnittää huomiota avoimuuteen suunnitellessaan ja toteuttaessaan kameravalvontaa työpaikalla. Kameravalvonnan lähtökohtina onkin avoimuus ja valvonnan rajoittaminen välttämättömään[826].

Avoimuusperiaate sisältää velvoitteen sekä informoida kameravalvonnasta että tiedottaa kameravalvonnan toteuttamisesta. Suomessa tällainen avoimuus työpaikalla toteutuu yhteistoimintamenettelyn kautta. Huomioitava on, että **EIT:n ratkaisun Bărbulescu v. Romania 5.9.2017** mukaan informointi valvonnasta ei ole pelkästään riittävää, vaan työntekijän oikeus yksityiselämän suojaan edellyttää myös kertomista valvonnan tarkoituksesta, muodosta, asteesta ja luonteesta.[827] Avoimuusperiaatteen mukaisesti kameravalvonnasta ja sen toteuttamistavasta on ilmoitettava myös näkyvästi niissä tiloissa, joissa on kameroita sijoitettuna[828]. Riittävänä voidaan pitää yleensä tilan kulkuyhteyden läheisyyteen laitettua ilmoitusta siitä, että kohteessa on kameravalvonta sekä onko kamera tallentava[829]. Työntekijöille on myös tiedotettava yhteistoiminta- tai kuulemismenettelyn jälkeen kameravalvonnan alkamisesta, sen toteuttamisesta ja tallenteiden käytöstä sekä työelämän tietosuojalain 16 §:n 2 momentin tarkoittamissa tilanteissa (esimerkiksi omaisuusrikostapausten ehkäisemiseksi) kameroiden sijainnista. Poikkeuksena ovat valvontakamerat yleisissä tiloissa ja asiakaspalvelutiloissa sekä valvontalaitteet, jotka ovat ainoastaan toiminnassa silloin, kun tilassa ei pitäisi olla

[823] HE 97/2018 vp: 20, 31; EV 236/2018 vp: 3; Nyyssölä 2018: 189–190; HE 162/2003 vp: 53.
[824] Frände, Korkka-Knuts & Wahlberg 2023: 439.
[825] HE 184/1999 vp: 230. Frände, Korkka-Knuts & Wahlberg 2023: 438.
[826] Alapuranen 2020: 118–119.
[827] Kurvinen 2019: 203–204, Bărbulescu v. Romania 2017: etenkin kohdat 133, 135, 140 ja 141.
[828] Ks. työelämän tietosuojalain 17 §.
[829] HE 162/2003 vp: 52–53; Frände, Korkka-Knuts & Wahlberg 2023: 437–438.

työntekijöitä[830]. Työpaikoilla tapahtuvan kameravalvonnan osalta on huomioitava myös tietosuoja-asetuksen säännökset koskien henkilötietojen lainmukaisuutta ja rekisteröityjen informointia[831].

Ennen kameravalvonnan käyttöönottoa on myös selvitettävä työntekijöiden yksityisyyteen vähemmän puuttuvien muiden keinojen käyttömahdollisuudet. Kameravalvonnan suunnittelun ja käytön yhteydessä tulee muistaa, että työntekijän yksityisyyteen ei saa puuttua enempää kuin on välttämätöntä toimenpiteiden tarkoituksen saavuttamiseksi. Lisäksi on huomioitava, että tallenteita käytetään vain siihen tarkoitukseen, jota varten tarkkailua on tehty. Katakri 2020 fyysisen tietoturvallisuuden osa-alueen F03-vaatimuksessa on määritelty kameravalvonnan tarkoitukseksi esimerkiksi laittoman tiedustelun ja poikkeamien ennaltaehkäisy, hälytysten todentaminen sekä tapahtuneiden poikkeamien selvittäminen. Katakrin vaatimuksessa on myös todettu, että vartiointihenkilöstö voi käyttää kameravalvontaa aktiivisena reaaliaikaisen kuvan tarkkailuna taikka passiivisena jälkikäteisen kuvamateriaalin analysointina. Lainsäädännöllisestä näkökulmasta valvonnan tarkoituksen määrittelyssä tehdään eräänlaista intressipunnintaa työntekijän oikeuksien ja työnantajan etujen ja lakisääteisten velvoitteiden välillä[832].

Lain mukaan kameravalvontatallenteet on hävitettävä heti, kun ne eivät enää ole tarpeellisia valvonnan tarkoitussidonnaisuuden toteuttamiseksi ja viimeistään vuoden kuluttua tallentamisen päättymisestä. Pidempiaikaisempikin säilyttäminen on mahdollista tarpeen tullen laissa säädetyin perustein[833] tai jos siihen liittyy esimerkiksi muu erityinen syy. Muita syitä voivat olla turvallisuusnormit tai muut työnantajalle kuuluvat velvoitteet[834]. Katakri 2020 F06.2-kulunvalvonnan vaatimuksessa kameravalvontajärjestelmien olisi suositeltavaa olla eurooppalaisten standardien ja niiden vähimmäisvaatimusten mukaisia, jolloin tallenteiden suositeltu säilytysaika olisi vähintään 1 kuukausi. Joka tapauksessa kameravalvontatallenteiden säilytysaika tulisi perustua riskiperusteisesti organisaation poikkeamien havainnointikykyyn.

---

[830] Neuvonen 2019: 260.
[831] Alapuranen 2020: 119.
[832] Kurvinen 2019: 203; ks. myös Bărbulescu v. Romania 2017: Kohdat 127 ja 141.
[833] Tällainen laissa määritelty syy viittaa työelämän tietosuojalain 17 §:n 2 momentin tarkoitetun asian käsittelyn loppuun saattamiseksi, jos se on tarpeen ja asia on tullut selvitettäväksi ennen säilyttämisen enimmäismääräajan loppua. Tällaisia 2 momentin käyttöoikeuksia tallenteille ovat yhteistoimintaneuvotteluiden ja tallenteiden tarkoitussidonnaisuuden estämättä: a) työsuhteen päättämisen perusteen toteennäyttö; b) lakiin perustuvan häirinnän, ahdistelun tai epäasiallisen käytöksen sisältävän toiminnan selvittäminen ja toteennäyttäminen edellyttäen, että työnantajalla on perusteltu syy epäilyksellensä; taikka c) työtapaturman tai muun työturvallisuuslaissa tarkoitetun vaaran tai uhkan aiheuttaman tilanteen selvittäminen.
[834] HE 162/2003 vp: 54.

Tekoälyn laaja-alainen käyttöönotto sekä sen tuomat mahdollisuudet ja haasteet tulevat tulevaisuudessa vaikuttamaan kameravalvontaan liittyvään sääntelyyn. Esimerkiksi jo nyt reaaliaikaisten biometristen etätunnistusjärjestelmien[835] käytöstä on linjattu tekoälysäädöksessä (2024/1689/EU). Tekoälysäädöksessä luonnollisten henkilöiden reaaliaikaiseen ja jälkikäteiseen biometriseen etätunnistukseen käytettäväksi tarkoitetut tekoälyjärjestelmät on luokiteltu suuririskiseksi. Riskitasoltaan korkeimmat käyttötavat kielletään kokonaan ja näitä ovat muun muassa biometrinen etätunnistaminen julkisilla paikoilla reaaliajassa, biometrinen etätunnistaminen jälkeenpäin (lukuun ottamatta viranomaiskäytössä vakavien rikosten tutkimiseksi ja tuomioistuinten ennakkoluvalla), tunteiden tunnistusjärjestelmien käyttö työpaikoilla sekä kasvokuvien ja valvontakameramateriaalin laajamittainen ottaminen kasvojentunnistustietokantojen luomiseksi tai laajentamiseksi[836].

Yhteenvetona voidaan todeta, että kameravalvonnalla tarkoitetaan jatkuvasti kuvaa välittävän tai kuvaa tallentavan teknisen laitteen käyttöön perustuvaa valvontaa. Myös reaaliaikainen kuvayhteys on henkilötietojen käsittelyä, sillä tietosuojaasetuksen mukaista käsittelyä on henkilötietojen siirto ja käyttö. Reaaliaikaisessa kameravalvonnassa henkilön kuva yleensä siirretään valvontakamerasta valvontamonitoriin, jolloin se on henkilötietojen käsittelyä viimeistään siinä vaiheessa, kun kuva muodostuu valvomomonitoriin. Lisäksi reaaliaikaista kuvaa voidaan käyttää luonnollisen henkilön käyttäytymisen arviointiin tai reaaliaikaiseen tunnistamiseen. Työelämän tietosuojalain 16 § mahdollistaa organisaation käyttämän kameravalvonnan tiloissaan muun muassa omaisuuden suojelemiseksi. Tieto on organisaation keskeistä omaisuutta. Näin ollen fyysisen tietoturvallisuuden suojakontrollina kameravalvonta on tarkoitettu kybertoimintaympäristön suojaamiseksi turvallisuuteen tai omaisuuteen liittyvien vaaratilanteiden ennaltaehkäisemiseksi ja selvittämiseksi. Työelämän tietosuojalaki määrittelee myös sallitun kameravalvonnan rajat työpaikalla. Kameravalvonnan on oltava avointa ja siitä tulee informoida työntekijöitä yhteistoimintamenettelyn kautta. Mikäli kameravalvonnassa tapahtuva kuvaaminen ja tallentaminen on tapahtunut työntekijöiden yksityisyyttä loukaten eikä työelämän tietosuojalain säännöksiä ole noudatettu, on mahdollista, että rikoslain mukaisen salakatselun tunnusmerkistö täyttyy. Jos

[835] Tekoälysäädöksen 3 artiklan 41 kohdan määritelmän mukaan biometrisellä etätunnistusjärjestelmällä tarkoitetaan tekoälyjärjestelmää, jonka avulla luonnolliset henkilöt voidaan tunnistaa ilman heidän aktiivista osallistumistaan (tyypillisesti etäältä) vertaamalla henkilön biometrisiä tietoja (esimerkiksi kasvokuvat, sormenjäljet) viitetietokantaan sisältyviin biometrisiin tietoihin. Sen sijaan 42 kohdan mukaan reaaliaikaisella biometrisellä etätunnistusjärjestelmällä tarkoitetaan biometristä etätunnistusjärjestelmää, jossa biometristen tietojen kerääminen, vertailu ja tunnistaminen tapahtuvat ilman merkittävää viivettä ja joka kattaa välittömän tunnistamisen lisäksi myös vähäiset viiveet, joilla pyritään ehkäisemään harhaanjohtamista.

[836] Euroopan parlamentti 2023; ks. myös tekoälysäädöksen 5 artikla.

kuvaamiseen tai katseluun liittyy ääntä, työelämän tietosuojalain 16 §:n lisäksi saattaa tulla sovellettavaksi salakuuntelua koskevan rikoslain säännös (RL 24 luku 5 §). Koska luonnollisen henkilön äänikin on henkilötietoa, ja ottaen huomioon työelämän tietosuojalain asettama työntekijöiden henkilötietojen tarpeellisuusvaatimus (3 §), monessa organisaatiossa ei ole tietoturvan kannalta perusteita käyttää äänen nauhoittamista kameravalvonnan yhteydessä.

3.5.3 Kulunvalvonta

Kameravalvonta ei ole ainoa keino turvata organisaation tietoja, sillä myös muilla teknisillä menetelmillä, kuten kulunvalvonnalla, voidaan parantaa tietoturvaa. Kameravalvonta voi olla myös integroituna osaksi kulunvalvontaa. Kulunvalvonta itsessään on osa organisaation fyysistä turvallisuutta, jossa työntekijöiden ja muiden ihmisten liikkumista rajoitetaan ja valvotaan organisaation tiloissa. Yleensä kulunvalvonta sisältää mekaanisia tai sähköisiä lukituksia (taikka näiden yhdistelmiä), joihin kelpaavat esimerkiksi mekaaniset avaimet, sähköiset kulkukortit tai biometriset tunnistetiedot[837]. Yhtä lailla myös ulkoistettu vartiointihenkilöstö, aulahenkilöstö tai organisaation muu oma henkilöstö voi osallistua valvontaan. Isoissa organisaatioissa hyvien käytänteiden mukaisesti vieraat tulisi hakea aulasta ja omalla henkilöstöllä tulisi olla kulkukortit, joita pidetään näkyvissä vain organisaation omissa tiloissa[838].

Työntekijöiden yksityisyyden suojan kannalta merkityksellistä on sähköinen kulunvalvonta sekä sellainen mekaaninen kulunvalvonta, jossa on mukana elektroniikkaa. Kulunvalvonnassa ovien ja muiden kulkureittien yhteyteen sijoitetut lukijat tallentavat tietoja työntekijän liikkumisajankohdasta sekä sähköisten lukitusten avaamisesta ja avaamisyrityksistä. Nämä tiedot tallentuvat organisaation tietojärjestelmään ja muodostavat henkilötietoja sisältävän henkilörekisterin.[839] Tällöin henkilötietojen käsittelyssä on otettava huomioon tietosuojalainsäädäntö ja henkilötietojen keräämistä koskevat reunaehdot samalla tavalla kuin kameravalvonnan toteuttamisenkin osalta. Kulunvalvonnan osalta noudatetaan myös kameravalvonnan tavoin tarpeellisuusvaatimusta ja avoimuusperiaatetta. Tarpeellisuusvaatimus on perusteltavissa esimerkiksi tietoturvallisuuden parantamisella sekä väärinkäytösten ennaltaehkäisyllä ja jälkikäteen selvittämisellä.

Avoimuusperiaatteen ja työelämän tietosuojalain 21 §:n mukaisesti kaikenlainen tekninen, työntekijöihin kohdistuva valvonta tulee käydä läpi

[837] Biometrisia tietoja ovat esimerkiksi kasvokuvat, sormenjäljet, silmän iiris ja ääni. Ks. Korja 2016b, s. 139–140.
[838] Järvinen 2022b: 85–86.
[839] Nyblin 2009: 25–27.

yhteistoimintamenettelyssä, jonka jälkeen työnantajan on määriteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan käyttötarkoitus, siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä[840].

On myös huomioitava, että tietosuoja-asetuksessa DPIA-arviointia on vaadittu nimenomaan silloin, kun henkilötietojen käsittelytoimi todennäköisesti aiheuttaa korkea riskin luonnollisen henkilön oikeuksille ja vapauksille. Tällaisen todennäköisen korkean riskin aiheuttaa työntekijöiden järjestelmällinen valvonta[841]. Tässä tapauksessa järjestelmällinen valvonta tarkoittaa rekisteröityjen seurantaan, tarkkailuun tai valvontaan käytettävää tietojenkäsittelyn tai tietojen keräämistä verkkojen välityksellä taikka yleisölle avoimen alueen järjestelmällistä valvontaa laajamittaisesti. Työntekijät katsotaan myös kuuluvaksi heikossa asemassa oleviin rekisteröityihin, mikä on tässä esimerkkikäsittelytoimessa toinen mahdollinen perustelukriteeri DPIA:n tekemiselle. Jos rekisterinpitäjä kuitenkin katsoo, että todennäköisesti aiheutuvaa korkeaa riskiä luonnollisen henkilön oikeuksille ja vapauksille ei aiheudu käsittelytoimesta, rekisterinpitäjän on perusteltava ja dokumentoitava syyt DPIA:n tekemättä jättämiselle.[842] Kuten aikaisemminkin on todettu myös biometriset tiedot osana tunnistusta ovat erityisiä henkilötietoja, jotka voivat aiheuttaa korkean riskin luonnollisen henkilön oikeuksien ja vapauksien kannalta. Näin ollen erityisesti sellaiset organisaation käyttämät kulunvalvontamenetelmät, joissa käytetään kasvokuvaa henkilön tunnistamiseksi tai sormenjälkitunnistusta, sisältävät biometrista erityistä henkilötietoa, jolloin DPIA tulisi tehdä. Tästä näkökulmasta tietosuoja-asetuksen velvoitteet ulottuvat myös työelämän tietosuojaa koskevaan osa-alueeseen.

Perinteisessä kulunvalvonnassa ovien ja muiden kulkureittien yhteyteen sijoitetut lukijat tallentavat tietoja muun muassa sijainnista ja ajankohdasta, jolloin työntekijä on avannut tai yrittänyt avata tietyn oven kulkutunnisteellaan. Näin ollen järjestelmän rekisteriin muodostuu myös sijaintitietoa. Kansallinen tietosuojaviranomainen on tietosuoja-asetuksen mukaisesti luonut luettelon käsittelytoimien tyypeistä, jolloin DPIA tulee tehdä[843]. Tässä luettelossa sijaintitietojen käsittely yhdistettynä heikossa asemassa olevien työntekijöiden järjestelmälliseen valvontaan on kriteeri, jolloin organisaation kulunvalvonnasta on tehtävä DPIA.

---

[840] Tietosuojavaltuutetun lausunto 4.9.2015.
[841] Esimerkkinä järjestelmällisestä valvonnasta on sähköisen kulunvalvonnan ja kameravalvonnan lisäksi työntekijöiden työasemien ja toiminnan valvonta internetissä.
[842] Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, s. 9–14.
[843] Ks. Tietosuojavaltuutetun toimisto 2018.

Yhteenvetona korostettakoon, että kulunvalvonta on yksi tärkeimmistä fyysisen tietoturvallisuuden suojakontrolleista aivan kuten esimerkiksi järjestelmien pääsynhallinnan kontrollit suojaavat järjestelmiä luvattomalta käytöltä. Organisaation kulunvalvonnassa tapahtuva henkilötiedon käsittelyperuste on väärinkäytösten ennaltaehkäisy ja jälkikäteisten väärinkäytösten selvittely, jolloin tavoitteena on rajoittaa ja valvoa henkilöiden liikkumista organisaation tiloissa. Keskeisiä käsiteltäviä tietoja erityisesti sähköisessä kulunvalvonnassa ovat esimerkiksi työntekijän kulkutunnisteen lisäksi ovien avausajankohdat ja -yritykset. Tällöin kulunvalvonnan lokien henkilötietojen käsittely perustuu pääsääntöisesti sijaintitietojen käsittelylle, joka on katsottava korkeariskiseksi henkilötietojen käsittelyksi. Näin ollen tietosuojalainsäädännön tarpeellisuusvaatimuksen ja avoimuusperiaatteen lisäksi tulee huomioida, että kulunvalvonnasta on tehtävä DPIA. Työntekijöiden sijaintitietoa käsitellessä tällaisessa järjestelmässä tulee olla erityisen tarkka siitä, että alkuperäinen turvallisuusperusteinen käsittelytarkoitus ei muutu joksikin toiseksi. Esimerkiksi vastaavan tiedon käsittely raakadatana tilojen käyttöasteseurannan ja raportoinnin tarkoituksia varten ei ole lainmukaista käsittelyä, sillä alkuperäinen käsittelytarkoitus on muu (käyttöasteseuranta) kuin turvallisuusperusteinen väärinkäytösten ennaltaehkäisy ja selvittely. Sijaintitietojen tehokkaalla anonymisoinnilla tilojen käyttöasteseurantaa olisi mahdollista toteuttaa, kunhan datasta ei ole mahdollista tunnistaa työntekijöitä[844].

Kulunvalvonta ja kameravalvonta yhdistettyinä ovat erittäin hyvä, organisaation fyysistä tietoturvallisuutta parantava yhdistelmä. Ne eivät kuitenkaan välttämättä ole riittäviä, jos muut organisaation tietoturvakäytänteet eivät toteudu, eli esimerkiksi ovia jätetään auki tai valvonnan toimivuutta ei koskaan testata. Tietoturvan sääntelyjärjestelmässä on puutteellisesti huomioitu fyysisen tietoturvallisuuden osa-alue, mutta tähän on tulossa muutosta NIS 2 -direktiivin implementoinnin myötä[845]. Silti fyysisen tietoturvallisuuden huomioiminen tulisi ulottaa kaikkiin organisaatioihin vähintään edes kulunvalvonnan osalta, jotta organisaation laitteet ja niiden sisältämä tieto (kyberympäristö) olisi asianmukaisesti suojattu.

3.5.4 Muu teknisin menetelmin toteutettu valvonta ja välitystiedot

Kamera- ja kulunvalvonnan lisäksi muuta teknisin menetelmin toteutettavaa valvontaa on esimerkiksi tietoliikenteen valvonta ja muu tietoturvavalvonta, jolla

---

[844] ks. Euroopan WP29-tietosuojatyöryhmä WP216: *Lausunto 5/2014 anonymisointitekniikoista*, s. 8: Tietosuojatyöryhmän näkemyksen mukaan anonymisointi on henkilötietojen myöhempää käsittelyä, jonka voidaan katsoa olevan henkilötietojen alkuperäisen käsittelyn tarkoituksen kanssa yhteensopivaa ainoastaan sillä ehdolla, että anonymisointiprosessilla voidaan luotettavasti tuottaa anonyymeja tietoja.
[845] Ks. luku 4.3.4 (”Fyysinen tietoturvallisuus osana riskienhallintaa”).

voidaan lisätä organisaation proaktiivisuutta havaita tietoturvauhkia ja automaattisesti estää tietoturvaloukkauksia. Tästä esimerkkinä työntekijöiden automaattinen pääsyn estäminen tietyille haitallisille sivustoille. Direktio-oikeus luo työnantajalle oikeuden päättää työnantajan järjestelmissä tapahtuman verkkoselailun laajuudesta sekä määrätä, mihin tarkoitukseen tietoverkkoa ja sähköpostia käytetään. Täten työnantaja voi estää pääsyn tietyille sivustoille rajoittamalla esimerkiksi liikennettä tiettyihin verkkotunnuksiin tai IP-osoitteisiin.

Työpaikalta lähetetyt sähköpostit, puheluiden ja internetin käytön valvonnalla saadut tiedot kuuluvat EIS 8 artiklan yksityiselämän suojan piiriin. Esimerkiksi **EIT:n ratkaisussa Copland v. Yhdistynyt kuningaskunta 3.7.2007**:

> *Ratkaisussa todettiin ihmisoikeussopimusta rikotun, kun työnantaja valvoi työntekijän puhelimen ja sähköpostin käyttöä kertomatta valvonnasta työntekijöille.*[846]

Koska kaikki viestiliikennetiedot katsotaan kuuluvan yksityiselämän suojan piiriin, työntekijän sallitun valvonnan on oltava tarkkarajaista sekä yksilön oikeussuojakeinot turvaavaa, sen on omattava hyväksyttävät tavoitteet, eikä esimerkiksi työssä käytettävien sosiaalisen median palvelujen käyttöehdot vähennä työnantajan vastuuta työntekijöidensä henkilötietojen suojasta[847]. Työntekijällä katsotaan olevan kohtuullinen odotus yksityisyyden osalta. EIT:n mukaan ei ole kuitenkaan poissuljettua, että työntekijän puhelimen, sähköpostin ja internetyhteyden käytön valvonta työpaikalla voi tietyissä olosuhteissa olla välttämätöntä hyväksyttävän tavoitteen saavuttamiseksi.[848] Työntekijöiden tulee olla tietoisia esimerkiksi puhelutallenteiden kuuntelusta ja tietoliikennetietojen tarkastamisesta. Näin ollen menettelyssä tulee tässäkin tapauksessa noudattaa yhteistoimintaa eli kuulla työntekijöitä ja järjestää valvonta niin, että työntekijät ovat siitä tietoisia.

Työelämän tietosuojalain 21 §:ssä on määritelty teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisestä, jotka kuuluvat yhteistoimintamenettelyn piiriin. Työnantajan on myös määriteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan käyttötarkoitus ja siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä.[849]

---

[846] Neuvonen 2019: 259–260; Nyblin 2009: 70–71.
[847] Alapuranen 2020: 103; Pesonen 2013: 167. Ks. myös Nyblin 2009: 70–71.
[848] Gullans, Pellonpää, Pölönen & Tapanila 2018: 841–842.
[849] Ks. myös yhteistoimintalaki (1333/2021) 8 § kohta 6 sekä 12 § kohta 3 ja 4. Lain mukaan työnantajan ja henkilöstön edustajan on käytävä säännönmukaista vuoropuhelua liittyen työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutettavan valvonnan tarkoituksesta, käyttöönotosta ja näissä

Työnantajan on annettava henkilökunnalle ohjeet tietoverkon käytöstä, ja nämä ohjeet on käsiteltävä yhteistoimintamenettelyssä sekä tiedotettava henkilökunnalle[850]. Isommissa organisaatioissa tällaisia ohjeistuksia yhteisistä pelisäännöistä verkon käyttämiselle ja liikesalaisuuksien käsittelylle löytyy hyvin osana tietoturvaohjeistuksia, ja niistä tiedotetaan hyvien tietoturvallisten käytänteiden mukaisesti muun muassa intrassa sekä osana perehdytystä ja henkilökunnan tietoturvakoulutusta. Pienemmissä tai tietoturvamaturiteetiltaan vähemmän kehittyneissä organisaatioissa tällaisia ohjeita ei välttämättä ole vaan tietoisuus toimintatavoista perustuu maalaisjärkeen tai pelkkään oletukseen. Joissain organisaatioissa ei välttämättä ole edes tiedossa, että tällaisten ohjeiden tekeminen pohjautuu lakiin eikä ainoastaan hyviin tietoturvallisiin käytänteisiin, jolloin ohjeiden tekeminen ei ole myöskään prioriteettilistan alkupäässä.

Verkkoselailusta palvelimelle tai päätelaitteelle jääneitä välitystietoja[851] ei saa käyttää työnantajan direktio-oikeuden toteuttamiseen, eli työntekijöiden yksityiskohtaiseen valvomiseen ja seuraamiseen. Työnantajan on tässä tapauksessa muistettava myös tietosuojaan liittyvät käsittelysäännöt välitystietojen ollessa yksilöivää henkilötietoa.[852] Eli yhteenvetona työnantajalla on direktio-oikeuden nojalla oikeus antaa määräyksiä, millaisia sivustoja työntekijöillä on oikeus selata työpaikan internetin välityksellä, sekä ohjeistaa internetin käyttöä. Sen sijaan työnantajalla ei ole yleistä oikeutta välitystietoja tarkkailemalla valvoa, noudattavatko työntekijät näitä määräyksiä ja ohjeita.[853] Luottamuksellisen viestinnän suojaan puuttuminen välitystietojen kautta on viimesijainen keino, jolloin esimerkiksi työnantajan asemassa oleva yhteisötilaaja ei saa seurata viestintäverkon ja -palveluiden käyttöä työajan seuraamiseksi tai sen selvittämiseksi, onko työntekijä ollut yhteydessä työterveyteen, henkilöstön edustajaan tai työsuojeluviranomaisiin.[854]

Turhien sijaintitietojen keräämisen osalta tulee myös olla tarkkana. Mikäli sijaintitietoja käsitellään järjestelmällisen valvonnan yhteydessä, tulee tehdä DPIA.

---

käytettävistä menetelmistä, sähköpostin ja tietoverkon käytöstä sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittelystä. Vuoropuhelua on käytävä myös sähköisen viestinnän palveluista annetun lain 146–156 §:ssä tarkoitetussa välitystietojen käsittelyssä noudatettavien menettelyjen perusteista ja käytännöistä.

[850] Ks. Pesonen 2013: 153. Sosiaalisen median käyttö on tietoverkon käyttöä samaan tapaan kuin internetin käyttö, minkä vuoksi työnantajan on annettava myös sosiaalisen median käytöstä ohjeet työelämän tietosuojalain mukaisesti.

[851] Aiemmassa lainsäädännössä on käytetty termiä *”tunnistamistieto”*, joka on korvattu termillä *”välitystieto”*. HE 221/2013 vp, s. 95: Välitystieto on oikeus- tai luonnolliseen henkilöön yhdistettävissä oleva tieto, jota viestinnän välittäjä käsittelee viestien välittämiseksi.

[852] Innanen & Saarimäki 2012: 176–177; Alapuranen 2020: 103.

[853] Nyblin 2009: 42.

[854] HE 48/2008 vp: 20; Hoikka, Neuvonen & Rautiainen 2016: 364.

Esimerkiksi kolmessa apulaistietovaltuutetun ratkaisussa useat julkisen sektorin toimijat olivat antaneet työntekijöille käytettäväksi tietokoneita, joihin asennettu Windows 10 -käyttöjärjestelmän toiminto keräsi sijaintietoja. Työntekijöillä ei ollut mahdollista muuttaa tätä asetusta ja työnantajat eivät tienneet tämän ominaisuuden olemassaolosta tai käyttäneet sijaintitietoja. Rekisterinpitäjä ja käsittelijät määrättiin poistamaan laittomasti kerätyt henkilötiedot.[855] Myös esimerkiksi **ratkaisussa TSV 5.7.2021 (dnro. 3843/163/20)** apulaistietosuojavaltuutettu katsoi sijaintitietojen keräämisen työelämän tietosuojalain 3 §:n tarpeellisuusvaatimuksen vastaiseksi:

> *Rekisterinpitäjä-työnantaja oli ottanut käyttöön noin 350 työntekijän osalta X Oy:n toimittaman mobiilisovelluksen, jonka tarkoituksena oli työajan seuranta ja työaikojen leimaaminen. Sovelluksen käyttäminen edellytti kuitenkin mobiililaitteessa paikannuksen sallimisen. Apulaistietosuojavaltuutetun mukaan, vaikka sovelluksella työaikaa koskevien leimausten tekeminen ei onnistu ilman sijaintitietojen käsittelyä, se ei tee niiden käsittelystä välittömästi tarpeellista työelämän tietosuojalain 3 §:n mukaisesti. Sellaisia palveluita tai järjestelmiä, joiden toiminnallisuudet eivät vastaa rekisterinpitäjän tarpeita tai mahdollista tietosuojaa koskevien säännösten noudattamista, ei tulisi ottaa käyttöön. Vaikka sovelluksen käyttö olikin vapaaehtoista, huomioitava on, että työelämän tietosuojalain 3 §:n tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella.*

Lokitiedot ovat keskeisessä roolissa teknisin menetelmin toteutetussa valvonnassa, jota organisaatioissa toteutetaan. Huomioitava on, että lokitietojen keräämisestä ja käsittelystä on spesifisti ja suoraviivaisesti säädetty lähinnä tiedonhallintalaissa, joka velvoittaa viranomaisia, mutta myös välillisesti esimerkiksi viranomaisten järjestelmien toimittajia, jotka suunnittelevat järjestelmiä. Lokituksen osalta huomioitavia säädöksiä löytyy tiedonhallintalain ohella epäsuorasti myös muualta kansallisessa lainsäädännössä.[856]

Tapauskohtaisesti lokitiedot saattavat olla sähköisen viestinnän palvelusta annetussa laissa tarkoitettuja välitystietoja[857], jolloin niiden käsittelyyn sovelletaan

---

[855] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 709; TSV 31.5.2022, dnro:t 6813/171/21, 1141/161/22 & 2464/161/22.
[856] Ks. lisää järjestelmien lokitusvaatimuksista luvusta 4.4.2 (”Järjestelmien lokitusvaatimukset tietoturvan sääntelyjärjestelmässä”).
[857] Mikäli välitystiedot voidaan liittää tunnistettavissa olevaan henkilöön, tiedot ovat tietosuoja-asetuksessa tarkoitettuja henkilötietoja. Tällöin tulee myös huomioida tietosuoja-asetuksen vaatimukset.

kyseistä lakia[858]. Välitystietojen käsittely on olennainen osa organisaation teknisen menetelmin toteutettua tietoturvavalvontaa, ja lähtökohtaisesti laki sähköisen viestinnän palveluista painottaa automaattisin menetelmin toteutettua välitystietojen käsittelyä ensisijaisena menetelmänä[859].

Välitystieto on oikeus- tai luonnolliseen henkilöön yhdistettävissä oleva tieto, jota viestinnän välittäjä käsittelee viestien välittämiseksi[860]. Näin ollen välitystietoja voivat olla muun muassa lähettäjän ja vastaanottajan sähköpostiosoitteet ja viestien aikaleimat sekä IP-osoitteet silloin, kun niitä käsitellään viestinnän välittämiseksi. Lain esitöistä ilmenee, että välitystieto voi olla joukko erilaisia tietoja, joka voidaan yhdistää tiettyyn tilaajaan tai käyttäjään eli oikeus- tai luonnolliseen henkilöön, sekä niitä käsitellään viestin välittämiseksi[861]. Lakia sanamuodon mukaisesti tulkittuna tiedoista tulee välitystietoja vasta sitten, kun niitä käsitellään viestinnän välittämiseksi. Asia ei ole kuitenkaan katsottu olevan niin yksinkertainen. Esimerkiksi välitystietojen luottamuksellisuuden perusoikeussuojan kariseminen ei tulisi olla mahdollista tietojen luovuttamisen yhteydessä tai käsiteltäessä aikaisemmin viestin välittämiseen käytettyjä tietoja muussa tietojärjestelmässä. Toisin sanoen välitystiedot pysyvät välitystietoina, vaikka niitä ei enää käsiteltäisi viestinnän välittämiseen.[862]

Huomioitava on se, että välitystiedot voivat koskea myös oikeushenkilöitä eli esimerkiksi oikeustoimikelpoisia valtioita, kuntia ja osakeyhtiöitä. IP-osoitteet voivat olla välitystietoja silloin, kun niitä käsitellään viestinnän välittämiseksi. Tällöin kriteerinä on se, että IP-osoite olisi yhdistettävissä henkilöön: sähköisen viestinnän palvelulain mukaan kyseessä voi olla sekä oikeushenkilö että luonnollinen

[858] Huomion arvioinen seikka on, että EU:n lainvalmistelussa parhaillaan oleva sähköisen viestinnän tietosuoja-asetus eli ePrivacy-asetus muuttanee sähköisen viestinnän palveluista annettua lakia sekä siihen liittyviä välitystietojen tietoturvaperusteista käsittelyä, joita on tässä tutkimuksessa käsitelty jäljempänä muun muassa pykälien 138, 272 ja 247 osalta. Esimerkiksi ePrivacy-asetuksen ehdotusluonnoksen mukaisesti sähköisen viestinnän tietojen luottamuksellisuudesta ja sallitusta käsittelystä on linjattu luonnoksen 5 ja 6 artikloissa.

[859] Ks. sähköisen viestinnän palveluista annetun lain 138 § ja 272 §, jotka koskevat viestinnän välittäjää ja lisäarvopalvelun tarjoajaa välitystietojen ja viestin sisällön käsittelyn osalta, sekä 149–150 §, jotka koskevat yhteisötilaajaa ainoastaan välitystietojen käsittelyn osalta.

[860] Huomioitava on, että henkilötieto koskee vain luonnollisia henkilöitä, jolloin välitystiedon määritelmä on laajempi koskiessaan myös oikeushenkilöitä. Ks. HE 221/2013 vp: 95.

[861] HE 222/2010 vp: 317.
Välitystietoihin on tulkittu kuuluvan tietoja, jotka viittaavat muun muassa viestinnän reititykseen, kestoon, ajankohtaan tai siirrettävän tiedon määrään, käytettyyn protokollaan, lähettäjän tai vastaanottajan päätelaitteen sijaintiin tietyn tukiaseman alueella, lähettävään tai vastaanottavaan verkkoon ja yhteyden alkuun, loppuun tai kestoon. Ks. HE 125/2003 vp, s. 46.

[862] Heiskanen 2020: 97–99, 103.

henkilö. Jälkimmäisen ollessa kyseessä, tulee soveltaa myös tietosuojalainsäädäntöä IP-osoitteen käsittelyn osalta IP-osoitteen ollessa henkilötietoa. Kaikissa tapauksissa IP-osoitetta ei välttämättä tulkita henkilötiedoksi[863], mutta tämä tulkinta ei estä sitä, etteikö IP-osoite silti voisi olla välitystieto. Tällöin IP-osoitteen tulee olla yhdistettävissä oikeushenkilöön. Huomioitava kuitenkin on se, että oikeushenkilön ollessa esimerkiksi pieni osakeyhtiö henkilöstömäärältään, tätä kautta voi tunnistaa epäsuorasti luonnollisen henkilön ja tällöin IP-osoite onkin katsottava henkilötiedoksi.

Ratkaisussa **KKO 2022:23** käsitellään lokitietoa välitystietona[864]. Tapauksessa oli sinänsä kysymys siitä, että VPN-yhteydellä salatun viestinnän osapuolen IP-osoitetta ei saanut takavarikoida. Korkeimman oikeuden ratkaisu eli niin sanottu vuosikirjan otsikko oli seuraava:

> *A Oyj tarjosi virtuaalisen erillisverkon (VPN) avulla toteutettavaa palvelua, joka salasi palvelun käyttäjän todellisen IP-osoitteen. Keskusrikospoliisi oli vieraan valtion oikeusapupyynnön perusteella takavarikoinut vieraassa valtiossa vireillä olevaan rikostutkintaan liittyen A Oyj:n hallusta lokitietoja, jotka muun ohella paljastivat käyttäjän todellisen IP-osoitteen.*
>
> *Korkein oikeus katsoi ratkaisusta ilmenevillä perusteilla, että A Oyj:tä oli pidettävä viestinnän välittäjänä ja että pakkokeinolain 7 luvun 4 §:n[865] mukainen takavarikoimis- ja jäljentämiskielto koski viestinnän välittäjän hallussa olevaa säännöksessä tarkoitettua välitystietoa.*

Kyseisen KKO:n ratkaisun mukaan tilaajan käyttämä IP-osoite oli yhdistettävissä internetliittymän haltijaan ja VPN-palvelussa käsiteltiin IP-osoitteita viestien välittämiseksi. Näin ollen VPN-palveluun tunnistautumisen yhteydessä tallentuneet IP-osoitteita sisältäneet lokitiedot katsottiin luottamuksellisen viestinnän suojan piiriin kuuluviksi viestinnän välitystiedoiksi.

---

[863] Tulkinnassa tulee huomioida muun muassa eri toimijoiden toimialasidonnaiset eroavaisuudet sekä käytettävissä olevat oikeuskeinot. Ks. lisää pohdintaa luvussa 3.2.1 (”Henkilötieto ja erityinen henkilötieto”).

[864] Tässä tutkimuksessa käytetään käsitettä välitystieto, vaikka ratkaisussa käytössä oleva käsite on tunnistamistieto. Ratkaisun KKO 2022:23 kohdassa 23 todetaan, että välitystiedoilla tarkoitetaan samaa asiaa kuin tunnistamistiedoilla. Myöhemmin pakkokeinolakia päivitettiin KKO:n ratkaisua vastaavaksi hallituksen esityksellä (HE 217/2022 vp, s. 25–26, 44), jolloin tunnistamistieto korvattiin käsitteellä välitystieto.

[865] Pakkokeinolain 7 luvun 4 §:n mukaan viestinnän välittäjän hallusta ei saa takavarikoida tai jäljentää asiakirjaa tai dataa, joka sisältää rikoksesta epäillyltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin liittyviä tietoja, kyseisen lain 10 luvun 6 §:n 1 momentissa tarkoitettuja välitystietoja tai 10 §:n 1 momentissa tarkoitettuja tukiasematietoja.

Ratkaisua on kritisoitu riittämättömästä analysoinnista sen osalta, oliko kysymys kuitenkaan lainkaan viestistä ja siihen liittyvistä välitystiedoista, jotka liittyvät aina tietyn viestin välittämiseen. VPN-palvelun käyttöönottoon kuului päätelaitteelle asennetun ohjelmiston ja VPN-palvelun välistä teknistä viestintää, joka tapahtuu ennen VPN-palvelun toiminnan ja siten myös käyttäjän kannalta merkityksellistä sähköistä viestintää. Teknistä liikennettä, kuten VPN-yhteyden muodostamista koskevaa liikennettä vailla yhteyttä tiettyyn viestiin, ei ole pidetty luottamuksellisen viestinnän suojan piiriin kuuluvana. Kritiikin mukaan tapauksessa itse viestiä ei vielä ollut olemassa, jolloin kysymys ei olisi voinut myöskään koskea välitystietoja.[866] Viestin käsitteeseen on katsottu kuuluvan lähes kaikenlaiset informaatiomuodot, mutta se ei sisällä puhtaasti viestiin liittymätöntä tietokoneiden välistä ohjaus- ja signalointiliikennettä[867].

Kritiikin pohdinta kohdistuu tekniseen viestintään päätelaitteen ja VPN-palvelun välillä unohtaen kuitenkin, että tapauksen alkuperäinen takavarikointipäätös koski nimenomaan VPN-palvelun IP-osoitteeseen liittyvää **lokitietoa** siitä, mihin IP-osoitteisiin tämä VPN-palvelun IP-osoite oli ollut yhteydessä[868]. Ratkaisussa on todettu, että VPN-palvelun toiminnan ja käyttäjän kannalta merkityksellisenä viestintänä on pidettävä käyttäjän VPN-palvelun salaaman IP-osoitteen avulla kolmannen osapuolen kanssa internetissä tapahtuvaa viestintää[869]. Ratkaisussa ilmi tuleva lokipyyntö ulottuu myös kolmannen osapuolen IP-osoitteeseen, josta saattoi palvelusta riippuen muodostua yhteyslokimerkintä[870]. Kuten aikaisemmin on todettu[871], IP-osoite yksilöi tietoverkkoon liitetyn laitteen ja auttaa tietojen ja viestinnän siirtämisessä laitteiden välillä IP-pakettien kulkiessa IP-osoitteiden välillä. Asiakkaan laitteella olevan VPN-ohjelmiston tarkoitus on muuttaa asiakkaan laitteen IP-osoite eli niin sanottu ”kotiosoite” käytetyn VPN-palvelun oman VPN-palvelimen IP-osoitteeksi, jonka ulkopuoliset näkevät ja samalla kotiosoite pysyy sijainniltaan piilossa ja reitittyy esimerkiksi USA:han. Perustoimintona VPN-ohjelmisto salaa tiedot ja viestin ennen lähetystä (A), jonka jälkeen se lähetetään VPN-

[866] KKO 2022:23, kohta 13; Viitanen 2022: KKO:n ratkaisut kommentein 2022:I.
[867] HE 222/2010 vp: 317.
[868] Saksan keskusrikospoliisin tutkinnassa oli tullut esiin VPN-palvelun IP-osoite. Keskusrikospoliisi oli Saksan viranomaisten kiireellisen oikeusapupyynnön johdosta 14.1.2019 antamallaan datan säilyttämismääräyksellä määrännyt A Oyj:n säilyttämään kyseiseen IP-osoitteeseen liittyvät käyttäjätiedot, rekisteröintitiedot ja lokitiedot tiettynä kolmena ajankohtana. Keskusrikospoliisi oli tämän jälkeen tekemällään takavarikkopäätöksellä määrännyt otettavaksi haltuun tai jäljennettäväksi A Oyj:n hallussa ollutta lokitietoa siitä, mihin IP-osoitteeseen datan säilyttämismääräyksessä mainittu IP-osoite oli ollut yhteydessä mainittuina aikoina. Ks. KKO 2022:23, asian tausta kohdat 2 ja 3.
[869] KKO 2022:23, kohta 13.
[870] Huomioitava on kuitenkin, että jotkin VPN-palvelut eivät välttämättä lokita tai säilytä lokeja VPN-palvelun kautta kolmansiin osoitteisiin muodostetuista yhteyksistä: Tämä tosin ei tullut selkeästi ilmi ratkaisussa.
[871] Ks. luku 3.2.1 (”Henkilötieto ja erityinen henkilötieto”).

palvelimelle (B) ja palvelimen kautta alkuperäiseen vastaanottaja-IP-osoitteeseen (C). Ilman VPN-palvelua viesti kulkisi salaamattomana suoraan alkuperäisestä koti-IP-osoitteesta (A) vastaanottaja-IP-soitteeseen (C). Oikeustapauksen kysymys koski nimenomaan palveluun liittyvän VPN-palvelimen IP-osoitteen lokitietoja (B). Oletettavaa on se, että viranomaisen lokitietopyyntö on nimenomaan koskenut merkityksellistä viestintää asiakkaan laitteen koti-IP-osoitteen (A) sekä kolmannen osapuolen vastaanottaja IP-osoitteen (C) välillä VPN-palvelimen (B) kautta eikä esimerkiksi muunlaista teknistä, palvelua valmistelevaa lokia. Näin ollen aikaisemmin mainittu kritiikki on aiheetonta, koska se ei huomioi riittävällä tasolla alkuperäisen lokitietopyynnön kohdetta eikä lokien eroavaisuuksia.

KKO:n ratkaisun analysoinnissa on syytä kiinnittää huomiota myös sähköisen viestinnän palveluista annetun lain mukaisiin roolituksiin. KKO:n ratkaisu on paikkaansa pitävä viestinnän välittäjän roolituksen osalta, sillä A Oyj välittää VPN-palvelussa salaaman käyttäjän IP-osoitteen avulla kolmannen osapuolen kanssa internetissä tapahtuvaa viestintää eli viestintä välittyy aikaisemmin käsitellyin perustein VPN-palvelun kautta[872]. Lopputulemaan pääsemiseksi ratkaisussa on käyty eri roolituksia läpi: A Oyj:n VPN-palvelu ei ole katsottu olevan viestintäpalvelu, se ei toimi viestintätapahtumassa teleyrityksenä, eikä A Oyj:tä voi myöskään pitää yhteisötilaajana[873]. Käydessään läpi eri roolitusvaihtoehtoja KKO ei kuitenkaan valitettavasti ottanut kantaa siihen, miksi A Oyj ei ollut heidän tulkintansa mukaan lisäarvopalvelun tarjoaja. Tämä rooli oli kokonaan jätetty ratkaisusta pois. Sähköisen viestinnän palveluista annetun lain mukaan lisäarvopalvelulla tarkoitetaan palvelua, joka perustuu välitys- ja sijaintitietojen käsittelyyn muuta tarkoitusta kuin viestinnän välittämistä varten. Useimmiten tällaisia lisäarvopalveluita ovat nimenomaan erilaiset tietoturvaa parantavat palvelut, kuten IP-osoitteita käsittelevät seurantatyökalut (esimerkiksi SIEM[874]), jolloin niiden päätehtävä on viestinnän välittämisen sijaan varmistaa osaltaan tietoturvallinen palvelu tai ympäristö. Ratkaisussa on selkeästi todettu, että VPN-palvelussa välitetään sähköistä viestintää sen olematta kuitenkaan viestintäpalvelu. Tämä toteama johtaa ristiriitaiseen tulkintaan siitä, että VPN-palvelun todellinen tarkoitus on joku muu kuin viestinnän välittäminen. Tällöin sen todellinen tarkoitus tai tehtävä olisi tietoturvallisuuden parantaminen, jolloin A Oyj:n rooli olisi lisäarvopalvelun tarjoaja. Olisi ollut parempi, jos KKO olisi vastakohtaisesti todennut VPN-palvelun olevan viestintäpalvelu[875], sillä tämä olisi selkeyttänyt ratkaisua. Lisäksi

[872] KKO 2022:23, kohta 13.
[873] KKO 2022:23, kohta 10.
[874] SIEM (Security Information and Event Management) on seurantatyökalu, joka tallentaa lokitietoa tunnistaakseen poikkeavuuksia ja tehdäkseen niistä hälytyksiä.
[875] Sähköisen viestinnän palveluista annetun lain mukaan viestintäpalvelulla tarkoitetaan palvelua, joka muodostuu kokonaan tai pääosin viestien siirtämisestä viestintäverkossa

perusteluissa olisi voinut käsitellä, miksi VPN-palvelun tarjoaja ei ole lisäarvopalvelun tarjoaja. Tällöin ratkaisu olisi luonnut kattavampaa tulkintakäytäntöä ja tulkinnallista arvoa sähköisen viestinnän palveluista annetun lain monimutkaisten roolituksien osalta. Eri organisaatioiden lakiosaajilta vaaditaan paljon palvelujen tekniikan tuntemista, jotta organisaatioiden on mahdollista tunnistaa sekä tietosuoja-asetuksen että sähköisen viestinnän palveluista annetun lain mukaiset roolinsa, oikeutensa ja vastuunsa.

Välitystietoja välittää viestinnän välittäjä, joka voi olla sähköisen viestinnän palveluista annetun lain 3 §:n mukaan teleyritys, yhteisötilaaja ja sellainen muu taho, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin. Yhteisötilaaja voi olla esimerkiksi työnantaja, joka tilaa viestintäpalvelun tai lisäarvopalvelun työntekijöidensä käytettäväksi. Näin ollen työnantaja voi olla sekä viestinnän välittäjä että yhteisötilaaja[876], joka voi käsitellä välitystietoina olevia lokitietoja sähköisen viestinnän palveluista annetun lain mukaisin käsittelyperustein.

Viestin välittäjän käsittelyperiaatteiden (SVPL 137 §) mukaisesti välitystietojen, esimerkiksi lokitietojen, käsittely on sallittua käsittelyn tarkoituksen vaatimassa laajuudessa eikä käsittelyllä saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Myös Katakri 2020 teknisen tietoturvallisuuden I11-vaatimuksessa painotetaan, että lokeihin saa kerätä vain tietoturvaan liittyvien toimenpiteiden kannalta välttämättömiä tietoja, eikä toimenpiteitä toteutettaessa saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa.

Välitystietoina toimivien lokitietojen käsittelyn jälkeen lokitiedot on hävitettävä tai muunnettava muotoon, jossa niitä ei voi yhdistää tilaajaan tai käyttäjään. Tällaisia lokitietoja saa ainoastaan käsitellä viestinnän välittäjän, esimerkiksi työnantajan, lukuun toimiva. Sähköisen viestinnän palveluista annetun lain mukaan välitystietoja voidaan myös luovuttaa ainoastaan tahoille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa, kuten esimerkiksi yhteisötilaajana toimivan työnantajan oikeus käsitellä ja selvittää työntekijöiden internetin käytöstä syntyviä välitystietoja väärinkäytöstapauksissa (146–156 §)[877].

---

sekä siirto- ja lähetyspalvelua joukkoviestintäverkossa ja henkilöiden välisen viestinnän palvelua.

[876] Ks. Heiskanen 2020, s. 105. Yhteisötilaaja voi toimia samalla myös viestinnän välittäjän roolissa tilatessaan viestintäpalvelun tai lisäarvopalvelun esimerkiksi työntekijöidensä käytettäväksi.

[877] Alapuranen 2020: 113.
Luvattoman käytön ja liikesalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi säädettyjä toimenpiteitä on käsitelty seuraavassa alaluvussa 3.5.5 (”Väärinkäytösten ehkäiseminen ja selvittäminen organisaatioissa”)

Sähköisen viestinnän palvelulain 138 §:n mukaan välitystietoina toimivien lokitietojen käsittely on mahdollista esimerkiksi tietoturvasta huolehtimiseksi 272 § säädetyllä tavalla, muun muassa viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Haittaa aiheuttavilla häiriöillä tarkoitetaan muun muassa haittaohjelmien levittämistä ja käyttämistä[878]. Sähköisen viestinnän palvelulain 272 § on oleellinen organisaatioiden tietoturvan kannalta, sillä se mahdollistaa teknisin menetelmin toteutetun tietoturvavalvonnan.

Organisaation toimiessa viestinnän välittäjän roolissa, sillä on **oikeus ryhtyä välittömiin toimiin tietoturvasta huolehtimiseksi (272 §)**. Sama oikeus koskee myös lisäarvopalvelun tarjoajaa, jonka tarjoama lisäarvopalvelu perustuu välitys- ja sijaintitietojen käsittelyyn muuta tarkoitusta kuin viestin välittämistä varten. Aikaisemmin pykälä koski teleyritystä ja yhteisötilaajaa, mutta nämä muutettiin viestinnän välittäjäksi tasapuolisten toimintaedellytysten ja kattavan tietoturvatason mahdollistamiseksi: käsite mahdollisti myös muille viestinnän välittäjille samat oikeudet tietoturvan toteuttamistoimenpiteisiin[879].

Sähköisen viestinnän palveluista annetun lain 272 § mahdollistaa laajemmat toimet tietoturvatoimenpiteiden osalta kuin mihin viestinnän välittäjällä ja lisäarvopalvelun tarjoajalla on lain 247 §:n velvollisuuden mukaan. 247 §:n mukaan viestinnän välittäjän on huolehdittava viestejä välittäessään palvelujensa, viestien, välitystietojen ja sijaintitietojen tietoturvasta. Vastaavasti viestinnän välittäjänä toimiva yhteisötilaaja on huolehdittava ainoastaan käyttäjiensä viestien, välitystietojen ja sijaintitietojen käsittelyn tietoturvasta, jolloin yhteisötilaajan tietoturvan huolehtimisvelvollisuus on suppeampi. Olennaista on tietoturvatoimenpiteiden suhteellisuus huomioon ottaen uhan vakavuus, kustannukset ja käytettävissä olevat tekniset mahdollisuudet. [880]

Sähköisen viestinnän palveluista annetun lain 272 §:n mukaisia välittömiä toimenpiteitä tietoturvasta huolehtimiseksi, jotka koskevat viestinnän välittäjää ja lisäarvopalvelun tarjoajaa, ovat esimerkiksi viestin sisältöä koskeva automaattinen selvittäminen, viestien välittämisen ja vastaanottamisen automaattinen estäminen tai rajoittaminen, tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattinen poistaminen viesteistä sekä muut edellä mainittuihin toimenpiteisiin rinnastettavat teknisluonteiset toimenpiteet. Lakipykälä painottaa nimenomaan

[878] Lohse 2015: 765; HE 221/2013 vp: 196–197; HE 125/2003 vp: 71.
[879] HE 226/2018 vp: 48
[880] HE 221/2013 vp: 188–189; Heiskanen 2020: 108.

automaattisia toimenpiteitä. Lisäksi toimenpiteet on toteutettava huolellisesti sekä mitoittaen suhteessa torjuttavan häiriön vakavuuteen.

Näiden toimien tavoitteena on viestintäverkkojen ja niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitseminen, estäminen, selvittäminen ja esitutkintaan saattaminen. Lisäksi toimien tavoitteena voi olla myös viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaaminen taikka viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisy. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta, luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä kyseisten tavoitteiden turvaamiseksi. Esimerkiksi luottamuksellisen viestin periaatteen osalta yksittäisen viestin sisältöä saa käsitellä manuaalisesti, jos a) viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn; ja b) viestin sisältöä koskevalla automaattisella selvittämisellä ei pystyä turvaamaan aikaisemmin mainittujen tavoitteiden toteutumista. Manuaalisesta viestin sisällön käsittelystä on tosin ilmoitettava viestin lähettäjälle ja vastaanottajalle, mikäli se ei vaaranna edellä mainittuja tavoitteita, kuten asian esitutkintaan saattamista.[881] Sähköisen viestinnän palvelulain 272 § mahdollistaa sekä asettaa rajoja teknisin menetelmin toteutetulle valvonnalle. Nykypäivänä teknisin menetelmin toteutettu valvonta kattaa paljon automaattisia, anomalioiden tunnistamiseen liittyviä tietoturvatyökaluja, jotka hälyttävät poikkeamista ja tekevät automaattisia hyökkäysten estoja. On tärkeää tunnistaa kyberuhkia sekä ehkäistä niitä proaktiivisesti, jotta organisaatioiden ja yhteiskunnan toimivuus sekä luonnollisten henkilöiden perusoikeudet olisivat turvattuja.

Yhteenvetona todettakoon, että organisaation tekemä *teknisin menetelmin toteutettu (tietoturva)valvonta* nostaa organisaation tietoturvatasoa mahdollistamalla tietoturvauhkien ennakoivan havaitsemisen sekä automaattiset tietoturvahyökkäysten estämiset. Sähköisen viestinnän palvelulain 272 § on tärkeä työkalu organisaatioiden tietoturvan kannalta, sillä se mahdollistaa sellaisen teknisin menetelmin toteutetun tietoturvavalvonnan, joka ottaa huomioon myös yksilöt ja heidän oikeutensa yksityisyyteen. Organisaation työntekijöillä on katsottu olevan kohtuullinen odotus yksityisyytensä suojaan, jolloin teknisin menetelmin toteutetun valvonnan ja tietoverkon järjestäminen kuuluvat yhteistoiminnan piiriin, työntekijän sallitun valvonnan on oltava tarkkarajaista ja työnantajan on annettava ohjeet henkilökunnalle tietoverkon käytöstä. Esimerkiksi valvonnassa käsiteltävät viestinnän välitystiedot katsotaan kuuluvan luottamuksellisen viestinnän perusoikeuden suojan alaan. Pääsääntöisesti työelämän tietosuojalain reunaehtoihin ja

[881] Sähköisen viestinnän palvelulaki 272 §.

työnantajan direktio-oikeuteen liittyen lokitietoja ei saa käyttää työntekijän yksityiskohtaiseen valvontaan, tarkkailuun eikä viestintäyhteyksien seurantaan keräämällä välitystietoja henkilörekisteriksi[882].

Teknisin menetelmin toteutettu valvonta lokien avulla on monimutkainen kokonaisuus, sillä lokitietojen keräämiseen ja käsittelyyn liittyvä lainsäädäntö ei ole suoraviivaista. Tämä johtuu siitä, että lainsäädännöstä on tunnistettavissa sekä järjestelmien lokitukseen liittyviä vaatimuksia[883] että välitystietoina toimivien lokitietojen käsittelyyn liittyviä vaatimuksia sähköisen viestinnän palvelulaissa. Lokitietojen osalta tulee ensiksi selvittää, onko kyseessä sähköisen viestinnän palveluista annetun lain mukainen välitystieto ja tietosuoja-asetuksen mukainen henkilötieto. Välitystieto on oikeus- tai luonnolliseen henkilöön yhdistettävissä oleva tieto, jota käsitellään viestien välittämiseksi. Esimerkiksi IP-osoitteet voivat olla välitystietoja silloin, kun niitä käsitellään viestin välittämiseksi. Kaikissa tapauksissa IP-osoitetta ei välttämättä tulkita kuitenkaan henkilötiedoksi, sillä tulkinnassa tulee huomioida muun muassa eri toimijoiden toimialasidonnaiset eroavaisuudet sekä käytettävissä olevat oikeuskeinot[884]. Tämä tulkinta ei kuitenkaan estä sitä, etteikö IP-osoite silti voisi olla välitystieto - tällöin sen tulee voida olla yhdistettävissä oikeushenkilöön. Mikäli kyseessä on välitystieto, tulee myös selvittää, mikä on organisaation roolitus sähköisen viestinnän palveluista annetun lain pohjalta. Työnantajana toimiva organisaatio voi olla sekä viestinnän välittäjä että yhteisötilaaja. Toisaalta organisaatio voi olla myös lisäarvopalvelun tarjoaja. Roolien määrityksen myötä on mahdollista tunnistaa lain vaatimat vastuut ja velvoitteet. Näin ollen sähköisen viestinnän palveluista annettu laki on hyvinkin keskeinen säädös lokitietojen käsittelyn osalta teknisin menetelmin toteutetussa tietoturvavalvonnassa, mutta myös tietosuojalainsäädäntö saattaa tulla sovellettavaksi.

3.5.5 Väärinkäytösten ehkäiseminen ja selvittäminen organisaatiossa

Organisaatioiden tietoturvallisuuden parantamiseksi on mahdollista käsitellä myös välitystietoja väärinkäytösten selvittämiseksi sähköisen viestinnän palveluista annetun lain 146–156 §:n puitteissa, jotka kuuluvat yhteisötilaajaa [885]

[882] Pesonen 2013:162.
[883] Esimerkiksi viranomaisen tiedonhallintalain 17 §. Ks. luku 4.4.2 (”Järjestelmien lokitusvaatimukset tietoturvan sääntelyjärjestelmässä”).
[884] Ks. lisää pohdintaa luvussa 3.2.1 (”Henkilötieto ja erityinen henkilötieto”).
[885] Sähköisen viestinnän palveluista annetun lain 3 §:ssä yhteisötilaajalla tarkoitetaan viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä ja yhteisöä, joka käsittelee viestintäverkossaan käyttäjien viestejä, välitystietoja tai sijaintitietoja. Hallituksen esityksen (HE 221/2013 vp, s. 95) mukaan yhteisötilaaja voi olla esimerkiksi elinkeinonharjoittaja, osuuskunta, osakeyhtiö, yhdistys, yliopisto tai valtion virasto. Yhteisötilaaja voi tilata viestintäpalvelun tai lisäarvopalvelun käyttäjiensä, esimerkiksi työntekijöidensä

koskevan erityissääntelyn alle. Mikäli välitystiedot voidaan liittää tunnistettavissa olevaan henkilöön eli kyseessä on henkilötieto, myös tietosuoja-asetuksen vaatimukset tulee ottaa huomioon tarpeellisessa laajuudessa mukaan lukien myös työelämän tietosuojalain vaatimukset. Siitäkin huolimatta, kuuluuko yhteisötilaajan roolissa toimiva työnantaja yhteistoimintalainsäädännön piiriin, työnantajan on vähintään kuultava työntekijöitä lain 146–156 §:ään liittyvien välitystietojen käsittelyn perusteista ja käytännöistä sekä tiedotettava niistä työntekijöille[886].

Sähköisen viestinnän palveluista annetun lain 146 §:ssä säädetään yhteisötilaajan, esimerkiksi työnantajan, oikeudesta käsitellä välitystietoja maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön taikka liikesalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi siten kuin lain 147–156 §:ssä säädetään. Tällainen käsittelyoikeus liittyy muun muassa yhteisötilaajien viestintäverkkojen ja viestintäpalveluiden käytön turvaamiseen[887]. 148 §:ssä myös painotetaan, että välitystietoja voivat käsitellä vain yhteisötilaajan viestintäverkon ja -palvelun ylläpidosta ja tietoturvasta sekä turvallisuudesta huolehtivat henkilöt. Huomioitava on, että laissa määriteltyjä väärinkäytöksiä ovat nimenomaan luvaton käyttö ja liikesalaisuuksien paljastaminen, joiden ehkäisemiseksi ja selvittämiseksi välitystietojen käsittely on mahdollista tietyt tietoturvatoimenpiteet toteuttaen.

Sähköisen viestinnän palvelulaki on yhteisötilaajaa koskevan sääntelyn osalta merkityksellinen, sillä se asettaa vaatimuksia toteuttaa tietoturvatoimenpiteitä organisaatiossa väärinkäytösten ehkäisemiseksi. Näin ollen lain 147 § asettaa työnantajana toimivalle organisaatiolle velvollisuuksia proaktiivisesti ennaltaehkäistä viestintäverkon ja -palvelunsa luvatonta käyttöä sekä liikesalaisuuksien paljastumista.

> Lain 147 §:n mukaan yhteisötilaajan on **luvattoman käytön ehkäisemiseksi** a) rajoitettava viestintäverkkonsa ja -palvelunsa pääsyä ja käyttöä; b) suojattava viestintäverkkonsa ja -palvelunsa käyttöä asianmukaisin tietoturvatoimenpitein; sekä c) määriteltävä minkälaisia sähköisiä viestejä viestintäverkon kautta saa välittää ja hakea, miten viestintäverkkoa ja -palvelua saa käyttää ja minkälaisiin kohdeosoitteisiin viestintää ei saa harjoittaa.

---

käytettäväksi. Tällöin tätä tarkoitusta varten yhteisötilaaja hallinnoi samalla omaa viestintäverkkoaan sekä tietojärjestelmää, jossa käsitellään käyttäjien välitystietoja ja sijaintitietoja erilaisin palvelimin ja päätelaittein. Näin ollen yhteisötilaajalle myös kertyy teknisiin järjestelmiin käyttäjien välitystietoja ja esimerkiksi sähköpostijärjestelmissä luottamuksellisia viestejä.

[886] Sähköisen viestinnän palvelulain 148 §.

[887] HE 48/2008 vp: 19; Hoikka, Neuvonen & Rautiainen 2016: 364.

> **Liikesalaisuuksien[888] paljastamisen ehkäisemiseksi** yhteisötilaajan pitää vastaavasti a) rajoittaa pääsyä liikesalaisuuksiin[889]; b) suojattava viestintäverkkonsa ja -palvelunsa käyttöä ja tietoja asianmukaisilla tietoturvatoimenpiteillä; sekä c) määriteltävä miten liikesalaisuuksia saa siirtää, luovuttaa tai muutoin käsitellä viestintäverkossa ja minkälaisiin kohdeosoitteisiin liikesalaisuuksia käsittelemään oikeutetut henkilöt eivät ole oikeutettua lähettämään sähköisiä viestejä. Yhteisötilaajan tulee huolehtia riittävästä tietoturvallisuuden tasosta[890]. Liikesalaisuudet on tosiallisesti suojattava niiden käsittelyn kannalta ulkopuolisilta tahoilta ja liikesalaisuutena suojattavan tiedon kanssa tekemisiin joutuvien olisi miellettävä tieto salaiseksi[891].

Lain 147§:n mukaan väärinkäytösten ehkäisemiseksi yhteisötilaajan on myös annettava kirjalliset ohjeet viestintäverkon tai viestintäpalvelun käyttäjälle, eli esimerkiksi työntekijöille. Välitystietojen käsittelyn salliminen edellyttää myös, että käyttäjällä on tieto tällaisista ohjeista[892]. Henkilökunnan säännöllisellä kouluttamisella ja tiedottamisella sekä uusien henkilöiden perehdyttämisellä tieto ohjeistuksista on ketterintä saattaa henkilökunnan tietoisuuteen. Isommissa organisaatioissa saattaa olla myös käytössä käyttösääntöjä, esimerkiksi käyttäjätunnusten ja IT-palveluiden sallitusta ja kielletystä käytöstä, joita käyttäjä sitoutuu noudattamaan työsuhteen alussa käyttäjätunnukset aktivoidessaan tai allekirjoittaessaan työsopimuksen.

Niin kuin laissa on mainittu, yhteisötilaajan on määriteltävä niin sanotut raamit muun muassa sähköisten viestien välittämiselle, hakemiselle ja lähettämiselle, liikesalaisuuksien siirtämiselle, luovuttamiselle ja muutoin käsittelemiselle sekä miten viestintäverkkoa ja -palvelua saa käyttää. Tämä tarkoittaa myös dokumentoituja periaatteita.

---

888 Liikesalaisuuslaissa liikesalaisuudella tarkoitetaan tietoa:
a) joka ei ole kokonaisuutena tai osiensa täsmällisenä kokoonpanona ja yhdistelmänä tällaisia tietoja tavanomaisesti käsitteleville henkilöille yleisesti tunnettua tai helposti selville saatavissa;
b) jolla edellä mainitun ominaisuuden vuoksi on taloudellista arvoa elinkeinotoiminnassa; ja
c) jonka laillinen haltija on ryhtynyt kohtuullisiin toimenpiteisiin sen suojaamiseksi.

889 Käytännössä tämä tarkoittaa sitä, että organisaatiossa vain tiettyjä tehtäviä hoitavat käyttäjät pääsevät liikesalaisuuksiin käsiksi. Pääsyä voidaan käytännössä rajoittaa muun muassa tietohallinnollisin toimenpitein, kuten käyttäjätunnuksin ja salasanoin tai muuten käyttäjäoikeuksia hallinnoimalla. Ks. HE 48/2008 vp, s. 22.

890 HE 48/2008 vp: 21; Hoikka, Neuvonen & Rautiainen 2016: 366.

891 HE 221/2013 vp: 155; Hoikka, Neuvonen & Rautiainen 2016: 367.

892 Hoikka, Neuvonen & Rautiainen 2016: 366.

Oleellinen huomio 147 §:n vaatimuksissa kohdistuu rajoitukseen, minkälaisiin kohdeosoitteisiin viestintää ei saa harjoittaa. Tällaiset kielletyt kohdeosoitteet voidaan määritellä kohtuullisen yleisellä tasolla[893]. Esimerkiksi kielletyiksi kohdeosoitteiksi olisi mahdollista määritellä kaikki ilmaiset webmail-osoitteet[894]. Käytännön tasolla organisaatioissa tulisi kieltää työntekijöiden työsähköposteista tehtävät automaattiset edelleen lähetyssäännöt kuluttajakäyttöön tarkoitettuihin heikomman tietoturva- ja tietosuojatason omaaviin sähköposteihin, jotka ovat työntekijöiden henkilökohtaisessa käytössä. Automaattiset edelleen lähetykset rikkovat myös useampaa tietosuojaperiaatetta[895], joita tietosuojalainsäädännön mukaan tulisi noudattaa koko henkilötietojen käsittelyn elinkaaren ajan. Usein onkin tehokkaampaa tehdä teknisiä estoja, esimerkiksi sähköpostin edelleen lähetyssääntöjen suhteen, kuin pelkästään ohjeistaa käyttäjää. Tämä korostuu myös henkilötietojen suojaamisessa osana oletusarvoista tietosuoja *”Privacy by Default”*: mikäli on vaihtoehtoja, tekniset toimenpiteet on priorisoitava ja toteutettava ensisijaisesti henkilötietojen tosiasiallisen suojaamisen suhteen. Tällöin dokumentointi ja ohjeistus on toissijaista. Järjestelmien ominaisuudet tulisi suunnitella niin, että ne minimoisivat inhimillisiä virheitä sekä näistä virheistä aiheutuvia riskejä[896].

Siitäkin huolimatta, että yhteisötilaajana toimiva työnantajaorganisaatio toteuttaisi sähköisen viestinnän palvelulain 147 §:n mukaiset ennakoivat tietoturvatoimenpiteet, väärinkäytöksiä saattaa silti ilmetä. Lain 149 § mahdollistaa yhteisötilaajalle välitystietojen käsittelyn työntekijöiden yksityisyys huomioon ottaen tietoyhteiskunnan palvelunsa sekä viestintäverkkonsa ja -palvelunsa luvattoman käytön selvittämiseksi. Samoin 150 § mahdollistaa välitystietojen käsittelyn liikesalaisuuksien paljastamisen selvittämiseksi. Tällöinkin välitystietojen käsittelyssä painotetaan automatiikkaa, aivan kuten teknisin menetelmin toteutettua valvontaa koskevassa sähköisen viestinnän palvelulain 272 §:ssä.

> Sähköisen viestinnän palveluista annetun lain 149 §:n mukaan yhteisötilaaja saa käsitellä välitystietoja **luvattoman käytön selvittämiseksi** automaattisen hakutoiminnon avulla, mikäli tapahtuma tai teko aiheuttaisi todennäköisesti yhteisötilaajalle merkittävää haittaa tai vahinkoa. Merkittävä haitta voisi muun muassa olla lisääntyneet kustannukset tai sellainen lisääntynyt tiedonsiirtokapasiteetin käyttö, tietoturvauhka, tai

[893] HE 48/2008 vp: 22.
[894] Ks. Nyblin 2008: 547–548.
[895] Tietosuojaperiaatteita ovat muun muassa käyttötarkoitussidonnaisuus, lainmukainen ja asianmukainen käsittely, läpinäkyvyys, tietojen minimointi, tarpeellisuus, luottamuksellisuus ja turvallisuus sekä rekisteröityjen oikeuksiin liittyvät periaatteet, kuten muun muassa tietojen tarkastaminen, poistaminen ja oikaiseminen.
[896] Saarenpää 2018: 26. Ks. lisää vastaavaa pohdintaa luvusta 4.4.1 (”Järjestelmien elinkaarimalli osana oikeudellista suunnittelua”).

> muu vastaava syy, joka vaarantaa, vaikeuttaa tai hidastaa viestintäverkon tai palvelujen käyttöä niille suunniteltuun käyttötarkoitukseen[897].
>
> Lain 150 §:n mukaan **liikesalaisuuden paljastamisen selvittämiseksi** välitystietojen käsittelyn automaattisen hakutoiminnon avulla edellytyksenä on se, että epäilty liikesalaisuuden paljastaminen kohdistuu yhteisötilaajan tai sen yhteistyökumppanin elinkeinotoiminnan kannalta keskeisiin liikesalaisuuksiin taikka teknologisen tai muun kehittämistyön tuloksiin, jotka todennäköisesti ovat merkittäviä elinkeinotoiminnan käynnistämisen tai sen harjoittamisen kannalta.

Lain esitöiden mukaan, mikäli käyttäjille annetut ohjeet ja muut tietoturvatoimenpiteet, joilla ei puututa käyttäjien viestintään, eivät ole riittäviä, välitystietoja voisi käsitellä lähtökohtaisesti automaattisen hakutoiminnon avulla[898]. Välitystietojen käsittely automaattisen hakutoiminnon avulla sekä luvattoman käytön että liikesalaisuuden paljastamisen selvittämisessä olisi mahdollista niin, että haku voisi perustua viestien kokoon, yhteenlaskettuun kokoon, tyyppiin, määrään, yhteystapaan tai kohdeosoitteisiin. Tällöin hakukone hakee viestintäverkosta automaattisesti poikkeamia tietyin ennalta määritellyin kriteerein[899], jolloin tällaisen määrittelyn tarkoituksena olisi se, että välitystietojen seuranta ei kohdistuisi tavanomaisiin sähköpostiviesteihin sekä rajoitukset olisivat muutoinkin asiallisia ja perusteltuja verkon käytön asiamukaisuuden varmistamisen kannalta[900]. Käsiteltäväksi saisi ottaa vain ne tiedot, jotka ovat välttämättömiä väärinkäytöksen selvittämiseksi[901].

Manuaaliselle välitystietojen käsittelylle on asetettu enemmän täytettäviä kriteerejä kuin automaattiselle välitystietojen käsittelylle:

> **Manuaaliselle välitystietojen käsittelylle luvattoman käytön selvittämiseksi** on asetettu ehdoksi *perusteltu syy* epäillä menettelyä kirjallisten ohjeiden vastaisesti ja, mikäli automaattisen hakutoiminnon avulla on havaittu viestinnässä poikkeama, tietoyhteiskunnan palvelun käytön kustannukset ovat nousseet epätavallisen korkeiksi, viestintäverkossa on

[897] HE 48/2008 vp: 25.
[898] HE 48/2008 vp: 39.
[899] HE 48/2008 vp: 24. Tällaiset ennalta määritellyt kriteerit voivat liittyä esimerkiksi viestin tyyppiin, yhteystapaan tai viestin kohdeosoitteeseen. Esimerkiksi viestin tyypillä tarkoitetaan viestin, sen osan tai liitteen tallennusmuotoa, kuten esimerkiksi .doc tai .mp3. Viestin yhteystavalla tarkoitetaan esimerkiksi protokollaa, minkä mukaisena se viestintäverkossa välitetään, kuten http tai tcp. Viestin kohdeosoitteella tarkoitetaan sellaisia palveluja tai muita osoitteita, joihin suuntautuvaa liikennettä yhteisötilaaja on kieltänyt, rajoittanut tai estänyt sen kokonaan.
[900] HE 48/2008 vp: 24.
[901] HE 48/2008 vp: 37.

havaittu sinne oikeudetta asennettu laite, ohjelma tai palvelu; taikka muusta edellä rinnastettavissa, yleisesti havaittavista seikoista voidaan päätellä, että viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään annettujen kirjallisten ohjeiden vastaisesti.

Liikesalaisuuden paljastamisen selvittämiseksi manuaalisen välitystietojen käsittelyn avulla on asetettu ehdoksi *perusteltu syy* epäillä liikesalaisuuden luvatonta antamista viestintäverkkoa tai -palvelua käyttäen ja, mikäli automaattisen hakutoiminnon avulla on havaittu viestinnässä poikkeama, liikesalaisuus julkaistaan tai sitä käytetään luvatta; taikka yksittäistapauksessa muusta edellä rinnastuvasta, yleisesti havaittavissa olevasta seikasta voidaan päätellä, että liikesalaisuus on luvattomasti annettu ulkopuoliselle.

Viestintäverkkojen luvattoman käytön ja viestintäpalvelujen ohjeen vastaisen käytön selvittämiseksi soveltuvat esimerkiksi automaattiset kapasiteetin käyttömittarit tai tunkeutumisenestosovellukset, kuten palomuurit. Samoja sovelluksia käytetään myös automaattiseen kapasiteetin seurantaan sekä vika- ja häiriötilanteiden havaitsemiseen. Samoilla sovelluksilla yhteisötilaajat voivat myös määritellä viestintäverkkonsa ja -palvelunsa käytölle rajat esimerkiksi estämällä liikennöinnin omasta verkostaan tiettyihin yhteysosoitteisiin taikka estämällä tietyn tyyppisen liikenteen kokonaan.[902]

Esimerkkinä voidaan mainita liikesalaisuuden paljastamisen selvittämiseksi tietohallinnollisina keinoina käyttäjälokien tarkastaminen, pääsyä rajoittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Näistä tiedoista käy ilmi, kuka on tallentanut mitäkin tietoja, missä muodossa, koska ja mille tallenteelle, minkä vuoksi tällaisten tietojen käsittelylle ei laissa aseteta rajoituksia.[903] Näin ollen yhteisötilaajalla on ilman lainsäädännön asettamia rajoituksia mahdollisuus selvittää omista tietojärjestelmistään, kuka on käsitellyt paljastettua liikesalaisuustietoa ja rajata potentiaalinen tekijäpiiri rikosilmoituksen tekemiseksi, mikäli liikesalaisuutta on suojattu tietojärjestelmässä asianmukaisella tavalla[904]. Rikosilmoituksen tekemisen osalta pitää myös muistaa, että esitutkintakynnyksen ylittyminen edellyttää, että on riittävästi selvitystä jonkin nimenomaisen rikoksen tekemisestä. Näin ollen ei ole riittävää pelkkä näyttö siitä, että joku saattaa tehdä rikoksen. Tällöin kannattaa tarkastella, täyttyisikö esimerkiksi rikoslain 30 luvun 4 §:ssä tarkoitetun yritysvakoilun tunnusmerkistön sijaan rikoslain 30 luvun 5 §:ssä tarkoitetun yrityssalaisuuden

[902] HE 48/2008 vp: 24.
[903] HE 48/2008 vp: 20, 39.
[904] Lehtonen 2008: 566.

rikkomisen tunnusmerkistö[905]. Esimerkiksi työntekijän kopioimat ja itselleen yksityiseen sähköpostiinsa lähettämät liikesalaisuuksia sisältävät tallenteet eivät vielä ole sellaisenaan liikesalaisuuden ilmaisemista toiselle[906].

Sekä luvattoman käytön että liikesalaisuuden paljastamisen selvittämiseksi on manuaalisen välitystietojen käsittelyn lisäedellytykseksi alleviivattu se, että *tietojen on oltava välttämättömiä luvattoman käytön ja siitä vastuussa olevien selvittämiseksi sekä luvattoman käytön lopettamiseksi taikka liikesalaisuuden paljastamisen ja siitä vastuussa olevien selvittämiseksi.* Tämä korostaa sitä seikkaa, että viestintäverkon käyttö ja liikesalaisuuksien luottamuksellisuus olisi ensisijaisesti pyrittävä takaamaan keinoilla, joissa ei puututa lainkaan viestinnän välitystietoihin, kuten esimerkiksi käyttäjähallinto- ja tietoturvatoimenpiteillä sekä käyttäjien ohjeistuksilla[907]. Tietojärjestelmiä voidaan seurata vapaasti muun muassa väärinkäytöksiä selvittäessä erilaisten lokitietojen avulla. Kuitenkin jokainen teknisin menetelmin toteutettu valvonta ja sen oikeutus on arvioitava erikseen sitä mahdollisesti koskevien erityissäännösten pohjalta sekä viime kädessä soveltamalla työelämän tietosuojalain tarpeellisuusvaatimusta. Lisäksi valvontatoimenpiteen oikeutus ei poista työnantajalta velvollisuutta käsitellä asiaa yhteistoimintamenettelyssä tai kuulla työntekijöitä sekä tiedottaa valvonnasta.[908]

Edellä mainitut tietoturvatoimenpiteet ovat erityisen kattavia ja onkin kritisoitu, miksi tarvitaan erillisiä välitystietojen käyttöoikeuksia. Esimerkiksi liikesalaisuuksien paljastamista ei olisi välttämättä tarpeen selvittää jälkikäteen välitystietojen avulla yhteisötilaajan toimesta, koska yhteisötilaajalla on etukäteen mahdollisuus estää ongelman realisoituminen. Potentiaaliset liikesalaisuuksien vastaanottajat ovat yleensä tunnettuja kilpailijoita, jolloin esimerkiksi yhteisötilaajan tietojärjestelmässä voidaan sulkea käytön ulkopuolelle sellaiset kohdeosoitteet, joihin liikesalaisuuksia käsittelemään oikeutetut henkilöt eivät saa lähettää viestejä tai muutoin olla yhteydessä. Lisäksi sähköpostijärjestelmän käyttäminen liikesalaisuuden paljastamiseen on epätodennäköistä ilmeisen paljastumisen vaaran takia ja muitakin tiedonsiirtotapoja on mahdollista käyttää, esimerkiksi tiedon sisältävän tallenteen postittaminen tai tapaaminen kasvotusten[909]. Näin ollen välitystietojen käsittelyoikeus ei välttämättä ole tarpeellinen eikä välttämätön liikesalaisuuden paljastamisen selvittämiseksi, sillä asianomistaja pystyy hankkimaan tarpeelliset tiedot tietohallinnollisin keinoin ja ennakollisin tietoturvallisuustoimenpitein.[910]

---

[905] Ks. tarkemmin Rautio 2022: 1024–1032.
[906] Nyblin 2008: 540–541.
[907] HE 48/2008 vp: 37, 39.
[908] HE 48/2008 vp: 3–4; Nyblin 2009: 23–24.
[909] TyVL 14/2008 vp: 4.
[910] Lehtonen 2008: 567.

Lopuksi todettakoon, että hyvien käytänteiden mukaista on toteuttaa tietoturvatoimenpiteitä proaktiivisesti ongelmien ehkäisemiseksi kuin reaktiivisesti ”tulipaloja sammuttaen”. Lainsäädäntö antaa työkaluja sekä väärinkäytösten ehkäisemiseksi että selvittämiseksi. Sähköisen viestinnän palvelulain 147 § on tärkeä, huomioitava säännös ennaltaehkäisevien tietoturvatoimenpiteiden osalta, joita yhteisötilaajana toimivan työnantajaorganisaation tulee toteuttaa väärinkäytösten ehkäisemiseksi ennen mahdollisten toteutuneiden väärinkäytösten tutkimista. Tällaisia väärinkäytöksiä ovat tietoyhteiskunnan, viestintäverkon ja viestintäpalvelun luvaton käyttö sekä liikesalaisuuksien paljastaminen. Laissa määritellyt tietoturvatoimenpiteet ennen välitystietojen käsittelyä väärinkäytösten ehkäisemiseksi ovat jo itsessään erittäin tehokkaita vahingontorjujia, mutta ne pitää ottaa käyttöön kattavasti toimiakseen ennaltaehkäisevästi.

Huomioitava on se, että sähköisen viestinnän palvelulain tietoturvatoimenpiteiden vaatimukset ilmenevät organisaatioiden tietoturvan sääntelyjärjestelmässä irrallisina, jolloin organisaatioilta vaaditaan lainsäädännön tuntemista. Lain vaatimusten tavoitettavuus ja ymmärrettävyys voi olla haastavaa etenkin pienemmissä organisaatioissa, joissa tietoturva ei välttämättä ole toimialan erityisosaamista ja resursointi on huonoa. Sääntelyn kokoaminen tietoturvan yleislakiin voisi edesauttaa sähköisen viestinnän palvelulain tietoturvavaatimusten tavoitettavuutta ja ymmärrettävyyttä. Erityisesti lain 147 §:n väärinkäytöksiä ennaltaehkäisevät tietoturvatoimenpiteet ovat hyvän tietoturvatavan mukaisia, joita voisi kohdistaa kaikkiin organisaatioihin oletusarvioisesti. Nykyisellään 147 §:n tietoturvavaatimukset ikään kuin hukkuvat tietoturvan sääntelyjärjestelmän muiden tietoturvasäännösten joukkoon, jolloin riski syntyy erityisesti alhaisen tietoturvamaturiteetin omaavien organisaatioiden osalta siitä, että säännöksen vaatimuksista ei olla tietoisia tai niitä ei ymmärretä.

3.5.6 Henkilöstöturvallisuus: työntekijöiden luotettavuus ja tiedon salassapito

Henkilöstöturvallisuus voidaan nähdä omana tietoturvallisuuden osa-alueena, mutta yksinkertaisemmassa jaottelussa se voidaan sijoittaa myös hallinnollisen tietoturvallisuuden alle. Henkilöstöturvallisuus kattaa tietoturva-asiat työntekijän koko työsuhteen tai ulkoistussuhteen elinkaaren ajalta eli jo henkilön rekrytointiprosessista työn tai toimeksiannon päättymiseen saakka ja sen jälkeen.

Henkilöstöturvallisuus on kiinteä osa riskienhallintaa ja sen sääntelyn kehitykseen ovat vaikuttaneet EU:n sääntelyn lisäksi työelämän rakenteelliset uudistukset ja

uudenlaiset turvallisuusuhat, kuten kyberrikokset ja teollisuusvakoilu[911]. Tämä heijastuu myös NIS 2 -direktiivin 21 artiklasta, jonka mukaan osana kyberturvallisuusriskien hallintatoimenpiteitä tulee huomioida henkilöstöturvallisuus[912]. Itse direktiivissä on erotettu kyberturvallisuuskoulutus omaksi kyberturvallisuusriskien hallintatoimenpiteekseen, mutta kansallisessa kyberturvallisuuslain 9 §:n kohdassa 6 henkilöstöturvallisuus ja kyberturvallisuuskoulutus on sijoitettu samalle toimenpideriville. Tämä on hyvä asia, koska tyypillisesti henkilöstön tietoturvaosaaminen on osa henkilöstöturvallisuutta.

Henkilöstöturvallisuuden menettelyillä varmistetaan henkilöiden tietoturvavastuut ja velvollisuudet, tietoturvaosaaminen ja taustatarkastukset sekä avainhenkilöriskien hallinta. Lisäksi nämä menettelyt kattavat väärinkäytösten estämistä, kuten vaarallisten työyhdistelmien tunnistamista ja välttämistä, työtehtäväkiertoa, sekä työsuhteen tai sopimuksen päättymisen.[913] Keskeisiä organisaation tietoturvaa parantavia, henkilöstöturvallisuuden ulottuvuuksia ovat näin ollen henkilöstön luotettavuuden ja tiedon salassapidon varmistaminen, sekä henkilöstön osaaminen ja vastuuttaminen. Tässä alaluvussa on tarkoituksena käydä läpi henkilöstön luotettavuuden ja tiedon salassapidon varmistamiseen liittyviä seikkoja henkilöstöturvallisuuden näkökulmasta, kun taas jäljempänä[914] käsitellään työntekijöiden osaamiseen ja vastuisiin liittyviä asioita.

Henkilöstöturvallisuudesta ei ole säädetty kansallisesti yhtä asianmukaisesti ja yhtenäisesti missään toisessa säädöksessä kuin mitä edellä mainitussa NIS 2 -direktiivin toimeenpanevassa kyberturvallisuuslaissa. Henkilöstön luotettavuudesta ja salassapidon varmistamisesta on kuitenkin hajanaisesti kansallisessa lainsäädännössä eri säännöksiä, jotka tulevat olemaan voimassa tulevaisuudessakin kyberturvallisuuslain rinnalla.

---

[911] Paasonen, Lindfors & Vainio 2022: 962.
[912] NIS 2 -direktiivin kohdan 79 mukaisesti kriittisten toimialojen toimijoiden on käsiteltävä kyberturvallisuusriskien hallintatoimenpiteissään henkilöstöturvallisuutta CER-direktiivistä ilmaistujen toimenpiteiden mukaisesti. CER-direktiivin 13 artiklan mukaan asianmukaisia toimenpiteitä henkilöstöturvallisuuden hallinnan varmistamiseksi ovat muun muassa kriittisiä tehtäviä hoitavien sekä taustatarkistuksia vaativien henkilöstöryhmien määrittäminen, pääsyoikeuksien vahvistaminen tiloihin, kriittiseen infrastruktuuriin ja arkaluonteisiin tietoihin pääsemiseksi sekä asianmukaisten koulutusvaatimusten ja pätevyyksien vahvistaminen.
[913] HE 57/2024 vp: 165. Hallituksen esityksessä henkilöstöturvallisuus on sisällöllisesti asianmukaisesti muotoiltu. Vrt. esim. Katakri, jossa henkilöstöturvallisuuden menettelyihin työsuhteen alussa ja aikana kuuluvat muun muassa henkilöturvallisuusselvitykset, salassapito- ja vaitiolovelvollisuusklausaalien ulottaminen sopimuksiin ja ohjeistuksiin ja niiden ymmärtäminen, käsittely-, käyttö- ja pääsyoikeudet sekä turvallisuuskoulutukset. Työsuhteen päättyessä henkilöstöturvallisuuden menettelyihin sisältyy esimerkiksi työnantajalle kuuluvien avainten, tägien ja laitteiden sekä tietoaineistojen luovutus sekä käsittely-, käyttö- ja pääsyoikeuksien poistaminen.
[914] Seuraava luku 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).

Yhtenä keskeisenä tarkasteltavana henkilöstöturvallisuuteen liittyvänä säädöksenä on luonnollisesti työelämän tietosuojalaki. Työelämän tietosuojalainsäädännön soveltamisala on laaja, jolloin laki ulottuu koskemaan myös yksityisen ja julkisen sektorin työnhakijaa. Työnhakijalla tarkoitetaan henkilöä, joka on hakenut avoinna olevaa työpaikkaa tai virkaa taikka, johon työnantaja on ottanut yhteyttä mahdollisen työhön ottamisen tarkoituksessa.[915] Yksityisyyden suojan toteuttaminen vaatii työnantajalta suunnitelmallisuutta, sillä kerättävien henkilötietojen on oltava tarpeellisia, käyttötarkoitussidonnaisuuden mukaisia ja tietojen käsittelyn on oltava asiallisia. Työnhakijasta kerättävien tietojen määrä ja sisältö on suunniteltava etukäteen.[916]

Organisaation tietoturvariskien hallinnan kannalta on kuitenkin oleellista tehdä taustaselvityksiä työnhakijoista ennen kuin uusi työntekijä pääsee käsiksi organisaation luottamuksellisiin tietoihin tai ei-julkisiin tiloihin. Näin ollen niin sanotut rekrytointien (ja toimeksiantojen) tietoturvallisuusvaatimukset tulee olla tiedossa hyvissä ajoin. Hyvien tietoturvallisten käytänteiden mukaisesti tulisi vähintään todentaa hakijan henkilöllisyys sekä tarkistaa taustat esimerkiksi verifioimalla opinto- ja työtodistukset oikeiksi. Tarvittaessa myös muunlaiset taustatarkistukset saattavat olla tarpeen. Henkilöluottotietojen käsittelystä säädetään työelämän tietosuojalain 5 a §:ssä ja huumausainetestiä koskevasta todistuksen käsittelystä säädetään työelämän tietosuojalain 7–8 §:ssä. Esimerkiksi lain 7 §:n mukaan työnantaja saa käsitellä huumausainetestiä koskevaan todistukseen merkittäviä tietoja tehtävään valitun työnhakijan suostumuksella vain silloin, kun työnhakijan on tarkoitus toimia sellaisessa työssä, joka edellyttää tarkkuutta, luotettavuutta, itsenäistä harkintakykyä tai hyvää reagointikykyä, ja jossa työtehtävien suorittaminen huumeiden vaikutuksen alaisena tai huumeista riippuvaisena voi vaarantaa työtehtävissä saatujen tietojen suojaa, käytettävyyttä, eheyttä ja laatua ja siten aiheuttaa haittaa tai vahinkoa salassapitosäännösten suojaamille yleisille eduille tai vaarantaa rekisteröityjen yksityisyyden suojaa tai oikeuksia. Työnhakija (tai työntekijä) toimittaa työnantajalle huumaisainetestiä koskevan todistuksen. Näin ollen työnhakijalla ei ole velvollisuutta toimittaa todistusta, mutta vastaavasti työnantaja voi jättää rekrytoimatta työnhakijan, joka ei toimita todistusta työnantajalle[917].

Työnantajan tulee hankkia ensisijaisesti työnhakijaa ja työntekijää koskevat tiedot häneltä itseltään. Työelämän tietosuojalain 4 §:n mukaan suostumusta ei

---

[915] Alapuranen 2020: 19; HE 75/2000 vp: 14.
Työnhakijoiden asema on erityisen ongelmallinen henkilötietojen käsittelyn ja yksityisyyden suojan kannalta, sillä yksityisyyden suojan loukkaukset ovat todennäköisiä ja työnhakijat itsekään eivät välttämättä kunnioita kyseistä suojaa. Ks. Koskinen 2020, s. 172.
[916] Koskinen 2020: 181.
[917] Koskinen & Ullakonoja 2020: 95.

kuitenkaan tarvita, mikäli viranomainen luovuttaa tietoja työnantajalle työelämän tietosuojalaissa säädetyn tehtävän suorittamiseksi tai jos tietojen keräämisestä tai saamisesta laissa erikseen nimenomaisesti säädetään. Näin ollen muun tietolähteen käyttäminen ei ole sallittua, paitsi jos siihen on saatu lupa tai kyseessä on erityistä luottamusta vaativa tehtävä. Luotettavuuden selvittäminen tulee ajankohtaiseksi erityisesti sellaisten henkilövalintojen yhteydessä, jolloin tehtävän hoitajalta edellytetään erityistä luottamusta, esimerkiksi salassa pidettävää tietoa käsitellään paljon tai työtehtävät vaativat laajoja pääsyoikeuksia järjestelmissä, taikka henkilölle annetaan taloudellista vastuuta.[918] Taustojen tarkistamiseksi ei pääsääntöisesti saa käyttää muita tietolähteitä kuin työnhakijalta itseltään saatuja tietoja (ellei ole suostumusta). Tällöin esimerkiksi työnhakijan henkilöllisyyden ja työhistorian verifioiminen käyttämällä Googlea ei ole asianmukaista. Ongelmallista työnhakijaa koskevien tietojen etsimisessä internetistä on tietojen epäluotettavuus, eikä Googlaamalla löydetyn tiedon kerääminen voi täyttää työelämän tietosuojalain tarpeellisuusvaatimusta[919].

Rekrytointiprosessiin saattaa kuulua luotettavuuden arvioinnin lisäksi mahdollisten turvallisuusselvitysten tekeminen salassa pidettävien aineistojen käsittelyyn osallistuville henkilöille. Katakri 2020 T10-vaatimuksessa painotetaan, että esimerkiksi viranomaisen on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Suositeltavaa olisi tällöin, että turvallisuusluokiteltuja tietoja käsittelevien henkilöiden luotettavuus selvitettäisiin tarvittaessa hakemalla henkilöstä asianmukaisen laajuinen henkilöturvallisuusselvitys. Selvitys voidaan hakea suppeana, mutta myös perusmuotoinen tai laaja turvallisuusselvitys ovat mahdollisia.

Henkilöturvallisuusselvitys ei koske ainoastaan viranomaisia vaan myös muita organisaatioita. Esimerkiksi yhteiskunnan kriittisen infrastruktuurin toiminnan varmistamisessa nousee esille tehtäviä, joissa ei välttämättä ole kysymys ainoastaan pääsystä tietoon, vaan mahdollisuuksista tosiasialliseen toimintaan. Tällaisia tehtäviä hoidetaan usein yksityisellä sektorilla, jolloin yksityisillä yrityksillä on merkittävä vastuu yhteiskunnan elintärkeiden toimintojen ylläpidossa. Turvallisuusselvitysmenettelyä voidaan toteuttaa näin ollen muun muassa yhteiskunnan toimivuuden kannalta merkityksellisen infrastruktuurin keskeisiä tehtäviä hoitavien taustojen selvittämiseksi.[920] Turvallisuusselvitys onkin vakiinnuttanut roolinsa

[918] Pesonen 2013: 164–165.
[919] Koskinen 2020: 232.
[920] HE 57/2013 vp: 16–17. Huomioitava on, että CER-direktiivin toimeenpanoa koskevassa hallituksen esitysluonnoksessa ehdotetaan perusmuotoisen turvallisuusselvityksen piiriin kuluvien tehtävien osalta muutosta turvallisuusselvityslain 19 §:ään. Aikaisemmin 19 §:n kohta 4 on painottanut tehtäviä, joissa voi vahingoittaa yhteiskunnan toimivuuden

osana rekrytointeja etenkin silloin, kun etsitään työntekijää kansallisen turvallisuuden tai erittäin merkittävän yksityisen taloudellisen edun kannalta tärkeisiin työtehtäviin[921].

Turvallisuusselvityslain (726/2014) tarkoituksena on säännellä sekä henkilöiden että yritysten luotettavuuden arviointia sekä tehostaa kokonaisturvallisuutta vahvistamalla yleistä turvallisuutta ja yritysturvallisuutta. Keskiössä ovat merkittävien yleisten ja yksityisten etujen turvaaminen, esimerkiksi merkittävä yksityinen taloudellinen etu.[922] Turvallisuusselvityksellä voidaan tarkoittaa sekä henkilö- että yritysturvallisuusselvitystä. Henkilöturvallisuusselvityksessä keskitytään henkilön taustojen selvittämiseen, kun taas yritysturvallisuusselvityksessä selvitetään yrityksen ja sen vastuuhenkilöiden luotettavuutta, yrityksen tietoturvallisuudentasoa ja sitoumustenhoitokykyä[923]. On hyvä tiedostaa tällaisten työkalujen olemassaolo. Lisäksi on huomioitava, että henkilöturvallisuusmenettelyyn pääseminen asettaa vähimmäisvaatimuksia organisaation tietoturvalle: yleisenä edellytyksenä on, että selvityksen hakijayritys on rajoittanut teknisillä ja muilla toimenpiteillä pääsyä suojattaviin tietoihin, huolehtinut toimitilojen ja tietojärjestelmien suojaamisesta sekä ryhtynyt muihin asianmukaisiin toimenpiteisiin tietoturvallisuuden ja muiden turvallisuusjärjestelyjen toteuttamiseksi. Edellä mainitut toimenpiteet voidaan lain mukaan toteennäyttää esimerkiksi hyväksytyn tietoturvallisuuden arviointilaitoksen antamalla todistuksella.[924] Esimerkiksi ISO/IEC 27001 -tietoturvallisuuden hallintajärjestelmän implementoimista ja ylläpitämistä koskevan sertifiointitodistuksen hankkiminen on varsin pätevä todiste organisaation tietoturvallisuuskäytännöistä.

Turvallisuusselvityslain 19–21 §:ssä säädetään perusmuotoisen, laajan sekä suppean henkilöturvallisuusselvityksen tekemisestä sekä näiden piiriin kuuluvista tehtävistä. Perusmuotoinen tai suppea henkilöturvallisuusselvitys voidaan myös 22 §:n mukaisesti tehdä organisaation työntekijälle, valittavalle työntekijälle tai ulkoistetulle työntekijälle, joka voisi aiheuttaa työnantajalle tai tämän asiakkaille taikka yhteistyökumppanille merkittävää taloudellista vahinkoa.

---

kannalta välttämättömän infrastruktuurin toimivuutta tai kriittisen tuotannon jatkuvuutta. Lakimuutoksella ehdotetaan, että kohdan loppuun tulisi lisäys ”--taikka voi näissä tehtävissään saamiensa salassa pidettävien tietojen oikeudettomalla käytöllä merkittävällä tavalla vaarantaa valtion turvallisuutta tai muuta merkittävää etua.” (Luonnos: Hallituksen esitys laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi, s. 129.) Näin ollen kyseisten tehtävien kautta tietoon pääsy lisättäisiin myös mukaan olennaiseksi seikaksi.

[921] Paasonen, Lindfors & Vainio 2022: 975.

[922] HE 57/2013 vp: 1, 25.

[923] Ks. turvallisuusselvityslain 3 §, 35 § ja 38 §.

[924] Turvallisuusselvityslain 18 §.

Työntekijä voisi aiheuttaa merkittävää taloudellista vahinkoa 1) saamalla tietojärjestelmään käyttöoikeudet, joiden käyttäminen oikeudettomasti voisi keskeyttää tai merkittävällä tavalla vaarantaa tietojärjestelmän toiminnan aiheuttaen esimerkiksi laajamittaisen tuotantotoiminnan keskeytymisen; taikka 2) saamalla käyttöönsä sellaisia tietoja liikesalaisuudesta, teknologisesta kehittämistyötä tai sen hyödyntämisestä niin, että tietojen oikeudeton luovuttaminen, käyttö tai muu käsittely aiheuttaisi taloudellista vahinkoa. Käytännössä esimerkiksi 1 kohdan mukaisia tehtäviä voisivat olla pääkäyttäjän tehtävät[925]. Tällöin myös aikaisemmin mainittujen yleisten turvallisuusvaatimusten lisäksi reunaehtoina henkilöturvallisuusselvityksen tekemiselle on kaksi muuta kriteeriä: organisaatioon voi sen toiminnan tai toimialan takia kohdistua yritysvakoilua tai selvityksen on oltava tarpeen erittäin tärkeän yksityisen taloudellisen edun suojaamiseksi[926].

Koska avoimuus on henkilötietojen suojan osalta keskeinen periaate ja tämä ilmenee myös yksityisyyden suojasta työelämässä annetussa laissa, avoimuutta korostetaan myös turvallisuusselvitysten tekemisten osalta. Henkilöturvallisuusselvityksen tekemisestä on lain mukaan ilmoitettava esimerkiksi työpaikkailmoituksessa tai muulla sopivalla tavalla, jotta hakijat tietäisivät ennakolta turvallisuusselvityksen tekemisestä. Tämä toimintatapa myös karsisi mahdollisesti hakijoita, jotka eivät täytä nuhteettomuusvaatimuksia, sekä täten yksinkertaistaisi valintaa ja vähentäisi tarpeettomien selvitysten laadintaa. Laki edellyttää myös turvallisuusselvityksen kohteen suostumusta, joka tulee antaa kirjallisena. Tällä on merkitystä myös henkilötietojen käsittelyn vaatimusten sekä avoimuuden turvaamisen kannalta. Suostumuksen varmistamisella oikeastaan samalla varmistetaan lain vaatima informointivelvoitteen toteutuminen eli se, ettei kenestäkään voida tehdä turvallisuusselvitystä hänen tietämättään.[927]

Työelämän tietosuojalain ja turvallisuusselvityslain lisäksi henkilöstöturvallisuudesta on säädetty myös kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) sekä tiedonhallintalaissa (906/2019)[928], jotka velvoittavat lähinnä viranomaisia. Esimerkiksi tiedonhallintalain 12 §:ssä velvoitetaan tiedonhallintayksiköitä tunnistamaan tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai lukuun toimivilta erityistä luotettavuutta. Tässä tulee huomioida myös organisaation ulkopuolella tehtävät käsittelytoimet[929]. Tiedonhallintayksiköiden lukuun toimivien tietojenkäsittelytoimet ovat merkityksellisiä huomioida siinä mielessä, että tiedon tie ulottuu usein myös organisaation ulkopuolelle, jonne organisaatiolla ei ole niin hyvää näkyvyyttä eikä

[925] HE 57/2013 vp: 43.
[926] Turvallisuusselvityslain 22 §.
[927] Turvallisuusselvityslaki 4–5 §; HE 57/2013 vp: 29.
[928] Paasonen, Lindfors & Vainio 2022: 962.
[929] Valtiovarainministeriön julkaisuja 2024:19: 13.

valvontamahdollisuuksia. Ongelma ei koske ainoastaan julkista sektoria, vaan myös yksityisellä sektorilla on käytössä ulkoistettua työvoimaa ja toimeksiantoja, jolloin organisaation omistamaa tietoa käsitellään organisaation tietojenkäsittelyympäristön ulkopuolella. Väärinkäytöksien riskiä mitigoidaan turvallisuusselvitysten lisäksi salassapitosopimuksilla.

Organisaation liikesalaisuuksien ja muiden luottamuksellisten tietojen suojaamista parantavia tekijöitä työntekijöiden luotettavuuden varmistamisen ohella ovat salassapitosopimukset (*non-disclosure agreement, "NDA"*), jotka tulee ulottaa työsopimussuhteisten työntekijöiden ohella organisaation ulkoistettuihin työntekijöihin, kuten siivoojiin, konsultteihin ja vartiointihenkilöstöön, sekä muunlaisiin toimeksiantoihin[930]. Huomioitava on myös sopimussuhteen jälkeinen aika: kirjallisten salassapitoklausaalien ja -sopimuksien (esimerkiksi työsopimusten tai toimeksiantosopimusten ohessa) on hyvä koskea myös sopimussuhteen päättymisen jälkeistä aikaa. Täysin työsuhteen perusteella syntyvä salassapitovelvollisuus lakkaa työsuhteen päätyttyä[931].

Salassapitoklausaalit ja -sopimukset eivät sinänsä suoraan estä väärinkäytöksiä, mutta niiden tarkoituksena on ennaltaehkäistä väärinkäytöksiä ja henkilötietojen tietoturvaloukkauksia. Rikoslaissa on erinäisiä vaitiolovelvollisuutta tai ilmaisukieltoa koskevia rikosnimikkeitä, joista työntekijöiden ja muiden sopimuskumppanien olisi syytä olla tietoisia.

Esimerkiksi salassapitorikosten yleisiä rikosnimikkeitä ovat salassapitorikos (RL 38 luku 1 §) ja salassapitorikkomus (RL 38 luku 2 §), jotka ovat asianomistajarikoksia ja niihin liittyy salassapitovelvollisuuden vastainen toiminta. Tällainen salassapitovelvollisuuden vastainen toiminta voi olla ilmaisukiellon rikkomista tai tietojen antamista sivulliselle, ja rikoksen kohteena on yksityisen henkilökohtaisia tai taloudellisia oloja taikka elinkeinoa koskeva seikka.[932]

Organisaatioita suojataan liikesalaisuuksien osalta myös rikosnimikkeillä yrityssalaisuuden rikkominen (RL 30 luku 5 §), yrityssalaisuuden väärinkäyttö (RL 30 luku 6 §) ja yritysvakoilu (RL 30 luku 4 §). Etenkin sananvapauden kannalta

---

[930] Liikesalaisuuksien suojaamiseksi työnantajat voivat käyttää tietoturvallisuustoimenpiteitä, joita ovat työntekijän kanssa tehtävät salassapitosopimukset sekä turvallisuusselvitykset. Ks. Ks. myös HE 48/2008 vp, s. 20.
Huomioitava kuitenkin on, että viranomaistoiminnan vaitiolovelvollisuus ei perustu täysin salassapitosopimuksiin, koska viranomaisen salassapidosta ja vaitiolovelvollisuudesta on säädetty laissa. Viranomaisen palveluksessa olevat henkilöt voivat antaa salassapitositoumuksen, jonka tarkoituksena on informoida virkamiehiä heidän salassapitovelvollisuudestaan. Ks. Laurikkala 2020, s. 50–51.
[931] Pesonen 2017: 287.
[932] Voutilainen 2019: 251–254.

merkityksellinen on yrityssalaisuuden rikkominen.[933] Rikoslaissa yrityssalaisuudella tarkoitetaan liikesalaisuutta[934], joka on määritelty erikseen liikesalaisuuslaissa (595/2018)[935]. Yrityssalaisuusrikoksien sääntelyuudistuksen taustalla vaikutti jo 90-luvulla muun muassa tietotekniikan uudet keinot, jotka nähtiin mahdollistaneen uusia tiedonhankintatapoja. Lisäksi tietovuotojen nähtiin olevan entistä todennäköisempiä ja vaikeampia jäljittää.[936] Huomioitava on, että yrityssalaisuusrikoksissa on oikeudettomuusedellytys[937], jota vastaavasti ei ole aikaisemmin mainituissa salassapitorikoksissa (RL 38 luvun 1§ ja 2§). Tällöin sellainen menettely, jota ei pidetä RL 30:5:n mukaisesti oikeudettomana, voidaan rangaista salassapitorikoksena tai -rikkomuksena.[938]

Viranomaistoiminnassa virkarikoksena on säädetty virkasalaisuuden rikkominen (RL 40 luku 5 §), joka on katsottu tekona rangaistavammaksi kuin salassapitorikos[939]. Rangaistavaksi on säädetty asiakirjan tai tiedon paljastaminen, jolloin se kattaa sekä asiakirjasalaisuuden että vaitiolovelvollisuuden rikkomisen[940]. Virkasalaisuuden rikkominen ulottuu virkamiehen lisäksi RL 40 luvun 12 §:n mukaisesti julkista luottamustehtävää hoitavaan henkilöön, julkista valtaa käyttävään henkilöön, julkisyhteisön työntekijään, tiettyihin ulkomaalaisiin virkamiehiin sekä niihin, joihin on muissa säädöksissä ulotettu koskemaan rikosoikeudellista virkavastuuta[941]. Mikäli teko ei ole rangaistava virkasalaisuuden rikkomisena, voidaan salassapitorikoksesta tai -rikkomuksesta tuomita se, joka laissa tai asetuksessa taikka viranomaisen lain nojalla erikseen määräämän salassapitovelvollisuuden vastaisesti paljastaa salassa pidettävän seikan. Vastaavia säännöksiä voidaan soveltaa myös liikesalaisuuksien paljastamiseen.[942]

---

933 Voutilainen 2019: 251–254. Ks. myös Viljanen 2023a: 714–770.
934 Liikesalaisuudella tarkoitetaan tietoa:
a) joka ei ole kokonaisuutena tai osiensa täsmällisenä kokoonpanona ja yhdistelmänä tällaisia tietoja tavanomaisesti käsitteleville henkilöille yleisesti tunnettua tai helposti selville saatavissa;
b) jolla edellä mainitun ominaisuuden vuoksi on taloudellista arvoa elinkeinotoiminnassa; ja
c) jonka laillinen haltija on ryhtynyt kohtuullisiin toimenpiteisiin sen suojaamiseksi.
935 HE 49/2018 vp: 1–2, 22–23. Liikesalaisuuslain myötä käsitteet liike- ja ammattisalaisuus tai yrityssalaisuus yhtenäistettiin Suomen lainsäädännössä, jolloin lainsäädännössä alettiin käyttämään yhdenmukaisesti termiä liikesalaisuus.
936 HE 66/1988 vp, s. 76; Viljanen 2023a: 715.
937 Esimerkiksi laissa tämä on ilmaistu niin, että hankitaan oikeudettomasti toisen liikesalaisuudesta tieto, oikeudettomasti ilmaistaan liikesalaisuus tai oikeudettomasti käytetään liikesalaisuutta.
938 Nyblin 2003: 236; Viljanen 2023a: 756–757.
939 Voutilainen 2019: 251–254.
940 HE 58/1988 vp: 60; Viljanen 2023b: 947.
941 Viljanen 2023b: 943.
Virkavastuun henkilöllinen soveltamisala määrittyy rikosoikeudellisen virkamieskäsitteen kautta. Ks. Laurikkala 2020, s. 34–35.
942 Viljanen 2023a: 753; HE 94/1993 vp: 143.

Viimeisenä esimerkkinä on turvallisuussalaisuuden paljastaminen (RL 12 luku 7 §) ja tuottamuksellisen turvallisuussalaisuuden paljastaminen (RL 12 luku 8 §). Näissä tapauksissa turvallisuussalaisuuden paljastaminen liittyy valtion turvallisuuteen ja toimintaan keskeisesti vaikuttavien tietojen paljastamiseen sivulliselle, jolloin tietojen tulee olla määrätty salassa pidettäviksi sekä tietojen salassapitointressinä tulee olla Suomen turvallisuus, ulkomaansuhteet tai kansantalous.[943] Turvallisuussalaisuuden paljastaminen (RL 12:7) eroaa vakoilusta siinä, että turvallisuussalaisuuden paljastaminen ei edellytä maanpetoksellista pyrkimystä hyödyttää toista valtiota taikka vahingoittaa Suomea. Suomea koskeva vahinko voi olla myös välillinen ja koskea esimerkiksi Suomen kansainvälistä mainetta ja uskottavuutta. Tuottamuksellisen turvallisuussalaisuuden paljastamisen (RL 12:8) kohdalla salaisuuden käsite on määritelty suppeammaksi ja se kattaa vain salassa pidettäväksi säädetyt tai määrätyt seikat. RL 12:7 koskevan turvallisuussalaisuuden kohdalla riittää jo se, että vähemmän merkittävien valtionsalaisuuksien paljastaminen on omiaan aiheuttamaan vaaraa maanpuolustukselle, turvallisuudelle, ulkomaansuhteille ja kansantaloudelle. RL 12:7 mukainen turvallisuussalaisuuden paljastaminen edellyttää tahallisuutta, kun taas RL 12:8:ssa tuottamuksellinen turvallisuussalaisuuden paljastaminen edellyttää törkeää huolimattomuutta.[944]

Yhteenvetona todettakoon, että henkilöstöturvallisuus on olennainen osa organisaation tietoturvallisuuden parantamista. Hallinnollisen tietoturvallisuuden toimenpiteinä henkilöstöturvallisuudessa keskiössä ovat organisaation tietoja käsittelevän henkilöstön luotettavuuden riittävä varmentaminen. Usein henkilöstön luotettavuuteen liittyvät toimenpiteet sijoittuvat työsuhteen tai toimeksiannon alkuun ja luotettavuuden selvitys voi taustatarkistuksien ohella sisältää turvallisuusselvityksien tekemisen. Turvallisuusselvitykset parantavat organisaatioiden tietoturvaa sekä suoraan että epäsuoraan: henkilöturvallisuusmenettelyyn kuuluvia organisaatioita velvoitetaan toteuttamaan asianmukaisia tietoturvatoimenpiteitä ja lisäksi reunaehtona on se, että organisaatioon voi sen toiminnan tai toimialan takia kohdistua yritysvakoilua taikka selvityksen on oltava tarpeen erittäin tärkeän yksityisen taloudellisen edun suojaamiseksi. Asianmukaisia vähimmäistietoturvatoimenpiteitä ovat turvallisuusselvityslain 18 §:n mukaan suojattaviin tietoihin pääsyn rajoitukset teknisillä ja organisatorisilla toimenpiteillä, toimitilojen ja tietojärjestelmien suojaaminen sekä muut asianmukaiset tietoturvatoimenpiteet ja turvallisuusjärjestelyt. Henkilöstön luotettavuuden varmentamisen ohella myös salassapitovaatimukset työ- ja toimeksiantosopimuksissa ovat oleellisia hallinnollisia tietoturvatoimenpiteitä, ja salassapidon velvoittavuus tulisi hyvien tietoturvakäytänteiden mukaisesti ulottaa sopimussuhteen jälkeiseen aikaan.

---

943 Voutilainen 2019: 251–254.
944 Ojala 2022: 341–343.

NIS 2 -direktiivin implementoivan kyberturvallisuuslain myötä henkilöstöturvallisuuden huomioiminen osana tietoturvariskienhallintaa paranee huomattavasti, koska aikaisemmin henkilöstöturvallisuutta ja siihen kuuluvia toimenpiteitä ei ole huomioitu kuin hajanaisin säännöksin lainsäädännössä.

3.5.7 Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut

Henkilöstön luotettavuuden ja organisaation tietojen salassapidon varmistamisen lisäksi henkilöstön tietoturvaosaaminen ja vastuuttaminen ovat tärkeitä hallinnollisia tietoturvatoimenpiteitä osana henkilöstöturvallisuutta, jotka parantavat organisaation tietoturvatasoa.

Henkilöstöturvallisuuden näkökulmasta tulevan työntekijän työsuhteen alkuasioihin pitäisi hyvien käytänteiden mukaisesti kuulua uuden työntekijän tietoturvakoulutus ja -perehdytys. Säännöllinen tietoturvakoulutus edesauttaa henkilöstön tietoturvatietoisuuden ja -osaamisen ylläpitämistä[945]. Näin ollen kertaluonteinen koulutus ei ole riittävää, sillä ihmismuisti on kovin lyhyt ja valikoiva sekä tietoturvaan liittyvät hyökkäystavat muuttuvat jatkuvasti. Tietoturvakoulutusta tulisikin järjestää henkilökunnalle ja henkilökuntaan rinnastettaville henkilöille, kuten esimerkiksi ulkoistetuille konsulteille, säännöllisesti.

Käytännössä asianmukainen henkilötietojen käsittely edellyttää henkilöstön ohjeistamista ja kouluttamista. Työnantajan on vaikea huolehtia henkilötietojen oikeanlaisesta käsittelystä, ellei työnantaja huolehdi henkilöstönsä osaamisesta[946]. Tietosuojaan ja tietoturvaan liittyvä koulutus organisaation työntekijöille onkin ”organisatorinen” toimenpide osana hallinnollista tietoturvallisuutta (henkilöstöturvallisuutta). Tähän liittyy näkemyseroja, esimerkiksi Voutilaisen näkemyksen mukaan koulutus on osa organisatorisia toimia, mutta myös osa teknisiä toimia erityisesti kouluttaessa henkilöstöä tietojärjestelmien käyttöön[947]. Todettakoon kuitenkin, että koulutus on aina organisatorinen eli hallinnollinen tietoturvatoimenpide, sillä se ei sisältäne organisaation tietoturvaa kohentavia teknisiä tietoturvatoimenpiteitä, vaikka siihen sisältyisi teknistä opetusta. Koulutuksella lisätään nimenomaan ihmisten tietoturvatietoisuutta ja teknistä osaamista, mikä myös osaltaan parantaa tietoturvaa. Näin ollen ihmisten tietoisuuden ja osaamisen lisääminen ei ole tekninen toimi.

Vaikka työntekijöiden kouluttamisella lisätään tietoisuutta ja osaamista, kouluttaminen ei täysin poista inhimillisten virheiden mahdollisuutta. Säännöllinen

945 Andreasson & Koivisto 2013: 33.
946 Nyyssölä 2018: 118–119.
947 Voutilainen 2019: 193.

koulutus ja tietoisuuden lisääminen kuitenkin pienentävät riskin todennäköisyyttä luottamuksellisen tiedon käsittelyvirheiden ja tietovuotojen osalta. Esimerkiksi **EUT:n ratkaisu 25.1.2024 C-687/21 MediaMarktSaturn**[948] on hyvä esimerkki yrityksen työntekijän tekemästä tietojen käsittelyvirheestä, jolloin rekisteröity väitti kärsineensä aineettomia vahinkoja:

> *Yrityksen työntekijän virheen johdosta henkilötietoja sisältäneet tulostetut asiakirjat olivat annettu luvatta kolmannelle osapuolelle rekisterinpitäjän alaisuudessa olevan työntekijän virheen vuoksi. Virhe huomattiin pian ja kolmas osapuoli ei hyödyntänyt saamiaan henkilötietoja. Rekisteröity vaati kuitenkin korvauksia aineettomasta vahingosta, joka oli aiheutunut rekisteröidyn mukaan omien henkilötietojensa hallitsemiskyvyn menettämisestä. Erääksi kysymykseksi nousi, riittääkö tietosuoja-asetuksen rikkomiseen se, että rekisteröidyn henkilötiedot päätyvät erehdyksessä virheen vuoksi paperitulosteena kolmannelle osapuolelle. EUT:n ratkaisun mukaan rekisterinpitäjällä on velvollisuus lieventää henkilötietojen tietoturvaloukkauksia koskevia riskejä, mutta ei velvollisuutta estää näiden tietojen kaikkia tietoturvaloukkauksia. Näin ollen luvaton pääsy tietoihin ei sellaisenaan riitä sen toteamiseen, että rekisterinpitäjän toteuttamat tekniset ja organisatoriset toimenpiteet eivät olisi asianmukaisia tietosuoja-asetuksen 24 ja 32 artiklassa tarkoitetussa merkityksessä. Rekisterinpitäjällä on kuitenkin vahingonkorvauskanteen yhteydessä todistustaakka siitä, että henkilötietoja käsitellään tavalla, jolla varmistetaan niiden asianmukainen turvallisuus. Tällöin tuomioistuimen on otettava huomioon kaikki rekisterinpitäjän osoittama näyttö siitä, että tekniset ja organisatoriset toimenpiteet ovat olleet asianmukaisia.* [949]

EUT:n ratkaisun perusteella voidaan päätellä, että tapauksessa yksi merkityksellinen arvioitava seikka on se, onko organisaation työntekijöitä riittävällä tasolla ohjeistettu ja koulutettu henkilötietojen käsittelyn suhteen. Tällöin olisi mahdollista arvioida, onko organisaation tietoturvatoimenpiteet olleet asianmukaisella

---

948 Ks. etenkin ratkaisun kohdat 39–45.

949 Osoitusvelvollisuuden periaatetta on tulkittava siten, että kyseessä olevalla rekisterinpitäjällä on kyseisen asetuksen 82 artiklaan perustuvan vahingonkorvauskanteen yhteydessä todistustaakka siitä, että sen yleisen tietosuoja-asetuksen 32 artiklan nojalla toteuttamat turvallisuustoimenpiteet ovat asianmukaisia. Tietosuoja-asetuksen 24 ja 32 artiklaa on tulkittava siten, että se, että kyseisen asetuksen 4 artiklan 10 alakohdassa tarkoitetut kolmannet osapuolet luovuttavat henkilötietoja luvattomasti tai pääsevät niihin luvattomasti, ei sellaisenaan riitä sen toteamiseen, että kyseessä olevan rekisterinpitäjän toteuttamat tekniset ja organisatoriset toimenpiteet eivät olleet asianmukaisia 24 ja 32 artiklassa tarkoitetussa merkityksessä. Ks. ratkaisusta EUT 14.12.2023, C-340/21 Natsionalna agentsia za prihodite erityisesti kohdat 39 ja 57.

tasolla: Johtuuko työntekijän virhe puhtaasti työntekijän tekemästä inhimillisestä virheestä ja on epätodennäköinen tapahtuma? Vai johtuuko henkilötietojen tietoturvaloukkaus organisaation matalasta tietoturvatasosta, jolloin riskitaso tapahtuman toistumiselle jonkun toisen asiakkaan kohdalla on suuri? Tapauksessa oli kyseessä kodinkoneita myyvä yritys, josta voi päätellä, että tietoturva ei ole välttämättä yrityksen ”pääosaamista”. Asianmukaisten tietoturvatoimenpiteiden arviointi tulisi perustua riskiperustaiseen arvioon, jolloin henkilöstön osaamisen puute voisi olla yksi tunnistettava uhka, joka mahdollisesti aiheuttaa riskejä luonnollisten henkilöiden oikeuksille ja vapauksille. Tapaus korostaa yksityisen sektorin ja ei-kriittisten toimialojen tietoturva- ja tietosuojavaatimusten tärkeyttä myös henkilöstön tietoturva- ja tietosuojaosaamisen suhteen. Henkilötietojen käsittelyn riskejä arvioitaessa tulisi joka organisaatiossa aina arvioida henkilötietojen käsittelyn ohjeistuksen riittävyyttä (myös käsittelytoimikohtaisesti) sekä mahdollisia koulutustarpeita. Esimerkiksi **MediaMarktSaturn** -tapauksessa kodinkoneita myyvän yrityksen kohdalla nykytila-arvio olisi jotakuinkin alla oleva:

> **Uhka:** henkilöstön osaamisen puute, jonka juurisyynä ovat puutteelliset henkilötietojen käsittelyn ohjeistukset ja riittämätön koulutus.
>
> **Riski rekisteröidylle:** henkilötietojen tietoturvaloukkaus, joilla vaikutuksia perusoikeuksiin (esimerkiksi yksityiselämän ja henkilötietojen suoja). Mielipaha, tunne yksityisyyden loukkaamisesta.
>
> **Riskin vakavuus (1–4):** 3 eli merkittävä (terveystietojen kohdalla voisi olla jopa 4, mutta kodinkoneita myyvässä yrityksessä käsiteltävät todennäköiset tiedot huomioon ottaen, vakavuus ei ole kriittinen).
>
> **Riskin todennäköisyys (1–4):** 4 eli lähes varma tai varma (riski on jo toteutunut).
>
> **Riskiluku (vakavuus * todennäköisyys):** 12 (erittäin korkea riski, jota on mitigoitava)
>
> **Riskin mitigointi:** henkilöstön ohjeistamisen parantaminen, säännöllisen tietoturva- ja tietosuojakoulutuksen järjestäminen.
>
> **Jäännösriskiluku:** 3 x 2 = 6 (riskin vakavuus ei pienene, mutta todennäköisyys pienenee varmasta mahdolliseksi. Jäännösriskiluku on hyväksyttävissä ilman tietosuojavaltuutetun ennakkokuulemista.)

Lainsäädännössä on vasta viime vuosina alettu painottamaan suoraan tietoturva- ja tietosuojaosaamisen tärkeyttä. Esimerkiksi kansallisen tietosuojalain (1050/2018) 6 §:ssä on erikseen mainittu erityisten henkilötietojen käsittelyyn

tarvittavista mahdollisista[950] tietoturvatoimenpiteistä, joista yksi on sellainen, jonka päämääränä on parantaa henkilötietoja käsittelevän henkilöstön osaamista. Edellä olevalla vaatimuksella ei suoraan rajata, mitä tällaiset keinot ovat henkilöstön osaamisen parantamiseksi, mutta käytännön tasolla se sisältää ohjeistukset sekä osaamista ja tietoisuutta lisäävät läsnä-, etä- tai verkkokoulutukset sekä tietoiskut. Myös esimerkiksi osaamisen testaaminen osana koulutuksen läpäisemistä voi olla vaatimuksen mukainen toimenpide.

Tietoturvanäkökulma huomioon ottaen tiedonhallintalaki (906/2019) velvoittaa lain mukaisen tiedonhallintayksikön johdon huolehtimaan, että tiedonhallintayksikössä on tarjolla koulutusta. Tiedonhallintalain 4 §:n mukaan tämän koulutuksen tarkoituksena on varmistaa henkilöstön ja tiedonhallintayksikön lukuun toimivien riittävä tuntemus tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista tiedonhallintayksikön ohjeista sekä voimassa olevista säädöksistä ja määräyksistä. Näin ollen tähän koulutukseen sisältyy tietoturva-asioita[951], mutta myös tietosuojalainsäädännön velvoitteiden läpikäyntiä. Jälleen huomioitava on se, että tiedonhallintalain koulutusvelvoitteessa on vahva viranomaisnäkökulma ja se velvoittaa laissa määriteltyjä tiedonhallintayksiköitä. Tiedonhallintalain velvoittama koulutus saattaa kuitenkin ulottua myös yksityisiin organisaatioihin, sillä usein yksityisellä sektorilla on ulkoistuksien ja muiden toimeksiantojen myötä pääsyjä julkishallinnon tietoihin.

NIS 2 -direktiivin voimaantulo ja sen kansallisen tason implementointi laajentavat tietoturvakoulutusvaatimuksia kansallisessa lainsäädännössä koskemaan useampaa toimijaa. NIS 2 -direktiivin 20 artiklan mukaan keskeisten ja tärkeiden toimijoiden hallintoelinten jäsenillä on velvollisuus osallistua koulutukseen ja kannustettava samalla keskeisiä ja tärkeitä toimijoita tarjoamaan säännöllisesti vastaavaa koulutusta työntekijöilleen. Koulutuksen on mahdollistettava henkilöille riittävien tietojen ja taitojen hankkimisen kyetäkseen tunnistamaan riskejä sekä arvioimaan kyberturvallisuusriskien hallintakäytäntöjä ja niiden vaikutusta toimijan tarjoamiin palveluihin. Direktiivin minimivelvoitteena on näin ollen direktiivissä määriteltyjen toimijoiden hallintoelinten jäsenien velvollisuus käydä kyberturvallisuus- ja riskienhallintakoulutuksessa sekä tarjota säännöllistä koulutusta. Lisäksi huomioitava on, että direktiivin 21 artiklassa myös painotetaan, että kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytettävä vähintään perustason kyberhygieniakäytännöt sekä kyberturvallisuuskoulutus. Tähän sisältyy muun muassa koulutusta kyberuhkista, verkkourkinnasta ja käyttäjän manipuloinnista[952].

[950] HE 9/2018 vp: 91. Tietosuojalain 6 §:n 2 momentin listaus tietoturvatoimenpiteistä ei ole kattava eikä pakottava, jolloin rekisterinpitäjän on harkittava ja päätettävä riskiperusteisesti suojatoimenpiteet.
[951] Ks. myös Valtiovarainministeriön julkaisuja 2024:19, s. 20–21.
[952] NIS 2 -direktiivin kohta 89.

NIS 2 -direktiivi implementoidaan keskeisten ja tärkeiden toimijoiden koulutusvaatimusten osalta kyberturvallisuuslakiin (9 § ja 10 §). Julkishallintoa koskevat koulutusvelvoitteet sijoittuvat tiedonhallintalakiin. Näin ollen NIS 2 -direktiivin mukaiset koulutusvelvollisuudet ovat hajaantuneet kahteen eri säädökseen.

Kyberturvallisuuslain mukaisen toimijan tulee huolehtia siitä, että henkilöstöllä on kyvykkyys toimia tavalla, joka vastaa kyberturvallisuuden hallintamallia ja hallintatoimenpiteitä. Organisaatiolla on vastuu henkilöstönsä osaamisesta: koulutuksella tai muulla vastaavalla tavalla tulisi varmistua, että henkilöstöllä on työtehtäviinsä nähden riittävä osaaminen viestintäverkon ja tietojärjestelmän suojaamisesta, kyberturvallisuusriskien tunnistamisesta, riskienhallintakäytännöistä ja niiden vaikutusten arvioinnista toimijan tarjoamiin palveluihin. Lisäksi osaamista on ylläpidettävä riittävällä tasolla.[953] Käytännössä ainoa tapa kerätä evidenssiä tämän lakivaatimuksen osalta on dokumentoida pidetyt koulutukset ja niihin osallistuvat henkilöt. Tätä ei kuitenkaan lain esitöissä eikä suoraan lainsäädännössä painoteta.

Hyvien käytänteiden mukaisesti henkilöstön tietoturva- ja tietosuojakoulutuksen on oltava säännöllistä, pakollista ja koulutuksen suorittaneista on jäätävä dokumentaatiota. Esimerkiksi Katakri 2020 T12-vaatimuksessa on suositeltu, että koulutuksiin osallistuneet henkilöt ja koulutuksen sisältö dokumentoitaisiin. Tällainen käytäntö edesauttaa lainsäädännössä ilmenevien koulutusvaatimusten toteutumisen todentamisessa. Ilman dokumentoitua evidenssiä johto ei pysty varmistamaan ja toteennäyttämään, että henkilökunnalla on tai pitäisi olla riittävä asiantuntemus. Tämä liittyy myös suuresti tietosuoja-asetuksen osoitusvelvollisuuteen ja rekisterinpitäjän todistustaakkaan vahingonkorvauskanteen yhteydessä siitä, että henkilötietoja käsitellään tavalla, jolla varmistetaan niiden asianmukainen turvallisuus[954]. Lainsäädännössä ja tietoturvaympäristössä tapahtuu jatkuvasti muutoksia, joten näin ollen tietyn alan tutkinto ei ole yksistään riittävä näyttö vaan osaamista pitää pystyä konkreettisesti todentamaan organisaation sisällä ja pitämään yllä. Toki jos henkilökunta ylläpitää itse omaa osaamistaan, esimerkiksi itseopiskelemalla tai sparraamalla toisiaan, ja siitä on riittävää evidenssiä, tämä voisi olla myös yksi tapa todentaa henkilökunnan riittävä asiantuntemus.

Toinen keskeinen henkilöstöturvallisuuden osa-alueeseen kuuluva hallinnollinen tietoturvatoimenpide on henkilöstön tietoturvavastuiden määrittely, dokumentointi ja jalkauttaminen. Organisaation henkilöstön ja sen toimeksiannon alaisuudessa toimivien työntekijöiden tulee tietää tietoturvavastuunsa sekä miten

---

[953] HE 57/2024 vp: 165. Osana 9 §:ssä tarkoitettuja hallintatoimenpiteitä johto huolehtii henkilöstön kyberturvallisuuskoulutuksen järjestämisestä (HE 57/2024, s. 170).
[954] Ks. EUT 25.1.2024, C-687/21 MediaMarktSaturn ratkaisun kohta 43 sekä ratkaisun EUT 14.12.2023, C-340/21 Natsionalna agentsia za prihodite kohta 57.

toimitaan tietoturvapoikkeamien kohdalla. Käytännön tasolla tätä velvoitetta voidaan edistää edellä mainitun tavoin ohjeistuksin ja koulutuksin, mutta myös kirjaamalla vastuita työ- ja toimeksiantosopimuksiin. Tyypillisesti ohjeistuksiin ja sopimuksiin tulisi hyvien käytänteiden mukaisesti kirjata, että jokaisen työntekijän vastuulla on noudattaa organisaation tietoturvapolitiikkoja ja -ohjeita sekä tunnistaa työhönsä liittyvä vastuu tietoturvallisuudesta ja henkilötietojen suojaamisesta. Työsopimuslain (55/2001) 3 luvun 1 §:n mukainen lojaliteettivelvoite tehostaa työntekijän tietoturvavastuita ja velvollisuutta noudattaa tietoturvaohjeistuksia: työntekijä on velvollinen tekemään työnsä huolellisesti noudattaen niitä määräyksiä, joita työnantaja antaa toimivaltansa mukaisesti työn suorittamisesta. Lisäksi työntekijän on vältettävä kaikkea, mikä on ristiriidassa hänen asemassaan olevalta työntekijältä kohtuuden mukaan vaadittavan menettelyn kanssa.

Huomioitava on se, että työntekijän, joka tahallaan tai huolimattomuudesta rikkoo tai laiminlyö työsopimuksesta johtuvia velvollisuuksia tai aiheuttaa työssään työnantajalle vahinkoa, on korvattava työnantajalle aiheuttamansa vahinko vahingonkorvauslain 4 luvun 1 §:n perusteiden mukaisesti[955]. Työntekijän aiheuttama vahinko voi kohdistua suoraan työnantajan omaisuuteen tai varallisuuteen, mutta vahinko voi myös ensin aiheutua kolmannelle taholle, ja tämän jälkeen ilmetä tulon saamatta jäämisen muodossa tai korvausvastuuna työnantajalle[956].

Organisaation työntekijöiden tietoturvarikkomusten osalta erilaisia oikeudellisia toimia ovat työsuhteen irtisanomisen tai työsopimuksen purkamisen lisäksi rikosilmoitus. Työntekijälle annettava kirjallinen varoitus toimii mahdollisesti irtisanomista edeltävänä toimenpiteenä, jos kyseessä ei ole sellainen niin vakava rikkomus tai laiminlyönti, että työnantajalta ei voida kohtuudella edellyttää sopimussuhteen jatkamista[957].

Työsopimuksen *purkaminen* edellyttää aina erittäin painavaa syytä, jollaisena voidaan pitää työntekijän työsopimuksesta tai laista johtuvien, työsuhteeseen olennaisesti vaikuttavien velvoitteiden niin vakavaa rikkomista tai laiminlyöntiä, että työnantajalta ei voida kohtuudella edellyttää sopimussuhteen jatkamista edes irtisanomisajan pituista aikaa[958]. Vastaavasti toistaiseksi voimassa olevan työsuhteen *irtisanominen* työnantajan toimesta edellyttää asiallista ja painavaa syytä, kuten työsopimuksesta tai laista johtuvien, työsuhteeseen olennaisesti vaikuttavien velvoitteiden vakavaa rikkomista tai laiminlyöntiä sekä sellaisten työntekijän

[955] Työsopimuslain 12 luvun 1 §. Kyseessä on yleinen vahingonkorvausvelvollisuus, joka on kyseisellä säännöksellä säännelty pakottavaksi eikä sitä voi sopimuksella säätää ankarammaksi. Ks. Koskinen & Ullakonoja 2020, s. 381–382.
[956] Koskinen & Ullakonoja 2020: 382.
[957] Työsopimuslain 7 luvun 2 §:n 3 momentti.
[958] Työsopimuslain 8 luku 1 §. Erittäin painava syy rinnastuu erittäin moitittavaan käyttäytymiseen tai laiminlyöntiin. Ks. Koskinen & Ullakonoja 2020, s. 281.

henkilöön liittyvien työntekoedellytysten olennaista muuttumista, joiden vuoksi työntekijä ei enää kykene selviytymään työtehtävistään[959]. Työsopimuksesta johtuvien velvoitteiden vakava laiminlyönti tai rikkominen voivat ilmetä joko yleisenä velvoitteiden vastaisena menettelynä tai työsopimuksessa sovitun erityisvelvoitteen laiminlyöntinä tai rikkomisena. Kummassakin tapauksessa edellytyksenä on, että sopimuksen vastainen toiminta tai laiminlyönti vaikuttaa niin vakavasti sopijapuolten keskinäiseen asemaan sopimussuhteessa, että työsopimussuhteen jatkamiselle ei ole edellytyksiä[960]. Esimerkiksi työtuomioistuimen ratkaisussa työntekijän ohjeiden vastainen toiminta ja valehtelu asian selvittelyssä katsottiin kokonaisuutena arvioiden rikkoneen työnantajan ja työntekijän luottamusta niin vakavasti, että painava syy työsuhteen purkamiselle oli luottamuspulan johdosta olemassa[961]. Työntekijöiden tietoturvarikkomuksista usein seuraa työntekijän ja työnantajan välisen luottamuksen väheneminen tai häviäminen työsuhteessa. Arvioinnissa tulee antaa merkitystä myös ohjeiden ja sääntöjen vastaisen toiminnan kestolle[962].

> Erityisen vakava, tietoinen tietoturvaohjeiden (ja työsopimuksessa määriteltyjen velvoitteiden) vastaisesti toimiminen, voisi olla lain kriteerien täyttävä työsopimuksen purkuperuste. Tällaiset rikkomukset todennäköisesti myös täyttävät esimerkiksi rikoslain 38 luvun tieto- ja viestintärikosten tunnusmerkistön. Purkamisperusteen täyttyminen edellyttää sitä, että sopijapuolen menettely loukkaa toista sopijapuolta niin syvästi, että hänen ei voida kohtuudella edellyttää sietävän sopimusloukkausta[963]. Purkamisperuste on olemassa silloin, kun työntekijä on täysin piittaamaton omista velvollisuuksistaan ja rikkoo niitä törkeästi[964].
>
> Työsuhteen irtisanominen on perusteltua ”lievienkin” tietoturvarikkomusten kohdalla, mikäli ne ovat toistuvia, tahallisia tai niihin liittyy törkeää huolimattomuutta, ja nämä toimet vaarantavat organisaation tietojen tietoturvan ja tietosuojan. Tällaisia voivat olla edellä mainituin perustein

[959] Työsopimuslain 7 luku 2 §. Huomioitava on lain 3 momentin täsmennys siitä, että työntekijää, joka on laiminlyönyt työsuhteesta johtuvien velvollisuuksiensa täyttämisen tai rikkonut niitä, ei kuitenkaan saa irtisanoa ennen kuin hänelle on varoituksella annettu mahdollisuus korjata menettelynsä. Lisäksi 4 momentin mukaan työnantajan on selvitettävä, olisiko irtisanominen vältettävissä sijoittamalla työntekijä muuhun työhön. Kuitenkin 5 momentin mukaan, jos irtisanomisen perusteena on niin vakava työsuhteeseen liittyvä rikkomus, että työnantajalta ei voida kohtuudella edellyttää sopimussuhteen jatkamista, ei 3 ja 4 momentissa säädettyä tarvitse noudattaa.
[960] Koskinen & Ullakonoja 2020: 286–287.
[961] TT 2020:4. Vastaavasti KKO:n ratkaisussa 1999:83 on katsottu ohjeiden vastaisesta toiminnasta syntyneestä luottamuspulasta johtuen ollut erityisen painava syy työsopimuksen irtisanomiseen.
[962] Pesonen 2017: 299.
[963] Koskinen & Ullakonoja 2020: 287.
[964] Pesonen 2017: 252.

> esimerkiksi tietoturvaohjeiden vastaisesti työntekijän omien tunnusten luovuttaminen toisen käyttöön, luvattomien ohjelmien asentaminen työkoneelle taikka etätyöskentely kielletystä kolmannesta maasta.

Lainsäädännön tasolla tietoturvallisuuden vastuuasiat näyttäytyvät eri tavoin. Esimerkiksi tietosuojalainsäädännössä rekisterinpitäjän vastuisiin kuuluu varmistaa henkilötietojen ja niiden käsittelyn asianmukainen tietoturvallisuus. Toteutuneiden tietoturvaloukkausten kohdalla vastuu ei harvemmin kohdistu yksittäiseen henkilöön[965], kuten toimitusjohtajaan, vaan vastuu lainsäädännössä on rekisterinpitäjänä toimivalla organisaatiolla sekä tapauskohtaisesti myös henkilötietojen käsittelijäorganisaatiolla. Huomioitava kuitenkin on, että organisaation ylin johto toimii niin sanottuna organisaation ”keulakuvana”, jolloin tietoturvaloukkauksissa vastuuasiat kulminoituvat loppujen lopuksi johtohenkilöiden vastuulle. Rikoslain mukaisissa tietosuojarikoksissa (RL 38:9) yksittäisen työntekijän tekemät henkilötietojen tietoturvaloukkaukset voivat henkilöityä, kuin myös muut tietoturvaloukkaukset, jotka ovat esimerkiksi rikoslain 38 luvussa säädetty rangaistaviksi.

Tietoturvatyön tulisi olla lähtöisin organisaation johdosta ja sen aktiivisuudesta, sillä ilman johdon tukea ja sitoutumista tietoturvatyö ei saavuta sille asetettuja tavoitteita eikä lainsäädännöllisiä velvoitteita. Tietoturvatyötä tulisi myös määritellä ja vastuuttaa vastuuhenkilölle, joka raportoi johdolle[966]. Keskisuurissa ja sitä isommissa organisaatioissa jokaisessa toiminnossa tai yksikössä olisi hyvä olla tietoturvasta vastaava henkilö[967]. Tietoturvallisuuden osalta pitäisi myös varmistaa riittävä tietoturvan asiantuntemus organisaatiossa sekä arvioida resursseja säännöllisesti[968]. Organisaation tietoturvaresursoinnin ja -asiantuntemuksen tärkeys sekä johdon merkitys tietoturvan selkärankana on kovin näkymätöntä lainsäädännössä.

Tietoturvan sääntelyjärjestelmän tulisi huomioida paremmin ja kokonaisvaltaisemmin yksilöt tietoturvan toteuttajana. NIS 2 -direktiivissä onkin havaittavissa tämän osalta asennemuutosta, sillä direktiivin 20 artiklassa painotetaan, että keskeisten ja tärkeiden toimijoiden hallintoelimien on a) hyväksyttävä 21 artiklan noudattamiseksi toteuttamat kyberturvallisuusriskien hallintatoimenpiteet; b) valvottava 21 artiklan täytäntöönpanoa kyberturvallisuusriskien hallintatoimenpiteiden osalta; ja c) saatettava vastuuseen, jos toimijat rikkovat kyseistä artiklaa.

---

[965] Pois lukien virkamiesten virkavastuu, johon kuuluu myös vastuu työssä tehdyistä virheistä (esim. HE 57/2024 vp, s. 201).
[966] Katakri 2020 T2-vaatimuksena on yleispiirteisesti linjattu, että tietoturvallisuuden hoitamisen tehtävät ja vastuut on määritelty.
[967] Andreasson & Koivisto 2013: 33.
[968] Ks. Katakri 2020: T05-vaatimus.

NIS 2 -direktiivin implementoivassa kyberturvallisuuslain 10 §:n mukaan toimijan ylin johto[969] on vastuussa viestintäverkkojen ja tietojärjestelmien kyberturvallisuutta koskevan riskienhallinnan toteuttamisesta ja valvonnasta toimijassa, mikä tarkoittaa myös viimesijaista vastuuta järjestää ja resursoida riskienhallinta asianmukaisesti sekä valvoa muun muassa kyberturvallisuuden riskienhallinnan toimenpiteitä. Johdon vastuun laiminlyönti voisi johtaa toimijaan kohdistuvaan kyberturvallisuuslaissa tarkoitettuun hallinnolliseen seuraamukseen. Lisäksi johdon vastuun vakava ja toistuva laiminlyönti voisi johtaa sellaiseen valvovan viranomaisen päätökseen, jolla kielletään määräajaksi henkilöä toimimasta 10 §:ssä tarkoitetussa ylimmän johdon tehtävässä.[970] Näin ollen kyberturvallisuuslaki vastuutta johtoa kyberturvallisuuteen liittyvistä tietoturvatoimenpiteistä, joka realisoituu erityisesti tietoturvaloukkausten tapahtuessa. Tietoturvaloukkausten kohdalla arvioitavaksi tulee, onko keskeisen tai tärkeän toimijan ylin johto huolehtinut tehtävistään. Mikäli ilmenisi, että ylin johto ei ole huolehtinut riskiperusteisesti siitä, että sillä on riittävät ja ajantasaiset kyberturvallisuuden riskienhallinnan toimenpiteet käytössään, vastuu tietoturvaloukkauksesta on organisaation johdolla.

Kyberturvallisuuslaki korostaa myös kyberturvallisuuden riskienhallinnan vastuiden määrittelyä ja kuvausta kyberturvallisuuden riskienhallinnan toimintamallissa (8 §). Lisäksi kyberturvallisuuslain 9 §:n henkilöstöturvallisuuden käsitteeseen sisältyy menettelyt, joilla varmistetaan henkilöiden tietoturvavastuut ja velvollisuudet. Henkilöstöä ja ulkoisia toimijoita voitaisiin tarvittaessa esimerkiksi tiedottaa heidän työtehtäviensä ja tarjoamiensa palveluiden turvallisuuteen liittyvistä vastuista ja velvoitteista, kuten esimerkiksi salassapitoon liittyen. [971]

---

[969] Ylimmällä johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa, toimitusjohtajaa tai muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa toimijan toimintaa. Tällainen voi olla myös yksityinen elinkeinoharjoittaja. Ks. HE 57/2024 vp, s. 170.

[970] HE 57/2024 vp: 170. Vastaavasti myös viranomaisen tiedonhallintalain 4 §:ssä on painotettu tiedonhallintayksikön johdon huolehtimisvastuuta. Tiedonhallintalain 4 §:n mukaan tiedonhallintayksikön johdon on huolehdittava mm. siitä, että tiedonhallintayksikössä on määritelty tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut sekä tiedonhallintayksikössä on tarjolla koulutusta, jolla varmistetaan henkilöstön ja tiedonhallintayksikön lukuun toimivien riittävä tuntemus tiedonhallintayksikön ohjeista ja voimassa olevasta tiedonhallintaa, tietojen käsittelyä ja asiakirjojen julkisuutta tai salassapitoa koskevista säädöksistä. HE 284/2018 (s. 73) mukaan tähän liittyen myös jokaisella tiedonhallintayksikössä toimivalla tulisi olla tieto tietoturvallisuuteen liittyvien vastuiden jakautumisesta tiedonhallintayksikössä. Valtiovarainministeriön suosituksessa tietoturvallisuuden vähimmäisvaatimuksista on painotettu dokumentoituja tietoturvallisuuden hoitamisen tehtäviä ja vastuita, eli pelkkä ajatustason määrittely ei ole riittävää (Valtiovarainministeriön julkaisuja 2024:19, s. 12). NIS 2 -direktiivin velvoitteiden vastuuasioiden osalta julkishallinnossa virkavastuutta voidaan pitää riittävänä johdon vastuun osalta. Julkisoikeudelliset toimijat rajataan seuraamusmaksun ulkopuolelle, mutta uhkasakko jää täytäntöönpanon tehosteeksi. Virkamiehen virkavastuuseen kuuluu vastuu työssä tehdyistä virheistä. (HE 57/2024 vp: 55, 201, 232).

[971] HE 57/2024 vp: 165.

Huomioitava on, että usein tiedottaminen saavuttaa vain osan henkilöstöä, joten se ei ole järin tehokas toimenpide, vaikka lain esitöissä näin ehdotetaankin. Turvallisuusvastuut pitäisi aina määritellä ja dokumentoida organisaation tieturvapolitiikoissa sekä työ- ja toimeksiantosopimuksissa.

Yhteenvetona voidaan todeta, että työntekijöiden tietoturvaosaaminen on tärkeää organisaation tietoturvan kannalta. Hallinnollisena tietoturvatoimenpiteenä osana henkilöstöturvallisuutta tietoturvaohjeistuksien luominen, ylläpito ja niiden jalkauttaminen koulutuksin ovat keskeisiä toimenpiteitä tietoturvaosaamisen kehittämisessä ja henkilöstön tietoturva-asenteiden parantamisessa. Työntekijöiden ohjeistaminen ja kouluttaminen sijoittuvat työsuhteen alkupään perehdyttämisen lisäksi koko työsuhteen elinkaareen osana tietoisuuden ja osaamisen ylläpitämistä. Ohjeistuksien olemassaolo ja kertaluontoinen koulutus eivät ole sellaisenaan riittäviä toimenpiteitä, vaan työnantajan on huolehdittava säännöllisestä tietoturva- ja tietosuojakoulutuksesta, jotta työntekijät osaisivat toimia tietoturvallisesti. Tietosuojalainsäädännön mukainen asianmukainen henkilötietojen käsittely edellyttää henkilöstön ohjeistamista ja kouluttamista. Vastaisuudessa myös NIS 2 -direktiivin implementoiva kyberturvallisuuslaki vaatii keskeisiä ja tärkeitä toimijoita tarjoamaan kyberturvallisuuskoulutusta henkilöstölleen. Kaiken kaikkiaan tietoturvan sääntelyjärjestelmässä esiintyvät vaatimukset liittyen tietoturva- ja tietosuojakoulutukseen tai osaamisen ylläpitoon vaihtelevat painotukseltaan ja sisällöltään. Lisäksi tietoturva- ja tietosuojaosaamiseen liittyvä vähimmäissääntely on hajaantunut useaan eri säädökseen. NIS 2 -direktiivin myötä sääntelyjärjestelmän painotus laajenee yhä enemmän säännöllisen tietoturva- ja tietosuojakoulutuksen suuntaan ja johdon vastuuseen tarjota koulutusta. Nykyinen, hajaantunut vähimmäissääntely ei kuitenkaan huomioi kattavasti henkilöstön osaamisen vaatimuksia yksityisellä sektorilla ei-kriittisten toimialojen suhteen, vaikka yrityksissä usein käsitellään henkilötietoja ja muita luottamuksellisia tietoja. Lisäksi organisaatioiden tietoturvan sääntelyjärjestelmä ei täysin huomioi hyviä käytänteitä esimerkiksi koulutukseen osallistuneiden henkilöiden dokumentoinnin osalta: koulutuksien osalta olisi hyvä dokumentoida osallistuvat henkilöt (sekä koulutuksen aihe ja ajankohta), jotta työnantajana voi tarvittaessa osoittaa, että se on kouluttanut henkilöstöään[972]. Näin ollen riittävän dokumentointivaatimuksen kirjaaminen koulutusvaatimusten yhteyteen olisi suotavaa kehittäessä tietoturvalainsäädäntöä, sillä se liittyy olennaisesti tietosuoja-asetuksen osoitusvelvollisuuteen ja rekisterinpitäjän todistustaakkaan vahingonkorvauskanteen yhteydessä siitä, että henkilötietoja käsitellään tavalla, jolla varmistetaan niiden asianmukainen turvallisuus. Hyvä tietoturvan sääntelyjärjestelmä huomioi nämä seikat.

[972] Esimerkiksi tahallisissa väärinkäytöstapauksissa työntekijä ei voi välttämättä tapauskohtaisesti vedota tietämättömyyteen tai osaamattomuuteen, jos työnantaja on säännöllisesti tarjonnut koulutusta.

Tietoturvaosaamisen ohella henkilöstön tulee tunnistaa omat tietoturvavastuunsa. Tietoturvavastuiden määrittely, kuvaaminen ja jalkauttaminen ovat olennaisia hallinnollisia tietoturvatoimenpiteitä henkilöstöturvallisuuden osa-alueella. Johdon toimiessa organisaation keulakuvana, päävastuu tietoturvallisuustoimenpiteiden toteutumisesta on johdolla. Kuitenkin jokaisella työntekijällä tulisi olla vastuu tietoturvallisuudesta työtehtäviä hoitaessaan ja nämä vastuut tulisi mainita muiden tietoturvapolitiikkojen ja -ohjeistuksien lisäksi työsopimuksessa. Tietoturvavastuuttaminen jo työsopimustasolla on ohjeistuksien ja koulutuksien ohella konkreettinen toimenpide, jonka avulla voidaan henkilöstön tietoturvarikkomusten kohdalla arvioida esimerkiksi sitä, onko kyseessä tietyn työntekijän kohdalla vahingosta tai tietämättömyydestä vai, onko kyseessä välinpitämättömyys, törkeä huolimattomuus tai tahallisuus. Näin on myös selkeämpää arvioida työsuhteen irtisanomisperusteiden asiallisuutta ja painavuutta sekä velvoitteiden rikkomisen tai laiminlyönnin vakavuutta. Lisäksi organisaatioilla tulisi olla selkeä ja läpinäkyvä tietoturvarikkomusten seuraamuskäytäntö, josta työntekijät olisivat tietoisia.

Lainsäädännön tasolla tietoturvallisuuden vastuut ovat näyttäytyneet monitahoisena. Esimerkiksi henkilötietojen tietoturvaloukkausten kohdalla päävastuu on rekisterinpitäjäorganisaatiolla (ja tapauskohtaisesti myös henkilötietojen käsittelijäorganisaatiolla), jolloin harvemmin vastuu lainsäädännön tasolla kohdistuu yksittäiseen henkilöön, ellei sitten kyseessä ole rikoslaissa määritelty virkamiehen virkavastuu, tietosuojarikos tai muu rikoslaissa määritelty rangaistava teko. Toinen vastuuta rajaava tekijä on se, että organisaatio pystyy osoittamaan, että sen toteuttamat tekniset ja organisatoriset toimenpiteet ovat olleet asianmukaisia 24 ja 32 artiklassa tarkoitetussa merkityksessä. Muutoin vastuu henkilötietojen tietoturvaloukkauksien syistä ja seurauksista on organisaatiolla, jolloin käytännössä kokonaisvastuu on organisaation johdolla[973], vaikka tietosuojalainsäädännössä

[973] Tietosuoja-asetuksessa tietosuojavastaavan tehtävä on raportoida suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle, mikä kuvastaa ylimmälle johdolle kuuluvaa vastuuta. Vertailun vuoksi myös työturvallisuuden kokonaisvastuu on ylimmällä johdolla. Työturvallisuuslain (738/2002) 2 luku velvoittaa työnantajaa huolehtimaan työntekijöiden turvallisuudesta työssä, toteuttamaan työolosuhteiden parantamiseksi tarvittavia toimenpiteitä sekä tarkkailemaan toimenpiteiden vaikutusta työn turvallisuuteen. Lisäksi työnantajan on arvioitava työn vaaroja ja pidettävä yllä ajantasaista selvitystä. Kyseisen lain 63 §:ssä on säädetty työturvallisuusrikkomuksesta, joka koskee esimerkiksi edellä mainitun selvityksen tekemisen laiminlyömistä. Lisäksi rikoslain 47 luvun 1 §:ssä on säädetty rangaistavaksi työturvallisuusrikos, jolloin esimerkiksi työturvallisuusmääräysten rikkomisesta tuomitaan sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Sekä työturvallisuusrikkomus että työturvallisuusrikos koskevat työnantajaan tai tämän edustajaa, kuten yksittäistä esihenkilöä. Moniportaisessa organisaatiossa työnantajan vastuu jakautuu ylimmän johdon lisäksi keskijohdolle ja lähiesimiehille, mutta ylimmällä johdolla on vastuullaan mm. työturvallisuuden yleisjohto- ja valvonta sekä työturvallisuuden aineellisten edellytysten varmistaminen (Työturvallisuuskeskus 2019, s. 8–9).

tätä ei tulekaan suoraan ilmi. Analogiana vastuun tulisi kohdentua ylimmän johdon lisäksi esihenkilöihin, aivan kuten työrikoksissa[974].

NIS 2 -direktiivin implementoiva kyberturvallisuuslaki lisää konkreettisesti sekä johdon vastuuta, mutta myös muun henkilöstön tietoturvavastuiden määrittelyä ja dokumentoimista. Tällöin tietoturvaloukkausten kohdalla arvioitavaksi tulee, onko keskeisen tai tärkeän toimijan ylin johto huolehtinut sille laissa määritellyistä tehtävistään. Asia on rinnastettavissa tietosuoja-asetuksen mukaiseen osoitusvelvollisuuteen asianmukaisten teknisten ja organisatoristen toimenpiteiden toteutumisen osalta. Mikäli ilmenisi, että ylin johto ei ole huolehtinut riskiperusteisesti siitä, että sillä on riittävät ja ajantasaiset kyberturvallisuuden riskienhallinnan toimenpiteet käytössään, vastuu tietoturvaloukkauksesta on organisaation ylimmällä johdolla.

Kyberturvallisuuslaki velvoittaa lähinnä kriittisiä toimialoja, joten tietoturvan vastuuasiat ulottuvat kaikkiin organisaatioihin lähinnä henkilötietoja suojaavan tietosuojalainsäädännön kautta. Tämä ei ole riittävää huomioon ottaen tietoturvallisuuden merkityksen kasvu nykyisessä verkkoyhteiskunnassa. Myös ei-kriittisten toimialojen toimijoita tulisi vastuuttaa sekä velvoittaa ottamaan huomioon tietoturvavastuut organisaatiossa. Käytännön tasolla tämä nykyisin tapahtuu mahdollisesti osana hankinta- ja ulkoistamissopimuksia. Tietoturvan yleislaissa, olisi mahdollista korostaa johdon sitoutumista tietoturvatyöhön, tietoturvatyön vastuuttamista sekä riittävää tietoturvaresursointia ja -osaamista.

974 Esimerkiksi rikoslain 47 luvun 7 §:n vastuun kohdentumisen osalta on todettu, että työnantajan tai tämän edustajan (eli mm. esihenkilön) menettelystä rangaistukseen tuomitaan se, jonka velvollisuuksien vastainen teko tai laiminlyönti on.

4 JÄRJESTELMIEN TIETOTURVARISKIEN HALLINTA

4.1 Luvun päämäärä

Tietosuojalainsäädännön yleisiä tietoturvavaatimuksia käsittelevän pääluvun jälkeen siirrytään käsittelemään yksityiskohtaisemmin nimenomaan organisaatioiden järjestelmien turvaamiseen liittyviä vaatimuksia lainsäädännössä. Pääsääntöisesti vaatimukset järjestelmien turvaamiseksi liittyvät tietoturvariskien (lähinnä kyberriskien) hallintaan, mutta lainsäädännössä on myös lisääntynyt muunlaiset järjestelmien tietoturvallisuuteen liittyvät vaatimukset.

EU:n verkko- ja tietoturvadirektiivi (2016/1148) eli NIS 1 -direktiivi kehitettiin alun perin lisäämään verkko- ja tietojärjestelmien turvallisuutta EU:ssa sekä parantamaan kansallista varautumista, minkä vuoksi sitä on tarkasteltu tässä tutkimuksessa järjestelmien tietoturvavaatimusten ja hyvän tietoturvatavan osalta. NIS 1 -direktiivi kumottiin kyberturvallisuusdirektiivillä eli NIS 2 -direktiivillä (2022/2555/EU) joulukuussa 2022 muun muassa siksi, että EU:ssa pystyttäisiin paremmin puuttumaan nykyisiin ja esille nousemassa oleviin kyberturvallisuushaasteisiin[975]. Näin ollen myös NIS 2 -direktiivi on keskeisessä tarkastelussa tässä luvussa ja sitä käsitellään yhdessä alkuperäisen NIS 1 -direktiivin kanssa. EU:n jäsenvaltioilla, kuten Suomella, on 21 kuukautta aikaa saattaa NIS 2 -direktiivi osaksi kansallista lainsäädäntöään[976]. NIS 2 -direktiivin täytäntöönpano tapahtuu kyberturvallisuuslailla. Tällöin myös NIS 1 -direktiivin täytäntöönpanosäännökset kumottaisiin sektorikohtaisista laeista.[977] Huomioitava kuitenkin on, että kyberturvallisuuden riskienhallintavelvoitteet eivät tällöinkään koske kaikkia kansallisia toimijoita, mikä tekee myös tietoturvallisuuden sääntelyjärjestelmästä puutteellisen ja sirpaleisen.

Alkuperäinen NIS 1 -direktiivi oli ensimmäinen yleiseurooppalainen kyberturvallisuutta käsittelevä oikeudellinen säädös, ja sitä kehitettiin yhtä aikaa tietosuoja-asetuksen kanssa. Näkökulman painotus kuitenkin erosi tietosuoja-asetuksesta: NIS 1 -direktiivin riskienhallintavaatimuksilla pyrittiin lisäämään verkko- ja tietojärjestelmien tietoturvallisuutta, kun taas tietosuoja-asetuksessa on asetettu kokonaisvaltaisemmin riskienhallintavaatimuksia henkilötietojen suojaamiseksi. Molemmat säädökset ovat kuitenkin velvoittaneet organisaatioita toteuttamaan tietoturvatoimenpiteitä, jotka ovat myös tämän tutkimuksen tarkastelun kohteena.

---

975 Ks. NIS 2 -direktiivin kohta 2.
976 Ks. LVM044:00/2022.
977 HE 57/2024 vp: 1, 61. Julkishallinnon täytäntöönpano NIS 2 -direktiivin osalta toteutuu tiedonhallintalain uuden 4a-luvun myötä.

Tietosuoja-asetuksen ja alkuperäisen NIS 1 -direktiivin näkökulmaeron lisäksi huomioitava on, että nämä säädökset eivät sisältäneet viittauksia toistensa teksteihin. NIS 1 -direktiivin 2 artiklassa oli viittaus vanhaan henkilötietodirektiiviin (1995/46/EY), vaikka tietosuoja-asetus oli tuolloin jo julkaistu. Tämä fakta ei kuitenkaan tarkoita sitä, etteikö tietosuoja-asetus ja NIS 1 -direktiivi olisivat liittyneet toisiinsa. Päinvastoin. Verkko- ja tietojärjestelmiä käytettäessä henkilötietojen käsittelyyn, molemmat oikeudelliset välineet ovat olleet tärkeitä. Tietosuoja-asetuksen ja NIS 1 -direktiivin välistä vuorovaikutusta ja ristiriitoja on esiintynyt erityisesti silloin, kun NIS 1 -direktiivin mukaisten digitaalisen palvelun tarjoajien tai keskeisen palvelun tarjoajien järjestelmissä on tapahtunut tietoturvaloukkaus ja järjestelmässä on käsitelty henkilötietoja. Tällöin kunkin säädöksen mukaiset velvoitteet on pitänyt arvioida ja toteuttaa erikseen. Loppujen lopuksi näillä säädöksillä on kuitenkin ollut sama tarkoitus: unionin sisäisten markkinoiden vahvistaminen. Näin ollen ne on pitänyt myös nähdä toisiaan täydentävinä säädöksinä.[978]

NIS 2 -direktiivi huomioi paremmin tietosuoja-asetuksen tekstitasolla, sillä direktiivin kohdan 14 mukaan kaikkeen NIS 2 -direktiivin mukaiseen henkilötietojen käsittelyyn sovelletaan tietosuojalainsäädäntöä ja yksityisyyden suojaa koskevaa unionin oikeutta, eikä direktiivillä etenkään rajoiteta yleisen tietosuoja-asetuksen soveltamista. Täten myös normien etusijajärjestys näyttäytyy selvemmin eli ristiriitatilanteessa ylempitasoisena lakina tietosuoja-asetus on etusijalla NIS 2 -direktiiviin nähden sen välittömän oikeusvaikutuksen ja suoran sovellettavuuden vuoksi. Kuitenkin esimerkiksi tietoturvaloukkauksien osalta aikaisempi käytäntö jatkuu eli sekä tietosuoja-asetuksen että NIS 2 -direktiivin raportointivelvoitteet tulee arvioida erikseen riippuen siitä, käsitelläänkö järjestelmässä myös henkilötietoja ja ulottuuko tietoturvaloukkaus niihin. NIS 2 -direktiivin myötä sen soveltamisalaan kuuluvien organisaatioiden tulee turvapoikkeamien kohdalla arvioida myös poikkeaman merkittävyyttä muun muassa vahinkojen suhteen, kuten esimerkiksi, aiheuttaako poikkeama *huomattavaa aineellista tai aineetonta vahinkoa* vaikutuksillaan luonnollisiin henkilöihin. Henkilötietojen ollessa kyseessä raportointivelvoitteet ovat tällöin läpileikkaavia ja raportoinnissa tulisi käyttää yhtenäistä sapluunaa.[979]

Alkuperäisen NIS 1 -direktiivin myötä organisaatioille täsmentyi velvollisuuksia huolehtia tietojärjestelmiensä ja viestintäverkkojensa riskienhallinnasta, jotka paransivat myös keskeisten toimijoiden kykyä varautua tietoturvaloukkauksiin.[980] Tämän neljännen pääluvun keskeiseksi tarkastelun kohteeksi nousee näin ollen

978 Hert, Markopoulou & Papakonstantinou 2019: 9–11.
979 Ks. lisää luvusta 3.3.4 (”Tietoturvaloukkauksien ja tietoturvapoikkeamien ilmoittaminen”).
980 HE 192/2017 vp: 60.

NIS 1 -direktiivistä implementoidut velvoitteet kansallisessa lainsäädännössämme, jotka koskevat tietoturvariskien hallintaa. Lisäksi luvussa on käsitelty NIS 2 -direktiivin kyberturvallisuuden riskienhallinnan vaatimuksia. Direktiivien vaatimukset kohdistuvat lähinnä verkko- ja tietojärjestelmiin, minkä vuoksi tässä pääluvussa käydään läpi lainsäädännössä esiintyviä järjestelmien tietoturvavaatimuksia kuitenkaan menemättä teknisiin yksityiskohtiin tutkimuksen rajaukset huomioon ottaen.

NIS 1 -direktiivin tietoturvavaatimukset kohdistuivat lähinnä olemassa oleviin järjestelmiin, vaikka hyvien käytänteiden mukaisesti järjestelmien ja palveluiden tietoturvavaatimukset tulisi huomioida niiden koko elinkaaren ajalta. NIS 2 -direktiivissä elinkaari on huomioitu paremmin, sillä direktiivin riskienhallintatoimenpiteiden mukaan turvallisuus on otettava huomioon jo järjestelmien hankintavaiheessa. Lähtökohtaisesti tuotteet, palvelut ja tietojärjestelmät tulisi suunnitella, valmistaa ja ylläpitää siten, että tietoturva ja tietosuoja muodostavat niiden sisäänrakennetun ja erottamattoman osan[981].

Elinkaaren hallinnan lisäksi oleellinen kysymys koskee myös järjestelmien ja palveluiden oikeudellista suunnittelua: mitä lainsäädännön vaatimuksia tulisi huomioida tietoturvallisuuden ja henkilötietojen suojaamisen osalta koko järjestelmän tai palvelun elinkaaren ajalta? Edellä mainittu kysymys huomioon ottaen, tämän pääluvun viimeisessä alaluvussa käsitellään järjestelmien elinkaareen ja toteutukseen liittyviä tietoturvavaatimuksia oikeudellisesta näkökulmasta. Vaikkakin tässä luvussa ovat keskiössä NIS 1 ja NIS 2 -direktiivin vaatimukset, on lisäksi muitakin säädöksiä, jotka parantavat organisaatioiden ja järjestelmien tietoturvatasoa. Tietosuoja-asetusta ei myöskään jätetä huomioimatta tässä luvussa, sillä se vaikuttaa etenkin järjestelmien oikeudelliseen suunnitteluun sisäänrakennetun ja oletusarvoisen tietosuojan -periaatteen (*”Privacy by Design and Default”*) kautta.

Näin ollen tämän pääluvun tavoitteena on tunnistaa voimassa olevan oikeuden pohjalta verkko- ja tietojärjestelmien tietoturvariskien hallintaan liittyvät vaatimukset sekä järjestelmiin liittyvät oikeudellisen suunnittelun vaatimukset osana organisaatioiden tietoturvan sääntelyjärjestelmää. Lisäksi keskeisenä tavoitteena on muodostaa käsitys näiden vaatimusten pohjalta lainsäädännön hyvästä tietoturvatavasta, jota vertaillaan tunnistettuihin hyviin käytänteisiin.

[981] Liikenne- ja viestintäministeriön julkaisuja 2021:1: 17.

4.2 Riskienhallinnan systematiikkaa ja hyvät käytännöt

4.2.1 Riskienhallinta osana tietoturvan kehittämistä ja parantamista

Nykyisessä tietoturva- ja tietosuojalainsäädännön kehityksessä on havaittavissa painotus riskienhallinnassa suorien tietoturvavaatimuksien sijaan. Esimerkiksi NIS 2 -direktiivin IV-luvussa on keskiössä kyberturvallisuusriskien hallintatoimenpiteet, jotka tosiasiassa ovat tietoturvatoimenpiteitä. Myös tietosuoja-asetuksessa painotetaan riskilähtöisyyttä, jonka myötä valittavien toimenpiteiden ja suojauksen tulee perustua organisaation tekemään riskiarvioon. Ennen kuin käsitellään yksityiskohtaisemmin verkko- ja tietojärjestelmien tietoturvariskien hallinnan myötä tulevia tietoturvavaatimuksia organisaatioille, on syytä aluksi käsitellä riskienhallintaan liittyvää systematiikkaa ja hyviä käytäntöjä.

Lainsäädännön riskiperustaisen lähestymistavan kehittymisen ohella myös organisaatioiden tietoturvatoiminnassa on tapahtunut muutoksia. Tietoturvallisuuden lähestymistapa on muuttunut kohti strategista tapaa, jossa korostuu kolme ulottuvuutta: lakien ja toimintaperiaatteiden noudattaminen, riskienhallinta sekä tietoturvallisuuden hallinta. Tämä merkitsee muutosta reaktiivisista teknisistä toimenpiteistä kohti proaktiivista, strategista lähestymistapaa.[982] Riskienhallinta[983] on kaikkea toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Sen päämääränä on tunnistaa ja hallita organisaation toimintaa haittaavia tekijöitä, välttää haitallisia tapahtumia taikka pienentää tapahtumien seurauksia sekä pitää riskit sellaisella tasolla, etteivät organisaation toiminta ja tavoitteet ole uhattuina.[984] Riskienhallinnan tavoitteena on mahdollistaa tavoitteiden saavuttaminen, jatkuvuuden takaaminen sekä organisaation menestyminen[985].

Tietoturvallisuuden tulisi olla osa organisaation toimintaa ja kokonaisvaltaista riskienhallintaa muodostaen myös perustan toiminnan jatkuvuudelle. Tietoturvallisuus integroituu organisaatioissa osaksi riskienhallintaa tietoturvallisuuteen liittyvien riskien kautta.[986]

> Katakri 2020:n osa-alueessa turvallisuusjohtaminen T03 on käsitelty turvallisuusriskienhallinnan vaatimuksia ja vaatimuksien toteuttamiseen liittyviä hyviä käytäntöjä. Viranomaisnäkökulman vuoksi vaatimus keskittyy lähinnä turvallisuusluokiteltujen tietojen turvaamiseen, jolloin niihin

[982] Porvari 2012: 84.
[983] Lisää riskistä käsitteenä ks. luku 2.2.3 (” Uhka ja riski sekä niiden keskeiset eroavaisuudet”).
[984] Andersson 2018: 3–4; Katakri 2015.
[985] Valtiovarainministeriön julkaisuja 22/2017a: 11, 16.
[986] Andreasson & Koivisto 2013: 32, 38.

kohdistuvat riskit on arvioitava ja tietoturvallisuustoimenpiteet on mitoitettava riskiarvion mukaisesti. Vaatimuksen toteutusesimerkki kuitenkin painottaa hyvien käytänteiden mukaisesti, että tietoturvallisuusriskienhallinta tulisi olla osa organisaation toimintaa ja muuta riskienhallintaa. Tietoturvallisuustoimenpiteet tulisi mitoittaa riskiperusteisesti, jolloin tietoturvallisuusriskienhallinnan avulla varmistettaisiin riittävien tietoturvallisuustoimenpiteiden toteuttaminen. Tietoturvallisuusriskienhallinta tulisi olla myös jatkuvaa ja järjestelmällistä toimintaa. Lisäksi sen toteuttamiseen tulisi osallistua riittävästi asiantuntijoita. Riskiarvio sekä siihen liittyvät valvonta- ja turvatoimet tulisivat olla dokumentoituna. Riskien arvioinnissa ja analysoinnissa olisi käytettävä toiminnon näkökulmasta asianmukaista ja ymmärrettävää informaatiota tuottavaa menetelmää. Saatuja tuloksia tulisi hyödyntää (turvallisuusluokiteltujen tietojen) tietoturvallisuustoimenpiteiden suunnittelussa ja toteuttamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa sekä muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä.

Katakrin F02-vaatimuksessa on myös käsitelty erikseen fyysisten turvatoimien riskien arviointia. Olennaista tässä vaatimuksessa on se, että fyysiset turvatoimet on mitoitettava riskien arvioinnin mukaisesti, jossa otetaan huomioon erinäisiä seikkoja liittyen luottamuksellisiin (turvallisuusluokiteltuihin) tietoihin. Tällaisia seikkoja ovat esimerkiksi tietojen salassapitoperuste, käsittelyyn ja säilytykseen liittyvä aika, paikka ja tapa, hälytystilanteiden vasteaika, ulkoistetut toiminnot (esimerkiksi siivous ja kiinteistöhuolto), sekä muut oman henkilöstön, rikollisen toiminnan tai tiedustelupalveluiden aiheuttamat arvioidut uhat tiedoille. Hyvien käytänteiden tavoin myös fyysisten turvatoimien riskien arviointi tulee olla säännöllistä ja osa koko organisaation riskienhallintaa, sekä lisäksi riskeillä tulee olla nimetyt omistajat.

Katakri 2015 ja 2020 versioiden välillä ei ole suuria eroja riskienhallinnan hyvien käytäntöjen osalta. Myös Katakri 2015 -version vaatimuksissa organisaation suojattavat kohteet tulisi olla tunnistettu, niille tulisi olla nimetty omistaja sekä niihin liittyvät riskit tulisi olla tunnistettu, arvioitu ja riskien suojausmenetelmät tulisi olla suhteutettu riskien tasoon nähden oikein. Lisäksi riskienhallinnan periaatteet tulisi olla kuvattu, riskienhallinnassa tulisi käyttää järjestelmällistä ja jatkuvaa menetelmää, ja turvallisuusjärjestelyt ja riskienhallintapäätökset tulisi olla dokumentoitu. Riskienhallinnassa tulee ottaa huomioon, että kaikilta riskeiltä ei voida täysin suojausjärjestelyillä suojautua. Tästä syystä turvallisuusjärjestelyiden monimuotoisuus (*defence in depth*) on tärkeää ja turvallisuustoteutuksissa tulee

käyttää useampien turvatoimien yhdistelmiä. Katakrin 2015 T05-osa-alueessa on käsitelty myös jatkuvuuden hallinnan osalta poikkeamahavaintoja, jotka ovat suositeltavaa tuoda osaksi riskienarviointia ja tämän pohjalta tarpeen mukaan päivittää jatkuvuus- ja toipumissuunnitelmia.[987] Vaikka Katakri 2015 ja 2020 vaatimuksissa on viranomaisnäkökulma ja etenkin vuoden 2020 versiossa on painotettu paljon turvallisuusluokiteltujen asiakirjojen suojaamista, näiden kriteeristöjen riskienhallintavaatimukset vastaavat hyviä yleisiä käytänteitä ja ovat sovellettavissa niiden ylätasoisuuden vuoksi myös muihin organisaatioihin.

Tietoturvallisuuteen liittyvät riskit eivät liity ainoastaan organisaatioon itsessään eivätkä ne siten ole täysin organisaation omassa hallinnassa, sillä yhä useammin organisaatiot ovat riippuvaisia ulkoisista sidosryhmistä. Näin ollen riskien arvioinnissa tulee kartoittaa sidosryhmät ja niihin liittyvät riskit.[988] Sidosryhmäriskeistä huomioitava on esimerkiksi ulkoistuksista ja toimitusketjuista muodostuvat riskit, joissa organisaation tietoa käsitellään organisaation ulkopuolella.

Organisaation kokonaisriskienhallinnassa tulisi myös huomioida tietosuojaan liittyvät riskit. Huomioitava kuitenkin on se, että henkilötietojen käsittelyn riskien arvioinnin fokuksessa on seuraukset luonnollisten henkilöiden oikeuksille ja vapauksille – ei organisaation toiminnalle. Tiedolla johtamisen kautta tietosuojariskeistäkin olisi mahdollista tunnistaa kriittisiä business-riskejä organisaation toiminnalle, jotka voisi nostaa osaksi organisaation kokonaisriskienhallintaa.[989] Tietosuojariskien eli henkilötietojen käsittelyyn liittyviin riskien arviointeihin kohdistuu käytännön toiminnassa keskeinen puute sen osalta, että riskienhallintaa toteutetaan formaalien mallien tai standardien mukaisesti sekä tiettyjen asiantuntijoiden osaamisen puitteissa, jolloin riskejä arvioidaan herkästi organisaationäkökulmasta rekisteröityjen oikeuksien ja vapauksien sijaan. Hyviin käytänteisiin pohjautuvien riskienhallintaohjeiden ja -mallien noudattaminen ei ole huono asia, sillä se todennäköisesti merkitsee sitä, että organisaation riskienhallinta on järjestelmällistä, säännöllistä ja määrämuotoista. Tätä mallia voi noudattaa tietosuojariskien hallinnassa, mutta samalla tulee huomioida eri sidosryhmien tiedonsaantitarpeet sekä lakisääteinen vähimmäisvaatimus arvioida riskejä ensisijaisesti rekisteröityjen näkökulmasta.

---

[987] Katakri 2015.
[988] Andreasson & Koivisto 2013: 38–39. Ks. myös Katakri 2020:n osa-alueessa turvallisuusjohtaminen T03.
[989] Ks. yksityiskohtaisemmin tietosuojariskien hallinnasta luvusta 2.2.2 (”Tietosuoja”), 2.2.3 (”Uhka ja riski sekä niiden keskeiset eroavaisuudet”) sekä 3.3.3 (”Henkilötietojen käsittelyn riskilähtöisyys ja riskiarviointi”).

Kyberriskeihin sovelletaan samoja riskienhallintaperiaatteita kuin muihinkin riskeihin. Teknologian ja kybertoimintaympäristön kehittyessä nopeasti kyberriskejä on kuitenkin hyvä arvioida muita riskejä useammin.[990] Tässä pääluvussa käsiteltävä NIS 1 ja 2 -direktiivien mukainen verkko- ja tietojärjestelmien riskienhallinta on kyberriskien hallintaa, sillä keskiössä on järjestelmien tietoturvan parantaminen kybertoimintaympäristössä. Käytännössä kuitenkin organisaatioiden tietoturvariskien hallinnassa ei välttämättä eritellä kyberriskejä omaksi osa-alueekseen vaan riskien arviointi saattaa olla järjestelmäkohtaista.

Onnistuneen riskienhallinnan tunnuspiirre on se, että riskienhallinta on sulautunut organisaation normaaliin toimintaan, jolloin sitä suoritetaan säännöllisesti ja ennakoivasti. Säännöllisestä riskienhallinnasta on taloudellista ja imagollista hyötyä organisaatiolle, mutta myös säännölliset riskienhallintatoimet ovat jokaisen organisaation häiriöttömän toiminnan edellytys[991]. Myös esimerkiksi henkilötietojen käsittelyyn liittyviä riskejä tulisi arvioida säännöllisesti sekä ennen uusia käsittelytoimia aloitusta, ja näiden riskiarvioiden perusteella suunnitella ja toteuttaa tietoturvatoimenpiteitä[992]. Käytännön toiminnassa tällainen säännöllisyys ei aina toteudu, sillä monissa organisaatioissa riskienhallintaa saatetaan toteuttaa kertaluontoisesti tietoturvariskien osalta eikä riskejä arvioida uudelleen säännöllisesti. Valitettavasti tietoturvamaturiteetiltaan epäkypsemmissä organisaatioissa riskienhallinnassa ei myöskään huomioida tietoturvaa tai tietosuojaa riittävällä tasolla tai ollenkaan, jolloin tietoturvakehittäminen ja poikkeamiin reagoiminen on enemmän reaktiivista kuin proaktiivista. Tällöin mahdollinen, säännöllinen riskien arviointi keskittyy lähinnä muihin riskeihin kuin tietoturva- ja tietosuojariskeihin, kuten esimerkiksi henkilöstö- ja liiketoimintariskeihin.

Tietoturvariskien hallinnan osalta tulee painottaa johdon vastuuta. Näin ollen sopiva ja hyvien käytänteiden mukainen vaatimuskehys löytyy OECD:n suosituksesta, jonka OECD on luonut digitaaliseen turvallisuuteen[993] kohdistuvien poikkeamien ja uhkien määrän kasvun myötä. Suositus koskee digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi: suosituksen yleisten periaatteiden mukaan **kaikkien** sidosryhmien[994] tulisi ymmärtää digitaaliseen turvallisuuteen kohdistuvat riskit ja niiden hallintakeinot sekä ottaa vastuuta riskien hallinnasta. Kaikkien

990 Traficomin julkaisuja 2/2020: 15.
991 Hyvönen 2017: 251–253.
992 Ks. esimerkiksi luku 3.3.3 (”Henkilötietojen käsittelyn riskilähtöisyys ja riskiarviointi”).
993 Digitaalista turvallisuutta käsitteenä on käsitelty luvussa 2.2.4 (”Keskeinen kyberterminologia”).
994 Sidosryhmiä tässä kontekstissa ovat hallitukset, julkiset ja yksityiset organisaatiot sekä yksilöt, jotka käyttävät digitaalista ympäristöä taloudellisessa ja yhteiskunnallisessa toiminnassaan.

sidosryhmien tulisi hallita näitä riskejä avoimesti, ihmisoikeus- ja perusarvonmyönteisellä tavalla sekä toimia yhteistyössä keskenään myös kansainvälisesti. Suosituksen toimintaperiaatteiden mukaan johtajien ja päättäjien tulisi varmistaa, että digitaaliseen turvallisuuteen kohdistuvien riskien arviointi tulisi olla jatkuvaa ja systemaattista, sen tulisi olla riskien käsittelyä koskevan päätöksentekoprosessin tukena ja tavoitella riskien pienentämistä hyväksyttävälle tasolle. Johtajien ja päättäjien tulisi myös varmistaa, että turvatoimenpiteet ovat oikein mitoitettuja ja soveltuvia riskiin nähden sekä huomioida innovaatiotoiminta osana digitaaliseen turvallisuuteen kohdistuvien riskien pienentämisessä. Viimeisimpänä johtajien ja päättäjien tulisi varmistaa, että käytössä on valmius- ja jatkuvuussuunnitelma, joka perustuisi myös riskien arviointiin.[995] Tästäkin OECD:n suosituksesta huolimatta johdon vastuuta tietoturvariskien hallinnan osalta ei ole kuitenkaan painotettu viime vuosien lainsäädännön kehityksessä riittävällä tasolla. NIS 2 -direktiivin myötä tähän tosin tulee parannus joidenkin organisaatioiden osalta, sillä direktiivin 20 artiklassa suoraan vastuutetaan keskeisten ja tärkeiden toimijoiden hallintoelimet hyväksymään 21 artiklassa esiintyvät kyberturvallisuusriskien hallintatoimenpiteet sekä valvomaan kyseisen artiklan täytäntöönpanoa.

Yhteenvetona todettakoon, että kaikissa tietoturvariskien hallintaan viittaavissa ohjeistuksissa ja viitekehyksissä painottuu mallista ja ajasta riippumatta sama aihe: tietoturvariskien hallinnan säännöllisyys ja systemaattisuus sekä turvatoimenpiteiden mitoittaminen riskiperusteisesti. Käytännön toiminnassa tällainen tietoturvariskien säännöllinen arviointi ei aina välttämättä toteudu, sillä säännöllinen riskiarviointi kohdistuu lähinnä muihin kuin tietoturvariskeihin tai tietoturvariskien arviointi on kertaluonteista tai hyvin epäsäännöllistä. Tämä havainto puoltaa sitä, että tietoturvariskien hallinnan velvollisuuksia voisi ulottaa lainsäädännöllä laajemmin kaikkiin organisaatioihin. Tietoturva- ja tietosuojalainsäädännön kehityksessä onkin ollut havaittavissa painotus riskienhallinnassa suorien tietoturvavaatimuksien sijaan. Kuitenkin valitettavasti riskilähtöisten tietoturvatoimenpiteiden toteuttaminen koskee kaikkia organisaatioita ainoastaan henkilötietojen turvaamisen osalta suoraan velvoittavan tietosuoja-asetuksen myötä. Tietosuojariskien arvioinnissa keskeisenä näkökulmana on luonnollisten henkilöiden oikeuksien ja etujen suojaaminen henkilötietojen käsittelyssä. Vastakohtaisesti organisaation tietoturvariskienhallinnassa painopiste on organisaation toiminnan ja tietojen suojaamisessa huomioimalla tietoturvariskien vaikutuksia esimerkiksi organisaation maineeseen, talouteen, jatkuvuuteen ja asiakastyytyväisyyteen. Tietoturvallisuuden tulisi olla osa kokonaisriskienhallintaa ja organisaation normaalia

[995] OECD 2015, *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity,* OECD/LEGAL/0415: 3, 5–7; Valtiovarainministeriön julkaisu 28/2016: 7, 13–15, 32, 44

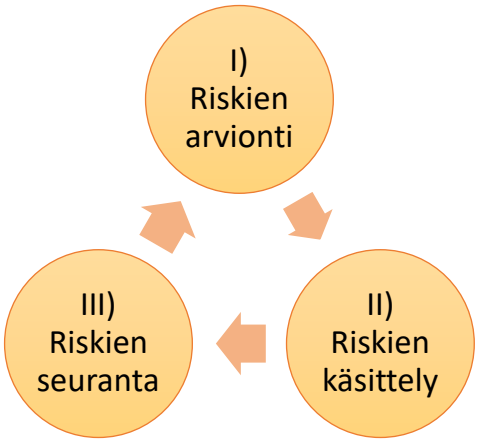
toimintaa. Lisäksi organisaation johdolla tulisi olla päävastuu riskienhallinnasta ja riskien hallintakeinojen toteutumisesta.

4.2.2 Hyvä riskienhallintaprosessi

Nykyisin lainsäädännön kehityksessä on painotettu paljon riskien huomiointia, arviointia tai hallintaa. Esimerkiksi tietosuoja-asetuksen 24 ja 25 artiklojen mukaan rekisterinpitäjän *on huomioitava* riskit, jotka kohdistuvat luonnollisen henkilön oikeuksiin ja vapauksiin. Toisena esimerkkinä on jo kumotun NIS 1 -direktiivin vaatimus, jonka mukaan keskeisten palvelujen tarjoajien piti järjestelmiensä tietoturvallisuuden takaamiseksi *arvioida* järjestelmiinsä kohdistuvat riskit. Tästä kolmantena esimerkkinä on NIS 1 -direktiivin implementoinnin myötä tullut lisäys useaan toimialakohtaiseen säädökseen[996], jonka mukaan *X:n on huolehdittava viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta*. Myös NIS 2 -direktiivin osalta riskitoimenpiteinä on huomioitu riskien hallinta: NIS 2 -direktiivin 21 artiklan mukaan toimijoiden tulee tehdä tietoturvatoimenpiteinä muun muassa riskianalyyseja sekä muita tietoturvatoimenpiteitä *hallitakseen* kyberturvallisuusriskejä.

Edellä mainituista lainsäädännön esimerkkitoimista *hallinta* on käsitevalintana parhain ja kattavin, sillä se vastaa hyviä käytänteitä. Esimerkeistä taas riskien huomiointi ei vastaa hyvien riskien hallintakäytänteiden systematiikkaa eikä se kuvaa riskienhallinnan riittävää tasoa ja siihen liittyviä eri vaiheita. Myöskään riskien arviointi ei ole yksistään riittävä toimenpidetasoltaan, koska se kuvaa vain yhtä riskienhallinnan vaihetta. Yksinkertaisimmillaan riskienhallinnan prosessi voidaan jakaa kolmeen vaiheeseen: riskien arviointi, käsittely ja seuranta. Näitä vaiheita on avattu yksityiskohtaisemmin seuraavaksi.

[996] Sähkömarkkinalaki (588/2013) 29 a §, maakaasumarkkinalaki (587/2017) 34 a §, ilmailulaki (864/2014) 128 a §, raideliikennelaki (1302/2018) 169 §, alusliikennepalvelulaki (623/2005) 16 § sekä laki liikenteen palveluista (320/2017) 140 § ja 161 §.



Kuvio 6. Riskienhallinnan vaiheet

Riskien arviointi

Riskien arvioinnilla tarkoitetaan toimenpiteitä, joilla pyritään tunnistamaan haavoittuvuuksia ja uhkia sekä niiden mahdollisia seurauksia. Se on tärkeä osa riskienhallintaa ja organisaatioiden tietoturvan kehitystyötä, jonka tulisi olla säännöllistä ja jatkuvaa toimintaa. Uhkien tunnistamisen jälkeen niiden todennäköisyys ja seuraukset arvioidaan.[997] Uhkista muodostuu riskejä. Riskien määrittelyn jälkeen organisaatio arvio riskinsietokykynsä eli sen riskin suuruuden tason, johon organisaatio on valmis sitoutumaan[998].

Formaalissa, ISO 31000 -standardiin pohjautuvassa mallissa riskien arviointiprosessia ennen tehdään toimintaympäristön määrittely eli riskienhallintapolitiikan, muuttujien ja riskikriteerien määritteleminen. Tämän jälkeen riskien arviointiprosessi jakaantuu kolmeen vaiheeseen: riskien tunnistaminen, riskianalyysi ja riskien merkityksen arviointi.[999] Nämä vaiheet on esitetty asian selventämiseksi alla olevassa kuviossa.

[997] Andersson 2018: 3–4; VAHTI 7/2003: 15, 18, 21, 41.
[998] Valtiovarainministeriön julkaisuja 22/2017a: 15.
[999] Valtiovarainministeriön julkaisuja 22/2017a: 18–20.

Kuvio 7. Riskien arvioinnin kolme vaihetta

Käytännössä tietosuojariskien arvioinnissa toteutuu samat vaiheet: Ensiksi arvioidaan henkilötietojen käsittelyyn liittyvät uhkat, jonka jälkeen tunnistetaan niistä aiheutuvat riskit rekisteröityjen oikeuksille ja vapauksille. Sitten tehdään riskianalyysi, eli arvioidaan uhkan todennäköisyyttä ja vaikutuksia, jolloin saadaan riskiä koskeva riskiluku. Tämän jälkeen riskiluvun kriittisyyden perusteella arvioidaan mahdollisia hallintakeinoja.

Organisaation riskejä arvioitaessa on huomioitava se, että ajan kuluessa riskin merkitys voi muuttua. Myös psykologisten ja inhimillisten tekijöiden vuoksi riskien käsittely-, tunnistamis- ja sietokyky voivat vaihdella yksilöittäin.[1000] Näin ollen riskejä tulisi olla arvioimassa useampi henkilö. Lisäksi riskien arvioijien tulee

[1000] Valtiovarainministeriön julkaisuja 22/2017a: 18–26.

omata substanssiosaamista, eli esimerkiksi tietoturvariskien kohdalla alan tietämystä ja osaamista. Ilman riittävää osaamista, on haastavampi tunnistaa mahdollisia uhkia.

Riskien hallintakeinot ja käsittely

Riskien arvioinnin jälkeen päätetään riskien hallintakeinoista, jonka jälkeen riskit käsitellään. Riskien hallintakeinot ovat tapoja, joilla riskiin reagoidaan.[1001] Täydellinen riskien hallitseminen on mahdotonta, joten organisaatio määrittelee aina tietoisesti tai tiedostomattaan oman riskinottohalukkuutensa sekä riskienhallintaan panostuksensa tason[1002].

Käytännössä riskien hallintakeinoja ovat riskin mitigointi, riskin poistaminen, riskin välttäminen, riskin siirtäminen ja riskin hyväksyminen.

1) Mitigointi: riskin mitigoinnilla eli pienentämisellä tarkoitetaan riskin merkityksen taikka suuruuden pienentämistä eri hallintakeinojen avulla.

2) Poistaminen: riskin poistaminen ei välttämättä ole koskaan täysin mahdollista, sillä yksittäisen riskin poistaminen saattaa aiheuttaa uusia riskejä. Riskien mahdollisiin seurauksiin voidaan kuitenkin ennakkoon varautua.

3) Välttäminen: riskin välttämisellä tarkoitetaan sellaista tilannetta, jossa kyseisestä toiminnasta pidättäydytään kokonaan ja siten vältetään riski.

4) Siirtäminen: riskin siirtämistä taikka jakamista kokonaan tai osittain yhden tai useamman osapuolen kanssa, esimerkiksi vakuutusyhtiön kanssa.

5) Hyväksyminen: riskit voidaan myös hyväksyä ja säilyttää sellaisenaan. Tällöin esimerkiksi organisaatio on saattanut arvioida, että riski on siedettävällä tasolla ja suojautumistoimenpiteet eivät merkittävästi kustannuksiin nähden pienennä riskiä. Joihinkin riskeihin saattaa myös liittyä positiivisia mahdollisuuksia, jolloin tiettyjä riskejä saatetaan tietoisesti hyväksyä.[1003] Turvallisuusriskien osalta tällaisia positiivia mahdollisuuksia kuitenkin harvoin tunnistetaan, sillä usein turvallisuustason heikkeneminen ja siitä koituvat seuraukset eivät aiheuta mitään positiivista[1004]. Lisäksi huomioitava on, että organisaation ei tulisi tietosuojariskien osalta koskaan

[1001] Andersson 2018: 3–4; VAHTI 7/2003: 6, 21.
[1002] Valtiovarainministeriön julkaisuja 22/2017a: 14.
[1003] Andersson 2018: 3–4; VAHTI 7/2003: 21; Valtiovarainministeriön julkaisuja 22/2017a: 15–16.
[1004] Ks. lisää pohdintaa riskin positiivisuuteen liittyen luku 2.2.3 (”Uhka ja riski sekä niiden keskeiset eroavaisuudet”).

> hyväksyä korkean tason riskejä luonnollisten henkilöiden oikeuksille ja vapauksille, vaan riskejä tulisi mitigoida. Mikäli henkilötietojen käsittelyn riskitaso olisi hallintakeinojenkin jälkeen korkealla tasolla, organisaation tulisi kuulla valvontaviranomaista ennen käsittelytoimien aloittamista.

Riskien hallintatoimenpiteiden jälkeen jäljelle jääviä riskejä kutsutaan jäännösriskeiksi, joihin ei voida taikka ei haluta vaikuttaa. Jäännösriskejä tulisi käsitellä organisaation johtoryhmän hyväksymän menetelmän mukaisesti ja tarvittaessa myös käsitellä johtoryhmän kanssa.[1005] Näin korostuisi myös johdon vastuu.

Riskien hallintakeinojen päättämisen lisäksi kyseisille keinoille tulisi päättää vastuulliset riskien käsittelijät sekä mahdollinen käsittelyaikataulu. Huomioitava on myös se, että riskienhallinta ja käsittelytoimenpiteiden toteutus voivat aiheuttaa itsessään prosessin aikana uusia riskejä, esimerkiksi jos käsittelytoimenpiteet epäonnistuvat tai ne tehdään tehottomuudesta tai kiireestä johtuen liian myöhään. Riskien käsittely vaatii myös aktiivista viestintää ja yhteydenpitoa riskeihin ja toimintaympäristöön liittyvien osapuolten kesken.[1006]

Riskien seuranta

Riskienhallinnan tehokkuuden kannalta on keskeistä, että riskien arvioinnin ja käsittelyn jälkeen riskien hallintakeinojen vaikuttavuutta seurattaisiin ja katselmoitaisiin säännöllisesti tai tapauskohtaisesti. Seurantaan kuuluu muun muassa organisaation toimintaympäristön ja riskien muutosten sekä riskikriteereiden muutostarpeiden havaitseminen. Dokumentointi on myös tärkeää, sillä tätä kautta organisaatio pystyy osoittamaan lakiperusteisten riskienhallintavaatimusten toteutumisen, sekä seuraamaan kustannuksia ja mahdollisesti myös oppimaan.[1007]

Dokumentoinnin tavoite on edistää riskien johdonmukaista ja tietoista hallintaa, jolloin olisi mahdollista selvittää, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Lisäksi dokumentoinnin avulla viranomainen voisi jälkikäteen arvioida riskienhallintavelvoitteiden toteutumista. Dokumentointia voisi toteuttaa esimerkiksi kirjallisten turvallisuusohjeiden, toimintasuunnitelmien ja riskiarvioiden taikka turvallisuustarkastustodistuksien muodossa. Dokumentointi voisi olla osana myös varautumista koskevia suunnitelmia sekä muita turvallisuusriskien hallintaa.[1008] Riskienhallinnan säännöllisyyden todentamiseksi ja osaltaan myös riskienhallintatyön helpottamiseksi dokumentoinnissa tulee huomioida

[1005] Valtiovarainministeriön julkaisuja 22/2017a.: 16.
[1006] Valtiovarainministeriön julkaisuja 22/2017a: 26–28.
[1007] Valtiovarainministeriön julkaisuja 22/2017a: 28.
[1008] HE 192/2017 vp: 65, 68, 70, 72, 74, 76, 78, 79.

kunnollinen versionumerointi, eli esimerkiksi kirjaamalla ylös päivämäärät, versio sekä tehdyt muutokset.

Lopuksi voidaan todeta, että nykylainsäädännön kehityksen osalta tietoturvariskien hallinnan vaatimukset ovat jatkuvasti parantuneet. Riskienhallintaprosessin (*arviointi – käsittely – seuranta*) osalta suurin tunnistettava puute lainsäädännössä on kuitenkin nimenomaan riskien seurannassa, sillä lainsäädännössä ei ole tarpeeksi suoraan vaadittu hyvien käytänteiden mukaisesti organisaatioita tekemään säännöllistä riskienhallintaa ja seuraamaan jo tunnistettuja riskejä säännöllisesti. Esimerkiksi nykyisellään lainsäädännössä ilmenevät vaatimukset hallita riskejä sisältävät hyvien käytänteiden pohjalta oletusarvoisesti myös riskien seurannan, mutta lainsäädännössä tulisi vielä korostaa suoraan seurannan säännöllisyyttä. Tulevan kyberturvallisuuslain myötä riskienhallinnan säännöllisyyttä on korostettu paremmin.

Esimerkiksi kyberturvallisuuslain 7 §:n mukaisesti toimijoiden tulisi *tunnistaa, arvioida ja hallita* toiminnoissaan tai palveluntarjonnassaan käytettävien viestinverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvia riskejä. Lisäksi toimijan toteuttamien riskienhallintatoimenpiteiden tulee olla *ajantasaisia,* oikeasuhteisia ja riittäviä suhteessa riskeihin. Kyberturvallisuuden riskienhallinta olisi tällöin luonteeltaan jatkuvaa ja hallintatoimenpiteiden tulisi olla ennen kaikkea ajantasaisia eli vastata ajantasaista teknologista kehitystä ja tunnettuja parhaita käytänteitä siitä, kuinka kyberturvallisuusriskeiltä voidaan suojautua tai niiden vaikutuksia minimoida. Kyberturvallisuuslain 8 §:n mukaisesti säädettyä riskienhallintavelvoitetta toteutetaan kyberturvallisuutta koskevalla riskienhallinnan toimintamallilla, jota on päivitettävä ja pidettävä ajantasaisena osana jatkuvaa riskien tunnistamista ja arviointia. Toimintamallissa tunnistetaan, analysoidaan, arvioidaan ja käsitellään viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvia riskejä *säännöllisesti.*[1009] Kyberturvallisuuslaissa ilmenevät riskienhallintavaatimukset vastaavat hyviä riskienhallinnan käytänteitä ja riskien arvioinnin säännöllisyyttä on korostettu erityisesti hallituksen esityksessä asianmukaisesti. Edistyksellistä on myös se, että hallituksen esityksessä on viitattu käytänteisiin, eli riskien hallintatoimenpiteiden tulisi vastata parhaita käytänteitä kyberturvallisuusriskeiltä suojautumisen osalta. Valitettavasti lain painotus kohdistuu vain rajattuun joukkoon toimijoita.

Huomioitava on se, että ajantasaisuuden korostaminen säännöllisyyden sijaan erityisesti säännöksissä voi aiheuttaa tulkinnallisia haasteita. Esimerkiksi toimija saattaa omasta mielestään pitää dokumentaatiotaan ajantasaisena, vaikka toimija katselmoi ja päivittää epäsäännöllisesti riskiarviointejaan 5 vuoden välein. Kun

[1009] HE 57/2024 vp: 159–162.

riskejä arvioidaan ”ajantasaisuuden” sijaan säännöllisesti vaikkapa vuosittain, on todennäköisempää, että dokumentaatio on myös ajantasainen ja uusia riskejä havaitaan proaktiivisemmin eikä reaktiivisesti. Ajantasaisuus ei käsitteenä ole täysin huono, mutta olisi parempi painottaa riskienhallinnan säännöksissä hyvien käytänteiden mukaisesti säännöllisyyttä.

4.3 Sääntelyjärjestelmän verkko- ja tietojärjestelmien tietoturvariskien hallinta

4.3.1 Keskeisten, tärkeiden ja kriittisten toimijoiden jaottelu lainsäädännössä

Alkuperäinen NIS 1 -direktiivi jakoi toimijat keskeisten palvelujen tarjoajiin sekä digitaalisen palvelun tarjoajiin, jonka myötä kansallista, toimialakohtaista tietoturvariskien hallintaa koskevaa lainsäädäntöä päivitettiin. Todettakoon kuitenkin näin alkuun, että NIS 2 -direktiivissä tätä toimialakohtaista jaottelua on laajennettu koskemaan suurempaa osaa taloudesta, jotta sen piiriin saadaan kaikki toimialat ja palvelut, jotka ovat elintärkeitä sisämarkkinoiden yhteiskunnallisten ja taloudellisten avaintoimintojen kannalta. Täten NIS 2 -direktiivillä pyritään erityisesti korjaamaan puutteet, jotka liittyvät keskeisen palvelun tarjoajien ja digitaalisen palvelun tarjoajien väliseen erotteluun. Tällainen erottelu on osoittautunut vanhanaikaiseksi, koska se ei kuvasta toimialojen tai palvelujen merkitystä yhteiskunnalliselle ja taloudelliselle toiminnalle sisämarkkinoilla.[1010]

Alkuperäisen NIS 1 -direktiivin mukaan keskeisten palvelujen tarjoajalla tarkoitettiin julkista tai yksityistä toimijaa, joka tarjosi sellaista keskeistä yhteiskunnan tai talouden kriittisten toimintojen ylläpitävää palvelua. Lisäksi palveluntarjoajan piti kuulua NIS 1 -direktiivin liitteessä II määriteltyihin keskeisten palvelujen ja niiden tarjoajia koskeviin toimialoihin ja toimialojen osa-alueisiin, jotta se katsottiin keskeisten palvelujen tarjoajaksi. Tällaisia toimialoja olivat energia, pankkiala ja finanssimarkkinoiden infrastruktuuri, liikenne, terveydenhuoltoala, juomaveden toimittaminen ja jakelu sekä digitaalinen infrastruktuuri. NIS 1 -direktiivin mukaan kyseisen toimijan oli myös oltava riippuvainen verkko- ja tietojärjestelmistä, joihin tulevalla poikkeamalla piti olla *merkittäviä haitallisia vaikutuksia* palvelun tarjoamiseen. Poikkeaman haitallisen vaikutuksen merkittävyyden arvioimiseksi (6 artikla) piti ottaa vähintään huomioon toimialakohtaisten tekijöiden lisäksi toimialojen väliset tekijät. NIS 1 -direktiivin mukaan tällaisia huomioitavia toimialojen välisiä tekijöitä olivat palvelusta riippuvaisten käyttäjien lukumäärä, toimijan

[1010] NIS 2 -direktiivin kohta 6.

markkinaosuus, poikkeaman vaikutus vakavuutensa ja kestonsa puolesta yleiseen turvallisuuteen sekä talouden ja yhteiskunnan toimintoihin, toimijan merkitys riittävän palvelutason ylläpitämisessä huomioon ottaen vaihtoehtoisten palvelun-tarjontakeinojen saatavuus sekä maantieteellinen levinneisyys alueella, johon poikkeama saattoi vaikuttaa. Myös NIS 1 -direktiivin liitteessä II määriteltyjen muiden toimialojen riippuvuus tarjotusta palvelusta oli yksi huomioitava tekijä arvioitaessa poikkeaman haitallista vaikutusta.

NIS 1 -direktiivin liite II:n toimialajaottelun mukaisesti keskeisten palvelujen tarjoajia koskevat riskienhallintaan ja tietoturvaan liittyvät vaatimukset jakaantuivat myös useaan eri kansalliseen, toimialakohtaiseen säädökseen. Merkittävä osa muista jäsenvaltioista toimivat toisin kuin Suomi, eli ottivat käyttöön alkuperäisen NIS 1 -direktiivin implementoinnin yhteydessä yhden niin sanotun kyberturvallisuuslain[1011]. Suomi teki näin ollen poikkeavan ratkaisun NIS 1 -direktiivin implementoinnin osalta, mikä myös sirpaloitti nykyistä tietoturvan sääntelyjärjestelmää.

NIS 1 -direktiivin liitteen II mukaisia toimialoja sekä NIS 1 -direktiivin implementoinnin kannalta keskeisiä, kansallisia toimialakohtaisia säädöksiä on sijoitettu seuraavaksi esitettyyn taulukkoon.

Taulukko 3. NIS 1 -direktiivin keskeisten palvelujen tarjoajien toimialat

Toimiala	Perustelu[1012] sekä keskeinen toimialakohtainen säädös
Energia • Öljy • Sähkö • Kaasu	Öljyn osa-alueella ei tunnistettu alkuperäisessä NIS 1 -direktiivissä asetettuja kriteerejä täyttäviä keskeisiä palveluita tai palvelun tarjoajia kansallisella tasolla. Sähkönjakelu on keskeinen palvelu yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi ja se on lähtökohtaisesti aina riippuvainen verkko- ja tietojärjestelmistä. Tältä osin NIS 1 -direktiivin mukaisena palveluna pidettiin sähkönjakelua jakeluverkossa ja suurjännitteisessä jakeluverkossa (pois lukien sähkönjakelu suljetussa jakeluverkossa) sekä siirtopalvelua kantaverkossa ja järjestelmävastaavan kantaverkonhaltijan tarjoamia järjestelmäpalveluita. Kaasun osa-alueella maakaasulla on merkittävä asema Suomen energiankulutuksessa ja näin ollen NIS 1 -direktiivin mukaiseksi keskeiseksi palveluksi katsottiin maakaasumarkkinalain mukainen siirtopalvelu siirtoverkossa ja järjestelmävastaavan siirtoverkonhaltijan tarjoamat järjestelmäpalvelut.

[1011] HE 57/2024 vp: 123–124.
[1012] HE 192/2017 vp: 44–56.

Toimiala	Perustelu[1012] sekä keskeinen toimialakohtainen säädös
	Sekä sähkön että kaasun osalta keskeisten palvelujen tarjoajien kontaktina on toiminut Energiavirasto, jolle on tullut ilmoittaa merkittävistä järjestelmien tietoturvallisuuteen liittyvistä häiriöistä. Keskeinen toimialakohtainen säädös: - sähkömarkkinalaki (588/2013) - maakaasumarkkinalaki (587/2017)
Pankkiala ja finanssimarkkinoiden infrastruktuuri	Pankkialan osalta NIS 1 -direktiivissä katsottiin keskeiseksi toimijaksi luottolaitokset sekä finanssimarkkinoiden infrastruktuurin osalta tietyt kauppapaikkojen ylläpitäjät ja keskusvastapuolet. Esimerkiksi pörssitoiminta katsottiin NIS 1 -direktiivissä määritellyksi keskeisten palvelujen tarjoajaksi, sillä sen toiminta on riippuvainen verkko- ja tietojärjestelmistä ja toimintaan kohdistuvalla tietoturvahäiriöllä voisi olla merkittäviä haitallisia vaikutuksia toiminnan harjoittamiseen. Keskeinen toimialakohtainen säädös: - laki luottolaitostoiminnasta (610/2014)
Liikenne • Lentoliikenne • Rautatieliikenne • Vesiliikenne • Tieliikenne	Liikenteen osalta palvelut on jaettu kolmeen tasoon: liikenteen ohjauspalveluihin, keskeisen infrastruktuurin ylläpitämiseen sekä liikennepalveluiden tarjoamiseen. NIS 1 -direktiivin mukaisia keskeisiä palveluita olivat tämän jaottelun perusteella: 1. Liikenteen ohjauspalvelut a. Lennonvarmistuspalvelu b. Rautatieliikenteen ohjauspalvelu c. Vesiliikenteen alusliikennepalvelu (VTS) 2. Keskeisen infrastruktuurin ylläpitäminen a. Lentoasemat / Lentoaseman pitäjä b. Rautatiet / Rataverkon haltija ja rautatieliikenteen harjoittajat c. Satamat / Satamanpitäjä d. Tieverkko / Tieinfrastruktuuriin liittyvät digitaaliset tietojärjestelmät (ITS-järjestelmät) 3. Liikennepalveluiden tarjoaminen

Toimiala	Perustelu[1012] sekä keskeinen toimialakohtainen säädös
	a. Liikennepalveluita voi tarjota useampi kilpaileva toimija kansallisella ja kansainvälisillä markkinoilla. Liikenteenohjauksen rooli tieliikenteen osalta on katsottu eroavan toistaiseksi muista liikennemuodoista, sillä ohjaus on perustunut paljolti tietojärjestelmistä ja viestintäverkoista riippumattomiin liikennesääntöihin ja tiemerkintöihin. Tieliikenteen ohjausta ei pidetty NIS 1 -direktiivin keskeisenä palveluna, mutta on huomioitu, että liikenteen älykkään automaation kehittyessä tätä tulee arvioida uudelleen. Keskeinen toimialakohtainen säädös: - ilmailulaki (864/2014) - raideliikennelaki (1302/2018) - liikennekaari (320/2017, laki liikenteen palveluista) - laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta (485/2004) - alusliikennepalvelulaki (623/2005) - laki liikennejärjestelmästä ja maanteistä (503/2005)
Terveydenhuoltoala • Terveydenhuollon tarjoajat (esim. sairaalat ja yksityisklinikat)	Terveydenhuollon alalla palveluntarjoajina toimivat yksityiset ja julkiset sosiaali- ja terveydenhuollon palvelujen antajat. NIS 1 -direktiivin mukaisena keskeisenä palveluna pidettiin terveydenhuollon asiakastietojen sähköistä käsittelyä sekä laitteiden käyttämistä ja ylläpitoa yksityisten ja julkisten sosiaali- ja terveydenhuollon palvelujen tarjonnassa. Järjestelmien asiakastietojen käsittelyn tietoturvallisuudesta, terveydenhuollon laitteita koskevat vaatimukset sekä velvoitteet häiriöiden ilmoittamisesta valvontaviranomaiselle olivat jo ennestään otettu huomioon sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007, nykyisin (703/2023) sekä eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista annetussa laissa (629/2010), jotka täyttivät myös NIS 1 -direktiivin vaatimukset. Näissä on säädetty muun muassa tietojärjestelmien tietoturvaan liittyvistä vaatimuksista, tietojärjestelmien arvioinnista tietoturvallisuuden arviointilaitoksen toimesta sekä laitteiden turvallisuudesta.

Toimiala	Perustelu[1012] sekä keskeinen toimialakohtainen säädös
	Keskeinen toimialakohtainen säädös: - laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (703/2023) - laki eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista (629/2010, nimike muutettu lailla 720/2021)
Juomaveden toimittaminen ja jakelu	Vesihuoltoa pidettiin alkuperäisen NIS 1 -direktiivin mukaisena keskeisenä palveluna, josta huolehtivat vesihuoltolaitokset. Kuitenkin kaikilla vesihuoltolaitokseen kohdistuvilla poikkeamilla ei välttämättä katsottu aiheutuvan direktiivissä tarkoitettua merkittävää haitallista vaikutusta. Täten hallituksen esityksessä täsmennettiin keskeisiksi palvelujen tarjoajiksi sellaiset vesihuoltolaitokset, jotka toimittavat vettä vähintään 5000 kuutiometriä per vuorokausi, sekä sellaiset vesihuoltolaitokset, jotka toimittavat näille vettä. Tällaisia huoltovarmuuden kannalta kriittisiä vesilaitoksia on noin 40 kappaletta Suomessa. Vesihuoltolain (119/2001) 15 § on sisältänyt jo ennestään varautumisvelvoitteen tietojärjestelmiin liittyviin riskeihin, mikä täytti myös NIS 1 -direktiivin verkko- ja tietojärjestelmien turvallisuusvaatimukset. Vesihuoltolaissa ei kuitenkaan ollut ennen velvoitetta ilmoittaa järjestelmien tietoturvahäiriöistä viranomaiselle, joten tämä oli uusi lisäys 15 b §:nä. Keskeinen toimialakohtainen säädös: - vesihuoltolaki (119/2001)
Digitaalinen infrastruktuuri • esimerkiksi nimipalvelujen tarjoajat, aluetunnusrekisterit ja IXP:t (Internet Exchange Point)	Teleyrityksen määritelmä on kattanut keskeisimmät digitaalisen infrastruktuurin toiminnot, muun muassa nimipalvelun tarjoamisen sekä internetin yhdysliikennepisteet tietyiltä osin. Vaikka teletoiminta on yhteiskunnan toiminnan kannalta keskeistä, teleyrityksiä ei ole käsitelty osana alkuperäisen NIS 1 -direktiivin soveltamisalaa. Tässä kontekstissa alkuperäisen NIS 1 -direktiivin mukaiseksi keskeiseksi palveluksi katsottiin kuitenkin aluetunnusrekisterin ylläpito. Aluetunnusrekisterien ylläpitäjän tietoturvavastuista säädetiin sähköisen viestinnän palveluista annetun lain 21 luvussa, ja näiden katsottiin täyttävän NIS 1 -direktiivin verkko- ja tietojärjestelmiä koskevat vaatimukset. FI-aluetunnusrekisteriä pitää Liikenne- ja viestintävirasto ja AX-aluetunnusrekisteriä ylläpitää Ahvenanmaan maakuntahallinto.

Toimiala	Perustelu[1012] sekä keskeinen toimialakohtainen säädös
	Keskeinen toimialakohtainen säädös: - sähköisen viestinnän palveluista annettu laki (917/2014)

Kuten aikaisemmin tässä tutkimuksessa on mainittu: NIS 2 -direktiivin toimeenpanon myötä NIS 1 -direktiivin täytäntöönpanosäännökset tullaan kumoamaan toimialakohtaisista, eli yllä mainituista laeista[1013]. Tämä tulee selkiyttämään ja yhtenäistämään nykyistä organisaatioiden tietoturvan sääntelyjärjestelmää.

Alkuperäisessä NIS 1 -direktiivissä oli myös eroteltu keskeisten palvelujen tarjoajista digitaalisen palvelun tarjoajat. Digitaalisen palvelun tarjoajalla tarkoitettiin sellaista toimijaa, joka tarjosi digitaalista palvelua. Digitaalisia palveluita olivat alkuperäisen NIS 1 -direktiivin määritelmän mukaan:

a) pilvipalvelu;

b) verkossa toimiva markkinapaikka; tai

c) verkossa toimiva hakukone.[1014]

Verrattuna edeltäjäänsä NIS 2 -direktiivissä digitaalisen palvelun tarjoajat kuuluvat direktiivin liitteen II mukaisiin muihin kriittisiin toimialoihin. Tässä liitteessä digitaalisen palvelun tarjoajat ovat *verkossa toimivien markkinapaikkojen tarjoajat, verkossa toimivien hakukoneiden tarjoajat sekä verkkoyhteisöalustojen tarjoajat*. NIS 2 -direktiivin 6 artiklan mukaan verkkoyhteisöalustalla tarkoitetaan alustaa, jonka avulla loppukäyttäjät voivat olla yhteyksissä toisiinsa, jakaa sisältöä, hakea tietoa ja viestiä keskenään erilaisilla päätelaitteilla, esimerkiksi pikaviestikeskusteluiden ja julkaisujen muodossa. Näin ollen suoranaista viittausta pilvipalveluun ei enää NIS 2 -direktiivissä ole osana digitaalisten palveluiden

[1013] Hallituksen esityksessä 57/2024 (s. 1) ehdotetaan säädettäväksi kyberturvallisuuslaki kyberturvallisuusdirektiivin täytäntöönpanemiseksi. Lisäksi esityksessä ehdotetaan muutettavaksi julkisen hallinnon tiedonhallinnasta annettua lakia, sähköisen viestinnän palveluista annettua lakia, ilmailulakia, raideliikennelakia, liikenteen palveluista annettua lakia, alusliikennepalvelulakia, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettua lakia, sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annettua lakia, sähkömarkkinalakia, maakaasumarkkinalakia, energiavirastosta annettua lakia, sähkö- ja maakaasumarkkinoiden valvonnasta annettua lakia, vesihuoltolakia, sakon täytäntöönpanosta annettua lakia, maa-asemista ja eräistä tutkista annettua lakia sekä vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annettua lakia.

[1014] Alkuperäisen NIS 1 -direktiivin vaatimusten mukaisesti digitaalisen palvelun tarjoajien kohdalla pienet yritykset sekä mikroyritykset eivät kuulu säädöksen soveltamisalaan. Pieniä yrityksiä ovat komission suosituksen mukaan alle 50 hengen yritykset ja, jonka vuosiliikevaihto tai taseen loppusumma on alle 10 miljoonan euroa (2003/361/EY).

määritelmää. Huomioitava kuitenkin on se, että pilvipalveluiden tarjoajat kuuluvat NIS 2 -direktiivin liitteessä I olevaan digitaalisen infrastruktuurin toimialaan, joka puolestaan kategorioidaan erittäin kriittiseksi toimialaksi.

Riippuen laeista, digitaalisten palveluiden osalta vaaditaan tarkkuutta tulkinnoissa, sillä esimerkiksi digipalvelulaissa (306/2019) digitaalinen palvelu on määritelty laveammin kuin NIS 2 -direktiivissä. Tässä laissa digitaalisella palvelulla tarkoitetaan *verkkosivustoa tai mobiilisovellusta sekä niihin liittyviä toiminnallisuuksia*. NIS 2 -direktiivin toimeenpanevassa kyberturvallisuuslaissa[1015] ei 2 §:n määritelmissä ole tarkennettu digitaalista palvelua. Vastakohtaisesti 2 §:n kohdassa 10 määritellään, että pilvipalvelulla tarkoitetaan digitaalista palvelua. Kuitenkin kyseisen lain liitteessä II digitaalisen palvelun tarjoajaksi on määritelty NIS 2 -direktiivin mukaiset toimijat.

Sääntelyjärjestelmässä esiintyvät käsite-erot voivat vaikeuttaa sääntelyjärjestelmän ymmärrettävyyttä ja epäyhtenäisyytensä takia johtaa virheellisiin tulkintoihin.

NIS 2 -direktiivin voimaan tulon myötä edellä kuvattu, vanhanaikaiseksi tituleerattu jaottelu keskeisten palvelujen tarjoajiin ja digitaalisen palvelun tarjoajiin loppui. Tällöin NIS 2 -direktiivin velvoitteet koskevat ensinnäkin **CER-direktiivin (2022/2557/EU, direktiivi kriittisten toimijoiden häiriönsietokyvystä) nojalla kriittisiksi toimijoiksi määriteltyjä toimijoita** näiden koosta riippumatta. Huomioitava on se, että CER-direktiivin toimialat ovat lähes identtiset NIS 2 -direktiivin toimialojen kanssa. CER-direktiivin toimialoja ovat: energia, liikenne, pankkiala, rahoitusmarkkinoiden infrastruktuuri, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, julkishallinto, avaruus sekä elintarvikkeiden tuotanto, jalostus ja jakelu. *CER-direktiivin mukaisia kriittisiä toimijoita* ovat julkinen tai yksityinen yhteisö, jonka jäsenvaltio on määritellyt 6 artiklan mukaisesti kuuluvan taulukkoliitteen kolmannessa sarakkeessa esitettyihin toimijaluokkiin. 6 artiklan mukaan kriittisen toimijan on myös tarjottava yhtä tai useampaa keskeistä palvelua, itse toimija toimii ja sen kriittinen infrastruktuuri sijaitsee kyseisen jäsenvaltion alueella ja poikkeamalla olisi merkittäviä haitallisia vaikutuksia toimijan yhden tai useamman keskeisen palvelun tarjoamiseen taikka muiden keskeisten palvelujen tarjoamiseen kyseisestä palvelusta riippuvaisilla CER-direktiivin mukaisilla toimialoilla. CER-direktiivin mukaiset kriittiset toimijat tulee määritellä ensimmäisen kerran vuonna 2026[1016].

[1015] Ks. HE 57/2024 vp: 274, 296.
[1016] HE 57/2024 vp: 12.

Toiseksi NIS 2 -direktiivin velvoitteet koskevat direktiivin liitteessä I ja II määriteltyjä toimialojen toimijoita, jotka ovat artiklan 3 mukaisesti **keskeisiä tai tärkeitä toimijoita**. Pääsääntönä on, että NIS 2 -direktiivin toimijat tulisivat olla komission suosituksen 2003/361/EY mukaisia keskisuuria organisaatioita[1017]. Kokokriteeri ei tosin päde 2 artiklan 2 kohdan mukaisesti palvelun tarjoajiin, jotka ovat verkkotunnusten rekisteröintipalveluja tarjoavia toimijoita, yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, luottamuspalvelun tarjoajia, aluetunnusrekistereitä sekä DNS-palvelun-tarjoajia. Kokorajoitus ei myöskään päde, jos toimia tarjoaa ainoana jäsenvaltiossa yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeistä palvelua; häiriö toimijan tarjoamassa palvelussa voisi vaikuttaa merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen; häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia; taikka toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta. Kokorajoitus ei myöskään koske kansallisessa lainsäädännössä määriteltyä keskustason julkishallinnon toimijaa. Tämän lisäksi kokorajoitus ei koske kansallisessa lainsäädännössä määriteltyä aluetason julkishallinnon toimijaa, joka riskiperusteisen arvioinnin perusteella tarjoaa palveluita, joiden häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimintoihin.

Verrattuna aikaisemmin esiteltyyn NIS 1 -direktiivin toimialajaotteluun, NIS 2 -direktiivin myötä toimialajaottelu laajenee ja kyberturvallisuuden riskienhallinnan velvoitteet koskevat yhä useampaa toimijaa. Käsitteiden ja systematiikan osalta NIS 2 -direktiivi vaikuttaa hieman sekavalta, koska direktiivin liitteissä I ja II korostetaan *kriittisiä toimialoja*, mutta itse direktiivin toimijat ovat joko keskeisiä toimijoita tai tärkeitä toimijoita. Sen sijaan kriittiset toimijat sijoittuvat CER-direktiiviin.

> NIS 2 -direktiivin **liitteessä I** määriteltyjä *erittäin kriittisiä toimialoja* ovat energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, tieto- ja viestintätekniikkapalveluiden (TVT-palvelujen) hallinta, julkishallinto ja avaruus. **Liitteessä II** määriteltyjä *muita kriittisiä toimialoja* ovat posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden tuotanto, jalostus ja jakelu, valmistus, digitaalisen palvelun tarjoajat ja tutkimustoiminta.

[1017] Yhtä lailla NIS 1 -direktiivi rajasi digitaalisen palvelun tarjoajien kohdalla pienet yritykset sekä mikroyritykset pois säädöksen soveltamisalasta.

Koska aikaisempaa NIS 1 -direktiivin jaottelua tituleerattiin vanhanaikaiseksi, tämänkaltainen NIS 2 -direktiivin mukainen jaottelu pitäisi luonnollisestikin olla vastakohtaisesti nykyaikaista. Sitä se ei kuitenkaan ole. Kyberturvallisuuden tärkeyden korostamiseksi sekä yhteiskunnan toimivuuden että yksilöiden oikeuksien toteutumisen osalta olisi ollut relevantimpaa ja ”nykyaikaisempaa” korostaa kaikkia edellä mainittuja liitteen I ja II mukaisia toimialoja tasavertaisesti kriittisinä sekä niiden mukaisia toimijoita tärkeinä. Nykyisellään muotoiltu hankaloittaa tietoturvan sääntelyjärjestelmän ymmärrettävyyttä.

Keskeisenä, positiivisena muutoksena NIS 1 ja NIS 2 -direktiivin toimialojen välillä on se, että NIS 2 -direktiivin myötä täysin uusia toimialoja ovat liitteen I mukaisesti jätevesi, yritysten välinen TVT[1018]-palvelujen hallinta, julkishallinto ja avaruus. Liitteen II mukaisesti täysin uusia toimialoja ovat posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden tuotanto, jalostus ja jakelu, tutkimustoiminta sekä valmistus. Esimerkiksi valmistukseen katsotaan kuuluvaksi lääkinnällisten laitteiden, tietokoneiden ja elektronisten tuotteiden, sähkölaitteiden, muiden koneiden ja laitteiden sekä kulkuneuvojen valmistus. Vastakohtaisesti alkuperäisen NIS 1 -direktiivin kohdassa 50 laitteiden valmistajat ja ohjelmistojen kehittäjät luettiin direktiivin ulkopuolelle, vaikkakin heidän tuotteensa katsottiin lisäävän verkko- ja tietojärjestelmien turvallisuutta: heitä kuitenkin koskivat tuotevastuuseen liittyvät säännöt. Näiden toimijoiden jättäminen NIS 1 -direktiivin soveltamisalan ulkopuolelle oli varsin perusteetonta, sillä tuotevastuusäännöt eivät ole riittäviä sellaisenaan lisäämään hyviä tietoturvallisia käytänteitä, kuten tietoturvariskien hallintaa.

NIS 2 -direktiivin myötä energia-alalla vaatimukset koskevat myös vety- ja latauspisteiden palveluntarjoajia, digitaalisen infrastruktuurin alalla muun muassa konesaleja sekä digitaalisen palvelun tarjoajien osalta myös verkkoyhteisöalustojen tarjoajia[1019]. Erityisesti konesalien ulottaminen NIS 2 -direktiivin piiriin on ollut tärkeä lisäys, sillä konesalit ovat kriittisiä organisaatioiden järjestelmien ja palveluiden toimimisen osalta.

Jäsenvaltiot voivat myös säätää, että vaatimuksia sovelletaan paikallistason julkishallinnon toimijoihin sekä opetus- ja koulutusalan laitoksiin, etenkin kun niissä harjoitetaan olennaisen tärkeää tutkimustoimintaa. Direktiivissä on erikseen määritelty tutkimusorganisaatioiksi toimijat, jotka eivät ole opetus- ja koulutusalan laitoksia. Toisin sanoen NIS 2 -direktiivi mahdollistaa velvoitteiden ulottamisen opetus- ja koulutusalan laitoksiin, vaikka ne eivät ole direktiivissä määriteltyjä (kaupallisia) tutkimusorganisaatioita. Näin ollen myös opetus- ja

[1018] TVT eli tieto- ja viestintätekniikka.
[1019] Ks. Liikenne- ja viestintäministeriö 2023.

koulutuslaitoksissa harjoitettava olennaisen tärkeä tutkimustoiminta jää jäsenvaltion määriteltäväksi. NIS 2 -direktiivin implementoimista tiedonhallintalakiin ei kuitenkaan uloteta koskemaan korkeakouluja tai muita opetus- ja koulutusalan laitoksia, ellei niiden ensisijaisena tavoitteena ole harjoittaa soveltavaa tutkimusta tai kokeellista kehitystyötä tutkimusten tulosten hyödyntämiseksi kaupallisiin tarkoituksiin[1020]. Näin ollen Suomessa ei käytetä tutkimuksen osalta kansallista liikkumavaraa, koska lakivelvoitteita ei pääsääntöisesti uloteta opetus- ja koulutusalan laitoksiin. Asiaa voisi jopa tulkita niin, että kansallisesti tärkeänä tutkimustoimintana nähdään ainoastaan kaupallisiin tarkoituksiin hyödynnettävä tutkimus. Tämä on harmillinen asia, sillä korkeakouluissa on myös sellaista tutkimustoimintaa, jossa käsitellään paljon erityisiä henkilötietoja, liikesalaisuuksia sekä kehitetään uusia keksintöjä ja innovaatioita. Toisin sanoen korkeakoulujen tutkimustoiminnassa on paljon suojattavaa tietoa ja tietoturvatasoltaan korkeakoulut pitäisi olla samojen vähimmäisvaatimusten piirissä kuin muut keskeiset ja tärkeät toimijat. Ratkaisu myös pirstaloittaa tietoturvasääntelyä, sillä viranomaisia koskevat NIS 2 -direktiivin vaatimukset implementoidaan tiedonhallintalakiin, jonka alkuperäisen 4 luvun tietoturvasääntely ulottuu tiedonhallintayksikköinä toimiviin korkeakouluihin. Hajaantuneen sääntelyn lisäksi tällaiset ratkaisut tekevät tietoturvan sääntelyjärjestelmästä epäyhtenäisemmän ja se näyttäytyy vähemmän oikeudenmukaisena. Huomioitava kuitenkin on, että NIS 2 -direktiivin mukaiset 4a-luvun kyberturvallisuutta koskevat velvollisuudet koskevat yliopistoja ja ammattikorkeakouluja, mikäli ne katsotaan CER-direktiivin mukaisiksi kriittisiksi toimijoiksi[1021].

Yhteenvetona todettakoon, että alkuperäinen NIS 1 -direktiivi ei yltänyt hyvin sille asetettuihin tavoitteisiin verkko- ja tietojärjestelmien suojaamisen osalta, koska se jätti ulkopuolelle monta verkkoyhteiskunnan kannalta kriittistä toimialaa. Suomi teki myös huonon ratkaisun sen osalta, että NIS 1 -direktiivi implementoitiin toimialakohtaisesti, sillä tämä ratkaisu epäyhtenäisti tietoturvan sääntelyjärjestelmää ja teki siitä vaikeammin tavoitettavan. NIS 2 -direktiivin myötä tietoturvan sääntelyjärjestelmä paranee huomattavasti, sillä sen vaatimukset tulevat koskemaan yhä useampaa toimialaa ja toimijaa EU:n jäsenvaltioissa kuin aikaisemmin. Esimerkiksi erityisen positiivista kyberturvallisuuden ja yksilöiden turvallisuuden parantamisen osalta on se, että NIS 2 -direktiivin vaatimukset ulottuvat myös TVT-palveluntarjoajiin sekä konesaleihin, koska näillä on tärkeä yhteys organisaatioiden ja yhteiskunnan palveluiden toimintaan. NIS 2 -direktiivi ei ole kuitenkaan

[1020] HE 57/2024 vp: 213.
Tutkimusorganisaatiot, jotka jakavat ja hyödyntävät tutkimustuloksia kaupallisiin tarkoituksiin, voivat olla tärkeitä osia arvoketjuissa, mikä tekee niiden viestintäverkkojen ja tietojärjestelmien turvallisuudesta merkityksellisen EU:n sisämarkkinoiden kyberturvallisuuden kannalta. Ks. HE 57/2024 vp, s. 150.
[1021] HE 57/2024 vp: 331–332.

täydellinen, sillä säädöksessä käytettävä käsitteistö on omiaan vaikeuttamaan tietoturvan sääntelyjärjestelmän ymmärrettävyyttä. Esimerkiksi NIS 2 -direktiivin velvoitteet kohdistuvat keskeisiin, tärkeisiin ja kriittisiin toimijoihin, vaikka epäselväksi jää, tuoko tällainen jaottelu jotain tulkinnallista lisäarvoa: NIS 2 -direktiivin vaatimukset koskevat CER-direktiivin mukaisia kriittisiä toimijoita sekä NIS 2 -direktiivissä käsiteltyjä keskeisiä ja tärkeitä toimijoita, jotka sijoittuvat kriittisille ja erittäin kriittisille toimialoille. Edistyksellisempää olisi ollut, jos NIS 2 -direktiivissä ilmenevät toimialat olisivat olleet tasavertaisesti kriittisiä ja toimijat esimerkiksi tärkeitä (lukuun ottamatta CER-direktiivin kriittisiä toimijoita). Huomioitava on myös se, että NIS 2 -direktiivin myötä digitaalisen palvelun määritelmä ei ilmene tietoturvan sääntelyjärjestelmässä johdonmukaisesti[1022].

NIS 2 -direktiivin vaatimukset tullaan implementoimaan pääosin kyberturvallisuuslain ja tiedonhallintalain kautta kansallisten, yksittäisten toimialakohtaisten säädöksien sijaan. Tämä on positiivinen kehitysaskel tietoturvavelvoitteiden yhtenäistämisen suhteen. Kansallisen harkinnan mukaisesti vähimmäisvaatimuksia voitaisiin ulottaa laajemmin muihinkin toimijoihin. Tällä hetkellä kuitenkin hallituksen esityksestä 57/2024 NIS 2 -direktiivin täytäntöönpanemiseksi ei ilmene, että sääntely ulottuisi julkishallintoa sekä keskisuuria ja suuria keskeisiä tai tärkeitä toimijoita pidemmälle pienempiin organisaatioihin tai muihin toimijoihin[1023]. Tuleva yleislakina toimiva kyberturvallisuuslaki on ainoastaan yleislaki lakien etusijajärjestys (*lex specialis*) huomioon ottaen. Sitä ei voida katsoa todelliseksi yleislaiksi, kuten esimerkiksi tietosuojaa koskevia säädöksiä, jotka ulottuvat kaikkiin henkilötietoja käsitteleviin organisaatioihin koosta tai toimialasta riippumatta. Tietoturvaan liittyvä sääntely on edelleenkin tulevaisuudessa hajaantunutta useampaan säädökseen, mikä vaikuttaa negatiivisesti tietoturvasääntelyn tavoitettavuuteen ja ymmärrettävyyteen. Lisäksi tällainen hajanainen, vain tiettyihin toimijoihin kohdistuva sääntely ei edistä asianmukaisesti yksilöiden oikeutta kyberturvalliseen toimintaympäristöön ja henkilötietojensa suojaan ”vähemmän tärkeiden” organisaatioiden toiminnan osalta.

[1022] Vertaa esimerkiksi: NIS 2 -direktiivissä digitaalisen palvelun tarjoajat ovat verkossa toimivien markkinapaikkojen tarjoajat, verkossa toimivien hakukoneiden tarjoajat sekä verkkoyhteisöalustojen tarjoajat. Kansallisessa digipalvelulaissa (306/2019) digitaalisella palvelulla tarkoitetaan verkkosivustoa tai mobiilisovellusta sekä niihin liittyviä toiminnallisuuksia.

[1023] Lain soveltamisalan ja toimijan määritelmän olisi tarkoitus vastata NIS 2 -direktiivin 2 ja 3 artikloja siten, että se kattaisi kaikki NIS 2 -direktiivin vähimmäissoveltamisalaan kuuluvat keskeiset ja tärkeät toimijat, pois lukien julkishallinnon sektori, jonka osalta NIS 2 -direktiivin mukaisten velvoitteiden täytäntöönpanosta säädettäisiin julkisen hallinnon tiedonhallinnasta annetussa laissa. Ks. HE 57/2024 vp, s. 145–146.

4.3.2 Eri toimijoiden tietoturvariskien hallintavelvoitteet

Alkuperäisen NIS 1 -direktiivin vaatimusten mukaan keskeisten palvelujen tarjoajien piti järjestelmiensä tietoturvallisuuden takaamiseksi toteuttaa teknisiä ja organisatorisia toimenpiteitä[1024], arvioida järjestelmiinsä kohdistuvat riskit sekä toteuttaa asianmukaiset toimenpiteet toiminnan jatkuvuuden takaamiseksi ja järjestelmien turvallisuuspoikkeamien hallitsemiseksi. Myös NIS 2 -direktiivissä esiintyy samantyyppinen vaatimus, sillä direktiivin 21 artiklan mukaan organisaation on toteutettava asianmukaisia ja oikeasuhteisia teknisiä, operatiivisia ja organisatorisia toimenpiteitä hallitakseen riskejä, joita kohdistuu toiminnoissaan tai palveluntarjonnassaan käytettävien verkko- ja tietojärjestelmien turvallisuuteen. Lisäksi tarkoitettujen toimenpiteiden on perustuttava kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan verkko- ja tietojärjestelmät sekä näiden järjestelmien fyysinen ympäristö poikkeamilta[1025].

NIS 1 -direktiivi jätti paljon tulkinnan varaa toteuttamisen osalta muun muassa sen suhteen, mikä katsottiin olevan asianmukaista. Sama asianmukaisuuden vaatimus toistuu myös NIS 2 -direktiivissä. Kuten aikaisemminkin tässä tutkimuksessa on todettu[1026], asianmukaisia toimenpiteitä ja turvallisuustasoa arvioitaessa ja niistä päätettäessä tulisikin perusteissa tukeutua riskien arvioinnin tuloksiin. Muutoin asianmukaisuuden arviointi olisi kovin henkilöitynyttä ja riippuen henkilön osaamisesta, arviointi voi johtaa puutteellisiin tietoturvatoimenpiteisiin ja siten myös alhaiseen tietoturvatasoon[1027]. NIS 2 -direktiivistä ilmenee paremmin se, että tietoturvatoimenpiteet perustuvat verkko- ja tietojärjestelmien turvallisuuteen kohdistuviin riskeihin kuin NIS 1 -direktiivistä. Huomioitava on se, että tästä näkökulmasta organisaation tietosuoja- ja tietoturvariskien arviointien kohde asianmukaisten tietoturvatoimenpiteiden osalta on eri. Tietosuojariskien arviointi on käsittelytoimikohtaista eli riskejä arvioidaan tietyn henkilötietojen käsittelytoimen kannalta, jolloin asianmukaiset tietoturvatoimenpiteet perustuvat tähän käsittelytoimikohtaiseen riskiarviointiin. NIS 2 -direktiivin mukainen riskiarvio kohdistuu järjestelmiin ja niiden turvallisuuteen, jolloin riskejä voidaan arvioida sekä järjestelmäkohtaisesti että osana laajempaa organisaation kokonaisriskienhallintaa. Tällöin asianmukaisia tietoturvatoimenpiteitä voisi esimerkiksi arvioida järjestelmäkohtaisen riskiarvion pohjalta, jolloin myös keskeiset ja

[1024] Teknisiä ja organisatorisia toimenpiteitä on käsitelty yksityiskohtaisemmin luvussa 3.4 (”Tietoturvan sääntelyjärjestelmän erilaiset tietoturvatoimenpiteet”).
[1025] NIS 2 -direktiivin kaikki vaaratekijät huomioiva toimintamalli tulee ilmi direktiivin kohdassa 79 sekä artiklassa 21.
[1026] Ks. luku 3.4.1 (”Tekniset ja organisatoriset toimenpiteet sekä operatiiviset toimenpiteet”).
[1027] Lisäksi riskejä tulisi olla arvioimassa useampi henkilö, joilla olisi substanssiosaamista, jotta relevanttien uhkien tunnistaminen onnistuisi. Ks. lisää hyviä käytänteitä luvusta 4.2.2 (”Hyvä riskienhallintaprosessi”).

yleisesti toistuvat järjestelmien tietoturvaan liittyvät kyberriskit voisi nostaa osaksi kokonaisriskienhallintaa.

Käytännössä asianmukaisia toimenpiteitä toiminnan jatkuvuuden takaamiseksi ja järjestelmien turvallisuuspoikkeamien hallitsemiseksi voisivat olla esimerkiksi jatkuvuus- ja toipumissuunnitelmien dokumentointi, henkilökunnan koulutus, proaktiiviset ja reaktiiviset menettelyt turvallisuuspoikkeamien hallintaan[1028], turvallisuustapahtumien jäljittäminen lokeista sekä varmuuskopiointi ja varmuuskopioiden palauttamisen säännöllinen harjoittelu. Tällaistenkin toimenpiteiden laajuus, kohdentaminen ja käyttökelpoisuus tulee perustua riskien arviointiin eli toimenpiteiden tulee olla riittävän tehokkaita riskien hallitsemiseksi. Lisäksi mikäli toimenpide sisältää henkilötietojen käsittelyä, tulee myös tällaisen käsittelyn osalta arvioida käsittelyn tarpeellisuutta sekä riskejä luonnollisen henkilön oikeuksille ja vapauksille.

NIS 1 -direktiivin mukaisia digitaalisen palvelun tarjoajia koskivat lähes samat vaatimukset kuin keskeisiä palvelujen tarjoajia, mutta järjestelmiensä turvaamiseksi teknisissä ja organisatorissa toimenpiteissä oli riskin tason mukaisesti otettava huomioon myös järjestelmien ja tilojen turvallisuus, poikkeamien käsittely, jatkuvuus, kansainvälisten standardien noudattaminen sekä seuranta ja testaukset. Lisäksi alkuperäisen NIS 1 -direktiivin kohdassa 49 painotettiin, että keskeisten palvelujen tarjoajien osalta riskin suuruus oli käytännössä isompi kuin riskin suuruus digitaalisen palvelun tarjoajille, koska keskeiset palvelut ovat olennaisia yhteiskunnan ja talouden kriittisten toimintojen ylläpitämiseksi. Näin ollen katsottiin, että digitaalisen palvelun tarjoajia koskevien turvallisuusvaatimusten tuli olla lainsäädännössä löyhempiä. Samassa lain kohdassa todettiin myös se, että digitaalisen palvelun tarjoajilla tuli olla vapaus toteuttaa sellaiset toimenpiteet, jotka he katsovat aiheellisiksi verkko- ja tietojärjestelmiensä turvallisuusriskien hallitsemiseksi[1029]. Tällainen NIS 1 -direktiivin ”pehmeämpi” sääntely tuli parhaiten ilmi vertailtaessa digitaalisen palvelun tarjoajan poikkeamien ilmoitusvastuuta keskeisen palvelun tarjoajien vastuisiin: digitaalisen palvelun tarjoajan poikkeaman ilmoitusvelvollisuutta sovellettiin ainoastaan, mikäli digitaalisen palvelun tarjoajalla oli pääsy tietoihin, joita tarvitaan poikkeaman vaikutuksen arviointiin[1030]. NIS 2 -direktiivissä ei enää ole vastaavaa kirjausta siitä, että digitaalisen palvelun tarjoajia koskevien turvallisuusvaatimusten tulisi olla lainsäädännössä löyhempiä kuin muiden toimijoiden vaatimukset. Tämä yksinkertaistaa ja selkeyttää sääntelyä.

[1028] Tähän voi liittyä esimerkiksi automaattisten havainnointi- ja hälytystyökalujen käyttäminen.
[1029] Andersson 2018: 8.
[1030] Hert, Markopoulou & Papakonstantinou 2019: 5:

Tietoturvariskien hallintaan liittyvä lainsäädäntö keskeisten palvelujen tarjoajien suhteen jakaantui NIS 1 -direktiivin myötä moneen eri kansalliseen, toimialakohtaiseen säädökseen[1031]. Suomi teki muista EU-maista poikkeavan ratkaisun, mikä ei ollut hyvä, sillä se teki tietoturvasääntelystä kovin sirpaleista ja epäyhtenäistä. Tätä sirpaleisuutta ja epäyhtenäisyyttä on pyritty seuraavaksi havainnollistamaan tässä tutkimuksessa kolmen esimerkkitoimialan kautta. Valittuja toimialoja ovat NIS 1 -direktiivin jaottelun pohjalta energia-ala, pankkiala ja finanssimarkkinoiden infrastruktuurit sekä liikenteen osalta rautatieliikenne, sillä ne ovat hyvin erilaisia toimialoja verrattuna toisiinsa[1032].

> **1) Energia-ala:** Sekä sähkömarkkinalaissa (588/2013) että maakaasumarkkinalaissa (587/2017) ei ole ennen NIS 1 -direktiivin velvoitteita ollut vaatimuksia tietojärjestelmiin ja viestintäverkkoihin kohdistuvasta riskien hallinnasta.
>
> NIS 1 -direktiivin implementointi tapahtui sähkömarkkinalakiin lisättynä 29 a §:nä, kun taas maakaasumarkkinalain osalta lisäys tehtiin 34 a §:nä.
>
> Molempien lisäyksien sisältö on sama, tosin sähkömarkkinalaissa puhutaan verkonhaltijasta ja maakaasumarkkinalaissa siirtoverkonhaltijasta. Pykälälisäyksien mukaan (siirto-)verkonhaltijan on huolehdittava tietojärjestelmiin ja viestintäverkkoihin kohdistuvien riskienhallinnasta sekä ilmoitettava viipymättä Energiavirastolle käyttämiinsä tietojärjestelmiin tai viestintäverkkoihin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena sähkönjakelu tai maakaasun siirto voi keskeytyä merkittävässä laajuudessa.
>
> Sähkömarkkinalakiin tehtiin myös lisäys 62 §:n osalta, jonka mukaan 29 a §:ä ei sovelleta suljettuun jakeluverkkoon eikä suljetun jakeluverkon

[1031] Esimerkiksi seuraavanlainen suppea lisäys tuli sähkömarkkinalakiin (588/2013, 29 a §), maakaasumarkkinalakiin (587/2017, 34 a §), ilmailulakiin (864/2014, 128 a §), raideliikennelakiin (1302/2018, 169 §), alusliikennepalvelulakiin (623/2005, 16 §) sekä lakiin liikenteen palveluista (320/2017, 140 § ja 161 §): *X-toimijan on huolehdittava viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Lisäksi X:n on ilmoitettava viipymättä Y:lle käyttämiensä tietojärjestelmiin tai viestintäverkkoihin kohdistuvasta merkittävästä tietoturvahäiriöstä, jonka seurauksena Z-palvelu voi keskeytyä merkittävässä laajuudessa tai Z-palvelun turvallisuuteen on vaikutuksia.*

[1032] Valittujen toimialojen erilaisuuden lisäksi valintaan vaikutti toimialojen kriittisyys yhteiskunnan jatkuvuuden kannalta kansallisella tasolla sekä tutkijan omat preferenssit mielenkiinnon mukaan. Digitaalinen infrastruktuuri on myös kriittinen ja kiinnostava ala, mutta tutkijan mielenkiinnon mukaisesti se rajautui pois, koska esimerkiksi sähköisen viestinnän palveluista annettua lakia kyseisen alan keskeisenä säädöksenä on käsitelty tässä tutkimuksessa laajasti erinäisten tietoturvavaatimusten osalta myös muualla tutkimuksessa, esimerkiksi luvuissa 3.5.4 (”Muu teknisin menetelmin toteutettu valvonta ja välitystiedot”) ja 3.5.5 (”Väärinkäytösten ehkäiseminen ja selvittäminen organisaatioissa”).

haltijaan. Myöhemmin sähkömarkkinalakiin tuli uutena lisäyksenä 49 a § koskien sähkökaupan keskitetyn tiedonvaihdon palveluita, jonka järjestelmävastaavan on huolehdittava käyttämiensä tietojärjestelmiensä riskienhallinnasta. Tähän kuuluu alkuperäisen NIS 1 -direktiivin mukaisesti muun muassa järjestelmien ja tilojen turvallisuus, tietoturvauhkien ja häiriöiden käsittely, liiketoiminnan jatkuvuus, mahdollisten kansainvälisten standardien noudattaminen ja seuranta sekä tarkastusten ja testausten huomioiminen. Säädöslisäyksen tarkoituksena on ollut asiakkaiden henkilötietojen ja markkinaosapuolten liikesalaisuuksien asianmukaisen käsittelyn varmistaminen sekä sähköalan yritysten toimintaan liittyvien tietojärjestelmien, tietoliikenneyhteyksien ja rajapintojen asianmukaisen tietoturvatason järjestäminen[1033].

Edellä mainitut lisäykset etenkin sähkömarkkinalain osalta kuvastavat hyvin eri toimijoiden hajanaisia tietoturvariskien hallintavelvoitteita. Hallituksen esityksessä kyberturvallisuusdirektiivin täytäntöönpanemiseksi ehdotetaan, että maakaasumarkkinalain 34 a § sekä sähkömarkkinalain 29 a § ja 49 a §:n 5 momentti kumotaan tulevan kyberturvallisuuslain myötä.[1034] Kuitenkin esimerkiksi sähkömarkkinalain 49 a §:stä jäisi voimaan 4 momentti, joka sisältää NIS 1 -direktiivistä implementoituja riskienhallintavelvoitteita. Tällöin NIS 2 -direktiivin implementointi ei ratkaise hajanaisen sääntelyn ongelmaa, koska järjestelmien tietoturvariskienhallinnan velvoitteita esiintyy edelleen monessa eri säädöksessä.

2) Pankkiala ja finanssimarkkinoiden infrastruktuurit: Laissa luottolaitostoiminnasta (610/2014) säädetään luottolaitostoiminnasta sekä muusta liiketoiminnasta, jossa yleisöltä hankitaan takaisinmaksettavia varoja. Riskienhallintalähtöisyys ja riskienhallinnan toteuttaminen on säädöksessä koko aika esillä. Lain 9 luvussa on säädetty muun muassa riskienhallintajärjestelmän vaatimuksista, jonka mukaan luottolaitoksella on oltava hallinto- ja ohjausjärjestelmä toimintaan kohdistuvien nykyisten ja tulevien riskien tunnistamiseksi, hallitsemiseksi, rajoittamiseksi, seuraamiseksi ja raportoimiseksi. Tämän järjestelmän on oltava kirjallisesti kuvattu, tehokas ja luotettava, jossa on kuvattu selkeä organisaatiorakenne, sisäisen valvonnan, hallinnon ja laskennan prosessit, riskien raportointiprosessi sekä riskienhallinnan kanssa sopusoinnussa olevat ja sitä edistävät palkitsemisjärjestelmien toimintaperiaatteet ja menettelytavat. Laissa on myös säädetty riskienhallintaan liittyvistä rooleista, jotka jakaantuvat

[1033] HE 144/2018 vp: 18.
[1034] HE 57/2024 vp: 239.

luottolaitoksen hallitukselle, riskivaliokunnalle ja riskien valvontatoiminnolle.

Laissa käsitellään paljon luotto-, markkina ja arvopapeririskejä sekä muita luottolaitostoimintaan liittyviä operatiivisia riskejä. Tietoturvallisuuteen ja tietoturvariskeihin viitataan suoranaisesti hyvin vähän, mutta esimerkiksi lain 9 luvun 16 §:ssä säädetään operatiivisesta riskistä. Tässä kontekstissa operatiivisella riskillä tarkoitetaan epäonnistuneista tai riittämättömistä järjestelmistä, henkilöistä, sisäisistä prosesseista tai ulkoisista tekijöistä aiheutuvia riskejä sisältäen myös verkko- ja tietojärjestelmien turvallisuuteen, häiriösietokykyyn ja eheyteen liittyvät riskit[1035]. 16 §:n mukaan luottolaitoksella on oltavat riittävät, turvalliset ja toimintavarmat tietojärjestelmät. Säädöksen tietoturva- ja riskienhallintanäkökulma kuvastaa myös hyvin toimialan parempaa tietoturvamaturiteettia verrattuna muihin toimialoihin.

Luottolaitoksella on oltava varautumis- ja jatkuvuussuunnitelmat liiketoiminnan vakavien häiriöiden varalta, häiriötilanteissa aiheutuvien vahinkojen rajoittamiseen sekä toiminnan jatkuvuuden turvaamiseen. Epäselväksi jää, mikä on varautumis- ja jatkuvuussuunnitelman ero tässä kontekstissa. Lähtökohtaisesti varautumissuunnittelun lopputuotoksena syntyy jatkuvuus-, toipumis- ja valmiussuunnitelmia. Finanssivalvonnan sivuilla on kuitenkin tiivistetty, että toimijoiden varautumissuunnitelmien sisältö tulee pohjautua selkeästi ja yksityiskohtaisesti skenaarioon, jossa mikään ulkomailla sijaitseva toimijoiden välinen tai sisäinen maksu- tai arvopaperijärjestelmä, toiminto tai tietovarasto ei ole kuukausiin käytettävissä[1036].

NIS 1 -direktiivin myötä lakiin luottolaitostoiminnasta ei tullut muutoksia. Lain operatiiviseen riskienhallintaan liittyvät velvoitteet sekä niitä täydentävä Finanssivalvonnan antama määräys operatiivisten riskienhallinnasta[1037] katsottiin täyttävän suoraan alkuperäisen NIS 1 -direktiivin 14 artiklan keskeisten palvelujen tarjoajien verkko- ja tietojärjestelmien turvallisuutta koskevat vaatimukset.[1038] NIS 1 -direktiivin myötä kuitenkin finanssivalvonnasta annettuun lakiin (878/2008) tehtiin muutokset direktiivin mukaisena toimivaltaisena viranomaisena toimimisesta (50p §) sekä Finanssivalvonnan ja viestintäviraston välisestä yhteistyöstä ja tietojenvaihdosta direktiivin mukaisten tehtävien hoitamisessa (52 a §).

[1035] HE 192/2017 vp: 19.
[1036] Finanssivalvonta 2020.
[1037] Finanssivalvonta 2014.
[1038] HE 192/2017 vp: 53.

Pörssitoimintaan liittyviä riskienhallintavaatimuksia ja häiriöiden ilmoittamista koskevat säännökset, jotka täyttävät alkuperäisen NIS 1 -direktiivin keskeisten palvelujen tarjoajia koskevat vaatimukset, sisältyivät kaupankäynnistä rahoitusvälineillä annetun lain (1070/2017) 3 lukuun[1039]. Kyseisen lain 3 luvun 1 §:n mukaan pörssin on varmistettava toimintaansa liittyvien riskien hallinta ja toimintansa jatkuvuus kaikissa tilanteissa. Lisäksi pörssin on varmistettava, että sen käyttämät järjestelmät ja menettelytavat turvaavat kaupankäyntijärjestelmän toiminnan luotettavuuden ja jatkuvuuden myös häiriötilanteissa. Pörssin on varmistettava, että sillä on riittävä kaupankäyntijärjestelmien häiriönsietokyky, riittävä kapasiteetti toimeksiantojen ja viestien ruuhkahuippujen käsittelyyn ja varmistettava asianmukainen kaupankäynti markkinoiden vakavissa stressiolosuhteissa. Pörssin on myös testattava säännöllisesti kuormituskokein kaupankäyntijärjestelmän toimintaa edellä kuvattujen vaatimusten täyttämiseksi. Edellä mainitun lisäksi pörssin tulisi myös muilla järjestelyillä varautua asianmukaisesti palvelujen jatkuvuuden turvaamiseen[1040]. Lain 3 luvun 2 §:ssä myös täsmennetään, että pörssin on ilmoitettava Finanssivalvonnalle ilman aiheetonta viivytystä muun muassa tavanomaisesta poikkeavista kaupankäyntiolosuhteista sekä rahoitusvälineeseen liittyvistä järjestelmän toimintahäiriöstä. Verrattuna esimerkiksi lakiin luottolaitostoiminnasta, kaupankäynnistä rahoitusvälineillä annetussa laissa on keskitytty pörssin järjestelmien kapasiteettiin ja häiriönsietokykyyn, mutta esimerkiksi dokumentoinnista ja jatkuvuussuunnitelmien teosta ei ole mainittu.

Kaiken kaikkiaan edellä käsitellyt pankkialaa ja finanssimarkkinoiden infrastruktuureja koskevat säädökset eli esimerkiksi laki luottolaitostoiminnasta sekä laki kaupankäynnistä rahoitusvälineillä ovat kattavia. Ne ovat kuitenkin systematiikaltaan kovin erilaisia verrattuina muihin NIS 1 -direktiivin myötä muokattuihin toimialakohtaisiin säädöksiin, mikä kuvastaa tietoturvan sääntelyjärjestelmän epäyhtenäisyyttä. Esimerkiksi pörssitoiminnan osalta laissa kaupankäynnistä rahoitusvälineillä ei mainita sanallakaan järjestelmien turvallisuutta.

3) Rautatieliikenne: Raideliikennelaissa (1302/2018) on säädetty rataverkon haltijan, rautatieliikenteen harjoittajien sekä liikenteenohjauspalvelun tarjoajan turvallisuus- ja riskienhallintavelvoitteista.

Raideliikennelain 6 §:n mukaan näiden toimijoiden on toteutettava tarvittavia riskienhallintatoimenpiteitä toistensa kanssa yhteistyössä. Tähän

[1039] HE 192/2017 vp: 53.
[1040] HE 151/2017 vp: 180.

liittyy myös muiden osapuolien toimintaan liittyvät riskit sekä alihankkijoiden velvoittaminen sopimusteitse riskienhallintatoimenpiteisiin. Kyseisillä toimijoilla on myös oltava turvallisuusjohtamisjärjestelmä (10 §), jonka on varmistettava kaikkien organisaation toimintaan kuuluvien riskien hallinta sekä muiden toiminnasta aiheutuvat riskit. Turvallisuusjohtamisjärjestelmää on päivitettävä huomioon ottaen lainsäädännössä tapahtuvat muutokset. Turvallisuusjohtamisjärjestelmän tarkoituksena on varmistaa, että rautatiejärjestelmä vastaa yhteen toimivuudeltaan turvallisuusvaatimuksia ja -menetelmiä sekä kansallisia oikeussääntöjä. Se on dokumentoitava ja kirjallisessa kuvauksessa on määriteltävä organisaation vastuunjakoa sekä osoitettava muun muussa jatkuvan parantamisen varmistamisen toteutuminen. Lisäksi siihen on sisällytettävä organisaation turvallisuuspolitiikka, tavoitteet turvallisuuden ylläpitämiseksi ja parantamiseksi sekä suunnitelman tavoitteiden saavuttamiseksi. Lain 12 §:n mukaan rautatieliikenteen harjoittajan ja rataverkon haltijan on myös laadittava vuosittain turvallisuuskertomus, jossa on oltava tiedot muun muassa turvallisuustavoitteiden ja -suunnitelmien toteutumisesta sekä sisäisistä turvallisuusauditoinneista.[1041]

Turvallisuusjohtamisjärjestelmän osalta ei määritellä, että turvallisuusjohtamisjärjestelmän tulisi olla jonkun tietyn standardin mukainen. Siinä on kuitenkin esimerkiksi ISO/IEC 27001 -tietoturvallisuudenhallintajärjestelmän standardiin rinnastettavia vaatimuksia. Näitä ovat esimerkiksi jatkuva parantaminen, turvallisuuspolitiikan kehittäminen, laadulliset ja määrälliset tavoitteet turvallisuuden ylläpitämisen ja parantamisen organisoimiseksi, henkilökunnan kouluttaminen, sisäinen auditointi sekä menettelyt riskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi[1042]. Raideliikennelaissa säädetty riskienhallintavelvoite sekä turvallisuusjohtamisjärjestelmää koskevat vaatimukset sääntelevät turvallisuutta kokonaisuudessaan eivätkä ainoastaan tietoturvallisuutta.

Alkuperäisen NIS 1 -direktiivin myötä rautatielakiin, joka on nykyisin kumottu, lisättiin uusi 41 a §. Tässä säädettiin viestintäverkkoihin ja tietojärjestelmiin kohdistuvista tietoturvahäiriöistä ilmoittamisesta sekä riskienhallintavelvollisuudesta. 41 a §:n mukaan valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan olisi huolehdittava käyttämiensä tietojärjestelmien ja viestintäverkkojen kohdistuvien riskien hallinnasta. [1043]

[1041] HE 105/2018 vp: 44–45, 156–159.
[1042] 2016/798/EU: Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/798 rautateiden turvallisuudesta.
[1043] HE 192/2017 vp: 90.

> Myöhemmin kyseinen velvoite siirrettiin raideliikennelain 169 §:än. Lisäksi kyseisten toimijoiden on ilmoitettava viipymättä Liikenne- ja viestintäministeriölle viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvahäiriöstä.
>
> Tämä velvoite ei kuitenkaan koske kaupunkiraideliikenteen rataverkon haltijaa, jonka velvoitteista on säädetty raideliikennelain 154–164 §:ssä. Kaupunkiraideliikenteen rataverkon haltijalla on myös oltava kaikki organisaatioon kohdistuvat riskit huomioiva turvallisuusjohtamisjärjestelmä (154 § ja 158 §) sekä tietoturvaan liittyen on huomioitava myös se, että 163 §:n mukaan rataverkon haltija tai muu liikenteenohjauspalvelusta vastaava saavat käyttää kaupunkiraideliikenteen viestintään viestintäverkkoa, jonka käyttäminen on varmistettu olevan tietoturvallista. Tämä tarkoittaa muun muassa sitä, että tietyt viestiliikennettä, turvalaitteita, onnettomuuksia ja vaaratilanteita koskevat tiedot on säilytettävä tavalla, joka turvaa ne oikeudettomalta puuttumiselta, sekä ne on hävitettävä niiden käyttötarkoituksen loputtua[1044]. Tässä kontekstissa tietojen säilyttämisen turvaaminen oikeudettomalta puuttumiselta olisi mahdollista muun muassa riittävillä pääsynhallinnan kontrolleilla, mutta myös muilla toimenpiteillä, kuten ottaen huomioon tilaturvallisuus ja henkilöstön kouluttaminen. Tapoja on täten monia, ja niiden käytöstä tuleekin päättää arvioimalla riskejä ja reagoimalla niihin asianmukaisesti.
>
> Vaikka NIS 1 -direktiivin velvoitteet eivät ole ulottuneet kaupunkiraideliikenteeseen, lain velvoittama turvallisuusjohtamisjärjestelmä edellyttää jo peruspilareiltaan hyviä turvallisuuskäytäntöjä ja riskienhallintaa. Kaiken kaikkiaan raideliikenteen tietoturvaan ja riskienhallintaan liittyvät vaatimukset kuvastavat hyvin esimerkkitoimialojen ja ylipäätänsä toimialakohtaisen lainsäädännön erilaisia ja hajanaisia tietoturvavaatimuksia sekä epäyhtenäistä, haasteellista NIS 1 -direktiivin implementointia.

Valittujen kolmen esimerkkitoimialan (energia-ala, pankkiala ja finanssimarkkinoiden infrastruktuurit sekä rautatieliikenne) tietoturvaan liittyvät riskienhallintavaatimukset eroavat huomattavasti toisistaan. Kaiken kaikkiaan toimialakohtaisten tietoturvatoimenpiteiden toteuttamisvelvollisuus on näyttäytynyt aikaisemminkin hyvin kirjavasti, sillä tähän on vaikuttanut joillain toimialoilla jo ennen NIS 1 -direktiivin voimaantuloa säädetyt tietoturvavaatimukset sekä toimialakohtainen maturiteettitaso riskienhallinnan ja turvallisuuden osalta. Esimerkiksi nykyisessä voimassa olevassa lainsäädännössä joitain toimijoita on velvoitettu ainoastaan toteuttamaan riskienhallintaa koskien tietojärjestelmien ja

[1044] HE 105/2018 vp: 125, 127, 220–221, 223

viestintäverkkojen tietoturvallisuutta, kun taas toisia toimijoita on velvoitettu ylläpitämään turvallisuusjohtamisjärjestelmää kaikkien toimintaan liittyvien riskien osalta.

Toisena hyvänä esimerkkinä on pankkialan ja finanssimarkkinoiden infrastruktuureja koskeva säädöskehitys, josta on pääteltävissä sekä toimialan korkeampi maturiteettitaso riskienhallinnan ja turvallisuuden osalta, mutta myös toimialan kriittisyys: NIS 2 -direktiivin hyväksymisen aikoihin marraskuussa 2022 hyväksyttiin DORA-säädös (2022/2554/EU, asetus finanssialan digitaalisesta häiriönsietokyvystä), jonka implementointi tapahtuu yhtäaikaisesti NIS 2- ja CER-direktiivien implementoinnin kanssa[1045]. DORA-säädös koskee lähes kaikkia rahoitusalan toimijoita NIS 2 -direktiivin lisäksi. NIS 2 -direktiivin mukaan DORA-säädöstä on kuitenkin pidettävä NIS 2 -direktiiviin liittyvänä alakohtaisena unionin säädöksenä finanssialan toimijoiden osalta[1046]. Näin ollen se on erityissäädös (*lex specialis*) suhteessa NIS 2 -direktiiviin[1047].

> Keskeistä DORA-säädöksessä on, että siinä säädetään tieto- ja viestintätekniikan (TVT) riskien hallinnasta sekä riskienhallintajärjestelmästä. NIS 2 -direktiivin tavoin DORA-säädöksessä on painotettu ylimmän johdon vastuuta[1048]. TVT-riskienhallintajärjestelmä on oltava dokumentoitu ja sitä on tarkasteltava vähintään kerran vuodessa, mikä on hyvä lisäys esimerkiksi verrattuna aikaisempaan luottolaitostoimintaa koskevaan sääntelyyn. DORA-säädöksessä korostetaan myös poikkeuksellisen hyvin proaktiivista tietoturvalähestymistä, esimerkiksi TVT-riskinhallintajärjestelmän on sisällettävä digitaalisen häiriönsietokyvyn strategia, jossa tulee asettaa selkeät tietoturvatavoitteet ja riskimittarit[1049]. Osana TVT-riskinhallintajärjestelmää finanssiyhteisöjen on myös laadittava dokumentoitu

[1045] Kesällä 2024 on ilmestynyt hallituksen esitys HE 67/2024, jonka tarkoituksena on antaa DORA-asetusta täydentävät kansalliset säännökset, panna täytäntöön DORA-muutosdirektiivi sekä antaa NIS 2 -direktiivin ja CER-direktiivin kansallista täytäntöönpanoa täydentävät säännökset pankkitoiminnan ja finanssimarkkinoiden infrastruktuurin osalta (ks. HE 67/2024 vp, s. 1).
[1046] NIS 2 -direktiivin kohta 28. DORA:n säännöksiä tieto- ja viestintätekniikan (TVT) riskienhallintaa, TVT:n poikkeamien hallintaa ja laajavaikutteisten TVT-poikkeamien raportointia sekä säännöksiä digitaalisen häiriönsietokyvyn testauksesta, tiedonjakojärjestelyistä ja TVT-palveluntarjoajana oleviin kolmansiin osapuoliin liittyvistä riskeistä on sovellettava NIS 2 -direktiivin säännösten sijaan. Sama koskee NIS 2 -direktiivin mukaista kyberturvallisuusriskien hallintaa ja raportointivelvoitteita sekä valvontaa ja täytäntöönpanoa DORA:n mukaisiin finanssialan toimijoihin.
[1047] DORA-säädöksessä asetetaan finanssialan toimijoille NIS 2 -direktiivin velvoitteita pidemmälle meneviä velvoitteita kyberuhkiin varautumiseksi. Näin ollen ei ehdoteta finanssialan toimijoita sisällytettävän kyberturvallisuuslakiin. Ks. HE 57/2024 vp, s. 32–33.
[1048] DORA-säädöksen 5 artikla.
[1049] DORA-säädöksen 6 artikla, kohta 8 c.

> tietoturvapolitiikka, otettava käyttöön verkko- ja infrastruktuurin hallinnointirakenne sekä toimintatavat, joilla rajoitetaan fyysinen tai looginen pääsy tieto-omaisuuteen ja TVT-omaisuuteen, laadittava periaatteet ja menettelyt pääsyoikeuksien ja niiden hallinnoinnin osalta, toteutettava vahvan todentamisen mekanismien edellyttämät toimitavat ja protokollat sekä niiden salausavaimien suojaustoimenpiteet, toteutettava TVT-muutostenhallintaa koskeva dokumentaatio menettelyineen sekä otettava käyttöön ohjelmisto- ja korjauspäivityksiä koskevat dokumentoidut toimintaperiaatteet[1050]. Kaiken kaikkiaan DORA-säädöksen tietoturvaa koskevat vaatimukset ovat hyvin yksityiskohtaiset läpi asetuksen. Huomioitavana seikkana aikaisemmin mainittuun jatkuvuus- ja varautumissuunnittelun systematiikkaan liittyen luottalaitostoiminnasta annettuun lakiin: DORA-säädöksessä keskitytään jatkuvuuden osalta sekä jatkuvuussuunnitelmiin että TVT-reagointi- ja palautumissuunnitelmiin[1051].

Yhteenvetona todettakoon, että *asianmukaisia* tietoturvatoimenpiteitä arvioitaessa ja niistä päätettäessä tulisi perusteissa tukeutua riskien arvioinnin tuloksiin. Tämä perusajatus ilmenee sekä tietosuoja-asetuksessa että NIS 2 -direktiivissä. Keskeinen eroavaisuus näissä kahdessa säädöksessä on se, että tietosuojariskien arviointi on käsittelytoimikohtaista, kun taas NIS 2 -direktiivin mukainen riskien arviointi kohdistuu järjestelmien turvallisuuteen (eli arvioinnista nousevat riskit ovat kyberriskejä), jolloin arviointia voidaan tehdä sekä järjestelmäkohtaisesti että osana laajempaa organisaation kokonaisriskienhallintaa. Kansallisella tasolla tietosuojariskien arviointi näyttäytyy toteutustavoiltaan yhtenäisenä, sillä lainsäädännön ja ohjeistuksien välillä ei ole eroavaisuuksia. Järjestelmien kyberriskien hallinta on vastakohtaisesti hyvinkin kirjavaa ja epäjohdonmukaista nykyisessä tietoturvan sääntelyjärjestelmässä ja näyttäisi siltä, että NIS 2 -direktiivin implementoinnin jälkeenkään verkko- ja tietojärjestelmien kyberriskien hallinta ei ole tietoturvan sääntelyjärjestelmässä yhtenäistä. Toimialakohtaisesta lainsäädännöstä on ollut hyvin vaikeaa ja monimutkaista muodostaa selkeää kokonaiskuvaa organisaatioiden lainsäädännöllisestä tietoturvan sääntelyjärjestelmästä sekä hyvästä tietoturvatavasta liittyen nimenomaan tietoturvariskien hallintaan. Lisäksi siinä missä lainsäädäntö on kovin epäyhtenäistä tietoturvariskien hallinnan toteuttamistavoilta, myös organisaatioiden käytännön työssä on paljon vaihtelevuutta.

Edellä nostetut esimerkkitoimialat ovat NIS 2 -direktiivin liitteessä I määriteltyjä erittäin kriittisiä toimialoja. NIS 1 -täytäntöönpanosäännökset kumotaan

[1050] Ks. yksityiskohtaiset vaatimukset DORA-säädöksen 9 artiklan kohdasta 4.
[1051] DORA-säädöksen 11 artikla.

toimialakohtaisista laeista[1052]. Esimerkiksi aikaisemmin mainittu sähkömarkkinalain 29 a § ja 49 a §:n 5 momentti sekä maakaasumarkkinalain 34 a § katsotaan tarpeelliseksi kumota päällekkäisen sääntelyn välttämiseksi. Myös raideliikennelain 169 §, jolla on pantu täytäntöön NIS 1 -direktiivin velvoitteita, ehdotetaan kumottavaksi päällekkäisen sääntelyn välttämiseksi. Muilta osin raideliikennelaki säilynee ennallaan esimerkiksi riskienhallintaa ja turvallisuusjohtamisjärjestelmää koskevien vaatimuksien osalta. Huomioitava on myös se, että tulevaisuudessakin kaupunkiraideliikenteen toimijat eivät kuulu vieläkään NIS 2 -direktiivin soveltamisalaan. Lisäksi esimerkiksi sähkömarkkinalain 49 a §:n 4 momentin osalta jää voimaan NIS 1 -direktiivin mukaisia riskienhallintavelvoitteita.[1053]

Kaiken kaikkiaan NIS 2 -direktiivin implementointi tulee yhtenäistämään tietoturvan sääntelyjärjestelmää, koska kyberturvallisuuslain myötä kumotaan toimialakohtaista päällekkäistä sääntelyä. NIS 2 -direktiivin implementointi ei kuitenkaan täysin ratkaise hajanaisen sääntelyn ongelmaa, koska **ensinnäkin** tietoturvaan liittyviä vaatimuksia tulee silti olemaan toimialakohtaisesti. Toimialakohtaisten eroavaisuuksien, kuten toimialan omaavan kypsemmän riskienhallinta- ja turvallisuusilmapiirin[1054] takia, ei kaikesta toimialakohtaisesta sääntelystä varmaan ikinä haluta tai pystytä täysin luopumaan. Tärkeintä olisi kuitenkin välttää päällekkäistä sääntelyä useammassa eri säädöksessä, jotta tietoturvan sääntelyjärjestelmä olisi johdonmukainen ja helpommin tavoitettava. **Toiseksi** hajanaisen sääntelyn ongelma ei tule täysin ratkeamaan, koska kaikki toimijat eivät kuulu NIS 2 -direktiivin soveltamisen piiriin eikä kansallisella tasolla myöskään ole kaikkia toimijoita koskevaa tietoturvan yleislakia, jossa säädettäisiin kaikkia toimijoita velvoittavasta tietoturvan vähimmäistasosta ja hyvästä tietoturvatavasta. NIS 2 -direktiivin mukaiset kyberturvallisuuden riskienhallinnan vähimmäisvaatimukset eivät koske esimerkiksi pienempiä tai ”vähemmän tärkeitä” organisaatioita. Sääntelyn yhtenäistämiseksi sekä sääntelyjärjestelmän johdonmukaisuuden ja tavoitettavuuden lisäämiseksi tulisikin pyrkiä alakohtaisten eroavaisuuksien poistamiseen tai minimoimiseen ja luoda kaikkia toimijoita koskevat vähimmäisvaatimukset. Hajaantunut sääntely vaikeuttaa myös tietoturvasäännösten

[1052] Esityksessä ehdotetaan muutettavaksi sähköisen viestinnän palveluista annettua lakia, ilmailulakia, raideliikennelakia, liikenteen palveluista annettua lakia, alusliikennepalvelulakia, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettua lakia, sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annettua lakia, sähkömarkkinalakia, maakaasumarkkinalakia, sähkö- ja maakaasumarkkinoiden valvonnasta annettua lakia sekä Energiavirastosta annettua lakia. Ks. HE 57/2024 vp, s. 1, 61.

[1053] HE 57/2024 vp: 29, 237, 239.

[1054] Tässä yhteydessä kypsempään toimialakohtaiseen turvallisuusilmapiiriin vaikuttavat muun muassa lainsäädännön vaatimukset ja käytännön toimintakulttuuri. Esimerkiksi pankkialalla jo lainsäädännön turvallisuusvaatimukset ovat yksityiskohtaisemmat ja organisaatiokulttuuri on turvallisuuskeskeinen.

yhteensovittamista sekä tietoturvan sääntelyjärjestelmän proaktiivisuutta toimintaympäristön muutosten ja EU:n lakiuudistusten osalta. NIS 1 -direktiivin implementointi oli hyvä esimerkki sääntelystä, joka ei tähdännyt proaktiiviseen sääntelyyn vaan EU-direktiivin minimiharmonisointiin, vaikka pidemmällekin menevämpi sääntely olisi ollut mahdollista.

4.3.3 NIS 2 -direktiivi ja kyberturvallisuusriskien hallinta

Alkuperäinen NIS 1 -direktiivi oli varsin puutteellinen ja suppea verrattuna nykyiseen NIS 2 -direktiiviin, sillä esimerkiksi monia oleellisia toimialoja jätettiin NIS 1 -direktiivin riskienhallintavelvoitteiden ja poikkeamien ilmoittamisvastuiden ulkopuolelle. Mitä tulee hyviin käytänteisiin, kansallinen lainsäädäntö sekä NIS 1 -direktiivi eivät ole myöskään velvoittaneet sen yksityiskohtaisemmin, miten tietoturvariskien hallintaa tulisi toteuttaa käytännön tasolla. Esimerkiksi NIS 1 -direktiivin implementoinnin yhteydessä todettiin, että toimijalla jäi vapaus valita järjestelmiinsä, liiketoimintaansa ja muuhun riskienhallintaansa sopivimmat menetelmät tietoturvariskien hallitsemiseksi[1055]. Hyvien riskienhallintaan liittyvien käytänteiden mukaisesti riskienhallinnan tulisi olla muun muassa säännöllistä ja dokumentoitua, mitä toimialakohtaisessa lainsäädännössä ei ole velvoitettu kaikkien toimijoiden osalta. Huomioitava on kuitenkin, että sen sijaan EU:n yleisen tietosuoja-asetuksen vaatimuksissa on yksityiskohtaisemmin asetettu dokumentointivaatimuksia osoitusvelvollisuuden toteutumisen todistamiseksi sekä dokumentoitavasta tietosuojariskien arvioinnista. Näin ollen esimerkiksi henkilötietojen käsittelyä aloittaessa tulee arvioida riskejä luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyen ja dokumentoida tämä prosessi osoitusvelvollisuuden todistamiseksi[1056].

NIS 2 -direktiivin implementoinnin myötä riskienhallinnan toteuttamisen velvoitteisiin tulee huomattavia parannuksia. Esimerkiksi toimijalla tulisi olla kattava kyberturvallisuuden riskienhallinnan toimintamalli, jolla tunnistetaan, analysoidaan, arvioidaan ja käsitellään viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvia riskejä säännöllisesti. Riskienhallinnan tavoitteena tulisi olla riskien käsittely niin, että niiden todennäköinen vaikutus on minimoitu, poistettu tai ulkoistettu. Lisäksi jäännösriskit tulisi hyväksyä perustellusti. Riskienhallinnan tulisi olla myös jatkuvaa ja riskien hallinnan toimintaperiaatteiden olisi suositeltavaa perustua ajantasaisiin toimialalla omaksuttuihin käytänteisiin ja standardeihin. Tällaisia standardeja voisivat olla esimerkiksi ISO 31000:2018-riskienhallintastandardi, mutta huomioitava on myös ISO/IEC

[1055] HE 192/2017 vp: 59.
[1056] Ks. lisää luku 3.3.3 (”Henkilötietojen käsittelyn riskilähtöisyys ja riskiarviointi”).

27005:2018 tietoturvariskien hallinnan standardi sekä jatkuvaa, dokumentoitua tietoturvariskienhallintaa painottava ISO/IEC 27001:2022 tietoturvallisuuden hallintajärjestelmän standardi. Näin ollen onkin suoraan havaittavissa, että muutos riskienhallinnan toteuttamisen osalta on suuri ja edistyksellinen verrattuna NIS 1 -direktiiviin: siinä missä NIS 1 -direktiivin osalta toimijoille jäi vapaus valita sopivimmat menetelmät tietoturvariskien hallitsemiseksi[1057], nykyisessä tulkinnassa suosituksena on perustaa riskienhallinnan toimintaperiaatteet toimialalla omaksuttuihin hyviin käytänteisiin ja standardeihin.

> Kyberturvallisuuslain 9 §:ä koskevan kyberturvallisuuden riskienhallinnan toimintaperiaatteiden ja toimintamallin olisi suositeltavaa perustua ajantasaisiin toimialalla omaksuttuihin parhaisiin käytänteisiin ja standardeihin[1058]. Käytänteisiin tai standardeihin ei ole vastaavaa viittausta julkishallinnon riskienhallinnan osalta.

NIS 2 -direktiivissä on todettu, että vastuu verkko- ja tietojärjestelmän turvallisuuden varmistamisesta lankeaa suurelta osin kyseisessä direktiivissä määritellyille keskeisille ja tärkeille toimijoille, joiden tulisi edistää ja kehittää riskinhallintakulttuuria. Täten myös kyseisten toimijoiden hallintoelinten tulisi hyväksyä kyberturvallisuusriskien hallintatoimenpiteet ja valvottava niiden täytäntöönpanoa. Hallintoelinten velvollisuuteen kuuluu myös osallistua koulutukseen, jonka avulla on mahdollista hankkia riittävät tiedot ja taidot tunnistaakseen riskejä ja arvioimaan kyberturvallisuusriskien hallintakäytäntöjä sekä niiden vaikutusta.[1059] Verrattuna NIS 1 -direktiiviin, NIS 2 -direktiivi lisää kyberturvallisuusriskien hallintaan liittyvää vastuuta johdon suuntaan. Tämä puolestaan tulee sitouttamaan johtoa tulevaisuudessa vahvemmin tietoturvatyöhön, mikä on erinomainen kehityssuunta.

NIS 2 -direktiivissä on myös painotettu, että säädettyjä kyberturvallisuusriskien hallintatoimenpiteitä ja raportointivelvoitteita tulee soveltaa asiaankuuluviin keskeisiin ja tärkeisiin toimijoihin riippumatta siitä, hoitavatko kyseiset toimijat itse verkko- ja tietojärjestelmiensä ylläpidon vai onko ylläpito ulkoistettu. Keskeisiä ja tärkeitä toimijoita olisi erityisesti kannustettava sisällyttämään kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa.[1060] ”Kannustus” sopimusten osalta ei ole kuitenkaan suoraan toimijoita velvoittava toisin kuin tietosuoja-asetuksen sopimusvaatimukset henkilötietojen suojaamiseksi ovat. Esimerkiksi tietosuoja-asetuksen 28 artiklan 3 kohdassa vaaditaan sopimuksessa säädettäväksi, että

[1057] HE 192/2017 vp: 59.
[1058] HE 57/2024 vp: 162.
[1059] Direktiivin kohta 77 ja 137, myös 20 artikla.
[1060] NIS 2 -direktiivin kohta 83 ja 85.

henkilötietojen käsittelijä toteuttaa kaikki 32 artiklan tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi.[1061]

Sopimusjärjestelyiden ohella keskeisten ja tärkeiden toimijoiden tulisi arvioida ja ottaa huomioon toimittajiensa tuotteiden ja palveluntarjoajiensa palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet ja toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt.[1062] Vaikka NIS 2 -direktiivin vaatimukset eivät suoraan kohdistu muihin kuin kriittisiin toimialoihin, sen vaatimukset todennäköisesti heijastuvat keskeisten ja tärkeiden toimijoiden sopimuskumppaneihin eli mahdollisesti myös ei-kriittisiin toimialoihin. Tällöin käytännössä lain vaatimusten ja sopimusjärjestelyiden seurauksena keskeisten ja tärkeiden toimijoiden palveluntarjoajista tulisi rajautua tietoturvatasoltaan epäkypsät organisaatiot pois, jotta keskeiset ja tärkeät toimijat voivat noudattaa lain vaatimuksia. Nämä palveluntarjoajat saattavat myös yhtä lailla sijoittua näille ”vähemmän” tärkeille toimialoille. Tällainen lainsäädännön heijastava vaikutus tekee tietoturvan sääntelyjärjestelmästä ristiriitaisen vaikuttaen negatiivisesti myös sen kohtuullisuuteen ja oikeudenmukaisuuteen.

NIS 2 -direktiivin IV-luku keskittyy kyberturvallisuusriskien hallintatoimenpiteisiin ja raportointivelvoitteisiin. Aivan kuten alkuperäisessä NIS 1 -direktiivissä, myös NIS 2 -direktiivissä on painotettu asianmukaisia ja oikeasuhteisia toimenpiteitä riskien hallitsemiseksi. Erona on, että teknisten ja organisatoristen toimenpiteiden osalta NIS 2 -direktiivi nostaa ylös myös operatiiviset toimenpiteet niin kuin edellisessä pääluvussa tässä tutkimuksessa on käsitelty[1063].

Direktiivin artiklan 21 kyberturvallisuusriskien hallintatoimenpiteissä on koostettu kohdassa 2 vähimmäistoimenpiteitä, joihin on sisällytettävä a) riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat, b) poikkeamien käsittely c) toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta, d) toimitusketjun turvallisuus, e) verkko- ja

---

[1061] Ks. lisää sopimusvaatimuksista luvusta 3.3.2 (”Henkilötietojen käsittelyn ja tietoturvan huomioiminen sopimuksissa”).

[1062] NIS 2 -direktiivin kohta 83 ja 85. Saman tyyppinen vaatimus esiintyy myös tuoreen kyberturvallisuuslain 9 §:n 4 kohdassa, jossa kolmansien osapuolien osalta on todettu, että kyberturvallisuuden riskienhallinnan toimintamallissa ja hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt (HE 57/2024 vp: 278).

[1063] Ks. luku 3.4 (”Tietoturvan sääntelyjärjestelmän erilaiset tietoturvatoimenpiteet) sekä erityisesti luku 3.4.1 (”Tekniset ja organisatoriset toimenpiteet sekä operatiiviset toimenpiteet”).

tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen, f) toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta, g) perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus, h) toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä, i) henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta, sekä j) tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa. Tämä listaus vähimmäistoimenpiteistä on varsin kattava ja moniulotteinen verkko- ja tietojärjestelmien turvaamiseksi verrattuna NIS 1 -direktiiviin vaatimuksiin. Se myös kuvastaa suuntaa, jossa organisaatioiden tietoturvan sääntelyjärjestelmässä on yhä enemmän alettu huomioimaan hyvien käytänteiden mukaisia tietoturvan vähimmäisvaatimuksia.

Lopuksi todettakoon, että vaikka keskeisenä näkökulmana NIS 2 -direktiivin vaatimuksissa on järjestelmien kyberturvallisuuden parantaminen, vaatimukset tulevat parantamaan myös organisaatioiden kokonaisvaltaista tietoturvan kypsyystasoa lisäämällä muun muassa henkilöstön tietoisuutta sekä parantamalla riskien- ja jatkuvuudenhallinnan prosesseja, poikkeamien käsittelyä sekä dokumentointia. Näin ollen NIS 2 -direktiivin vaikutukset ovat paljon kauas kantoisemmat ensinnäkin direktiivin velvoittavuuden laajentumisen myötä, mutta toiseksi myös vaatimusten kattavuuden takia. Keskeinen muutos verrattuna NIS 1 -direktiiviin on esimerkiksi se, että NIS 2 -direktiivissä suosituksena on perustaa riskienhallinnan toimintaperiaatteet toimialalla omaksuttuihin hyviin käytänteisiin ja standardeihin[1064]. Toinen keskeinen positiivinen asia on se, että NIS 2 -direktiivi lisää kyberturvallisuusriskien hallintaan liittyvää johdon vastuuta, mikä myös osaltaan tulee sitouttamaan johtoa enemmän tietoturvatyöhön. Kolmantena korostamisen arvoisena, edistyksellisenä seikkana vaatimusten kattavuuden osalta on toimitusketjuriskien huomioiminen, sillä niiden kriittisyys on noussut viime vuosina jatkuvasti: rikolliset voivat yrittää päästä huomaamattomasti organisaatioiden tietoihin ja järjestelmiin kiinni alihankintaketjujen ja kolmansien osapuolien palvelujen kautta. NIS 2 -direktiivi kannustaa täten sisällyttämään paremmin kyberturvallisuusriskien hallintatoimenpiteitä myös sopimusjärjestelyihin. Lisäksi NIS 2 -direktiivi velvoittaa keskeisiä ja tärkeitä toimijoita arvioimaan toimittajiensa ja palveluntarjoajiensa tuotteiden ja palveluiden kyberturvallisuusriskien hallintatoimenpiteitä ja kyberturvallisuuskäytäntöjä. Vaikka NIS 2 -direktiivin vaatimukset ulottuvat suoraan kriittisiin toimialoihin, vaatimuksilla voi olla myös epäsuoria vaikutuksia muihin toimialoihin ja toimijoihin. Yksilöiden oikeuksien toteutumisen sekä yhteiskunnan toimivuuden osalta kybertoimintaympäristössä tämä

[1064] Vrt. NIS 1 -direktiivissä toimijoille jäi vapaus valita sopivimmat menetelmät tietoturvariskien hallitsemiseksi.

lainsäädännöllinen kehitys tulee olemaan merkityksellistä, mutta samanaikaisesti organisaatioiden tietoturvan sääntelyjärjestelmä ilmentää ”vähemmän tärkeiden” toimijoiden osalta vaikeasti tavoitettavaa ja ymmärrettävää sääntelyä, joka on siten myös kohtuutonta ja epäoikeudenmukaista.

4.3.4 Fyysinen tietoturvallisuus osana riskienhallintaa

NIS 2 -direktiivin tekniset, operatiiviset ja organisatoriset toimenpiteet on perustuttava 21 artiklan mukaisesti kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan sekä verkko- ja tietojärjestelmät että näiden järjestelmien fyysinen ympäristö poikkeamilta. NIS 2 -direktiivi ei täten sisällä ainoastaan kyberturvallisuusvaatimuksia järjestelmille, vaan vaatimukset ulottuvat myös fyysisen tietoturvallisuuden osa-alueelle. Fyysiset tietoturvatoimenpiteet ovat olennainen osa kyberturvallisuuden parantamista eli esimerkiksi järjestelmien ja laitteiden suojaamista, vaikka toki fyysisellä tietoturvalla pyritään suojaamaan myös muun muassa paperisia dokumentteja ja arkistoja.

Fyysisen ympäristön poikkeamia voivat olla esimerkiksi varkaus, tulipalo, tulva, televiestintä- tai sähkökatko sekä luvaton fyysinen pääsy tietoihin tai tietojenkäsittely-ympäristöön. Toimenpiteiden tulisi olla eurooppalaisten tai kansainvälisten standardien, kuten ISO / IEC 27000-sarjan standardien, mukaisia.[1065]

Käytännön tasolla fyysiseen tietoturvallisuuteen kuuluu rakennuksen tilojen sekä niihin sijoitettujen laitteiden suojaaminen fyysisiltä uhkilta, esimerkiksi vesi- ja palovahingoilta, sähkö- ja lämmitysjärjestelmien häiriöiltä sekä ihmisten aiheuttamalta ilkivallalta tai murroilta[1066]. Katakrin vaatimuksien mukaan fyysiset turvatoimet tulisi toteuttaa monitasoisen suojaamisen periaatteen mukaan eli turvatoimilla, jotka täydentävät toisiaan. Parhaimmassa suunnittelussa tilat muodostaisivat kehäsuojauksen mukaisesti sisäkkäisiä vyöhykkeitä, jolloin korkeimman suojaustason vaativat tilat olisivat sisimpinä ja mahdolliset julkiset tilat lähellä rakennuksen ulkokuorta. Rakennuksen ulkokuoressa tulisi käyttää turvallisuutta parantavia rakenteellisia ratkaisuja, joita täydentävät turvallisuustekniset ratkaisut. Kulku rakennuksen sisään sekä vyöhykkeiden sisällä tulisi olla valvottua ja hallittua kulunvalvontajärjestelmällä. Lisäksi olisi hyvä käyttää riittävää turvatoimien yhdistelmää, kuten esimerkiksi kameravalvontaa, murtohälytysjärjestelmää, koulutettua turvallisuushenkilöstöä (vartijoita), turvavalaistusta sekä muita fyysisiä esteitä. Turvaratkaisujen käytön tulisi perustua riskiarviointiin. Työntekijät olisi oltava mahdollisuuksien mukaan helppo tunnistaa, esimerkiksi kuvallisen

[1065] NIS 2 -direktiivin kohta 79.
[1066] Hakala, Vainio & Vuorinen 2006: 11.

henkilökortin avulla. Vierailijoilla tulisi olla vierailijakortti sekä saattaja tai mahdollisesti pääsy kokonaan kielletty tiettyihin korkeamman turvallisuustason tiloihin. Näin ollen pääsy alueille ja tietoihin olisi rajattu tiedonsaantitarpeen mukaan ja kulkuoikeuksia hallinnoitaisiin sekä avaimia ja avaintunnisteita valvottaisiin. Salakatselua ja -kuuntelua vastaan olisi myös suojauduttu ja työpisteillä olisi ohjeistettu ja jalkautettu puhtaan pöydän -periaate.[1067]

Nykyisessä, voimassa olevassa kansallisessa lainsäädännössä on huomioitu tiettyjä fyysisen tietoturvallisuuden kontrolleja lähinnä tietosuojan näkökulmasta, kuten esimerkiksi kameravalvonnan vaatimukset työelämän tietosuojalaissa[1068]. Lisäksi esimerkiksi viranomaisia koskee tiedonhallintalain 15 §:n mukainen toimitilaturvallisuuden vaatimus. Kyseisen lain kohdan mukaan tietoaineistoja on käsiteltävä ja säilytettävä riittävän turvallisissa toimitiloissa tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi. Lisäksi viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein tietoaineistojen suojaaminen fyysisiltä vahingoilta[1069]. Se, onko jokin toimitila riittävän turvallinen tai tietoturvatoimenpiteet tarpeellisia, vaatii riskien arviointia.

Fyysistä tietoturvallisuutta on huomioitu myös vaihtelevasti muussa toimialakohtaisessa lainsäädännössä. Esimerkiksi alkuperäisen NIS 1 -direktiivin 16 artiklan mukaan digitaalisen palvelun tarjoajien oli turvallisuustoimenpiteiden osalta otettava huomioon järjestelmien ja tilojen turvallisuus. Kun NIS 1 -direktiivi implementoitiin sähköisen viestinnän palveluista annettuun lakiin, myös tilaturvallisuus otettiin huomioon direktiivin mukaisesti. Kyseisen lain 247 a §:n mukaan digitaalisen palvelun tarjoajien on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta, jossa on huomioitava muun muassa järjestelmä- ja tilaturvallisuus. NIS 1 -direktiivin täytäntöönpanoon liittyen tämän pykälän osalta ei kuitenkaan otettu yksityiskohtaisemmin kantaa tilojen turvallisuuteen, mutta todettiin, että fyysinen ja digitaalinen turvallisuus kietoutuvatkin yhä läheisemmin yhteen[1070]. Huomioitava on se, että edellä mainittu lakipykälä tilaturvallisuuden osalta rajautuu lähinnä digitaalisen palvelun tarjoajiin. Lisäksi kyseinen 247 a § kumotaan NIS 2 -direktiivin implementoivan kyberturvallisuuslain myötä[1071].

[1067] Ks. Katakri 2015 ja 2020 F-osion vaatimukset.
[1068] Ks. lisää luku 3.5.2 (”Kameravalvonta”).
[1069] Tiedonhallintalain 15 §, kohta 2. Ks. myös Valtiovarainministeriön suositus tietoturvallisuuden vähimmäisvaatimuksista, jossa on suositeltu toimitilaturvallisuuden varmistamiseksi toteutettavan ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä turvallisuutta vaarantavien tekojen ennalta ehkäisemiseksi, havaitsemiseksi, jäljittämiseksi sekä turvallisuustason palauttamiseksi. Suosituksena on myös hyödyntää Julkri-kriteeristöä fyysisen turvallisuusvaatimusten suhteen. (Valtiovarainministeriön julkaisuja 2024:19, s. 28)
[1070] HE 192/2017 vp: 6.
[1071] HE 57/2024 vp: 346.

Voimassa olevaa hajaantunutta sääntelyä kuvastaa hyvin myös sähkömarkkinalain 49 a §:n 4 momentti, jossa tilojen turvallisuus on otettu samalla tavalla huomioon kuin sähköisen viestinnän palveluista annetussa laissa: järjestelmävastaavan kantaverkonhaltijan on huolehdittava sähkökaupan keskitetyn tiedonvaihdon palvelujen tuottamisessa käyttämiinsä tietojärjestelmiin kohdistuvasta riskien hallinnasta sekä huomioitava riskienhallinnassa muun muassa järjestelmien ja tilojen turvallisuus. NIS 2 -direktiivin implementointia koskevan HE 57/2024 mukaan sähkömarkkinalain 49 a §:stä kumotaan ainoastaan Energiaviraston määräyksenantovaltuutta koskeva 5 momentti, jolloin 4 momentti jäisi voimaan sellaisenaan[1072]. Tämä tarkoittaa sitä, että 4 momentin riskienhallinnan velvoitteet järjestelmien ja tilojen turvallisuudesta, tietoturvauhkien ja häiriöiden käsittelystä sekä jatkuvuudenhallinnasta jäävät voimaan sellaisenaan, mikä lisää päällekkäistä, hajaantunutta sääntelyä entisestään NIS 2 -direktiivin implementoinnin myötä.

Pääosin direktiivin toimijoita koskevat velvoitteet implementoidaan osana yleislakina toimivaa kyberturvallisuuslakia. Julkishallintoa koskevat velvoitteet sen sijaan saatetaan osaksi tiedonhallintalakia. Tämä on sinänsä erikoista, koska tavoitteena on alun perin ollut päällekkäisen sääntelyn ehkäiseminen kumoamalla NIS 1 -direktiivin myötä tulleet toimialakohtaiset säännökset. Nyt kuitenkin näyttäisi siltä, että NIS 2 -direktiivi parantaa fyysisen tietoturvallisuuden osa-alueen huomioimista jopa niin hyvin, että täsmälleen samat asiat fyysisen ympäristön huomioimisesta tullaan implementoimaan kansallisella tasolla kahteen kertaan eri säädöksiin. Kyberturvallisuuslain 8 § ja 9§ sekä julkishallintoa koskevan tiedonhallintalain 18 b § ja 18 c § edellyttävät samoja asioita: toimijan tulisi laatia kyberturvallisuuden riskienhallinnan toimintamalli, jossa tulisi tunnistaa viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvat riskit kaikki vaaratekijät huomioivan lähestymistavan mukaisesti. Lisäksi kyberturvallisuuden riskienhallinnan toimenpiteet tulisi sisältää muun muassa toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.[1073] Sääntely tulee olemaan edelleenkin hajanaista tietoturvavelvoitteiden osalta, mikä on huomattavissa erityisen selkeästi fyysisen tietoturvallisuuden vaatimuksista niiden hajaantuessa useaan eri säädökseen.

Kyseiset fyysisen tietoturvallisuuden ja toimitilaturvallisuuden vaatimukset ovat kuitenkin tarpeellisia, sillä aikaisemmin lainsäädännössä ei ole huomioitu tietoturvallisuuden kaikista ulottuvuuksista fyysistä tietoturvaa kovin hyvin. Yhteiskunta ja teknologia kuitenkin muuttuvat, jolloin myös lainsäädännön vaatimuksien tulisi vastata tähän muutokseen. Digitalisaation ja teknologian kehittymisen

[1072] HE 57/2024 vp: 367.
[1073] HE 57/2024 vp: 277–278, 301–302.

myötä työelämässä on tapahtunut muutoksia, joiden myötä erityisesti niin sanottua tietotyötä on mahdollista tehdä entistä enemmän erilaisissa ympäristöissä. Nykyiset fyysisen tietoturvallisuuden vaatimukset eivät huomioi riittävällä tasolla nykyajan työskentelymuotoja eli etätyötä, hybridityöskentelyä tai monipaikkaista työskentelyä[1074]. Riskitaso esimerkiksi luottamuksellisen tiedon vuotamiselle on täysin erilainen työskennellessä organisaation lukituissa, kamera- ja kulunvalvonnalla suojatuissa tiloissa kuin työskennellessä kahvilassa, junassa taikka yhteisöllisissä co-working-tiloissa.

Huomioitava on myös mobiililaitteet, joiden avulla työskentely ja organisaation tietoaineistoihin käsiksi pääseminen on teknologian kehittymisen myötä helppoa ja nopeaa. Lisäksi nämä mobiililaitteet saattavat kulkea viikonloppuisinkin työntekijän vapaa-ajan riennoissa mukana, mikä lisää tietovuotojen riskiä erityisesti silloin, jos laite katoaa.

Lainsäädännössä ilmenevät fyysiset suojaustoimenpiteet kohdistuvat lähinnä organisaatioiden toimitiloissa oleviin järjestelmiin tai tietoaineistoihin. Esimerkiksi tiedonhallintalain 15 §:n mukaan tietoaineistoja on käsiteltävä ja säilytettävä riittävän turvallisissa toimitiloissa. Entäpä sitten kun tietoaineistoja käsitellään junassa tai kannettavaa tietokonetta säilytetään kauppareissun ajan autossa? Taikka kun tietoaineistoja käsitellään ja säilytetään kodissa, jossa ovet ovat auki takapihalle aina kesällä tai samassa kodissa asuu kotibileitä järjestäviä teinejä? Yhtä lailla nykyiset toimitilaturvallisuuden sekä jatkuvuudenhallinnan käytännön ohjeet ovat kritisoitavissa tästä modernien työskentelytapojen huomioimisen puutteesta. Esimerkiksi usein suosituksissa ja ohjeissa viitataan vuoden 2013 VAHTI:n toimitilojen tietoturvaohjeeseen, joka on varsin vanhentunut modernien työskentelytapojen näkökulmasta[1075]. Huomioitava kuitenkin on, että tuoreessa valtiovarainministeriön suosituksessa tietoturvallisuuden vähimmäisvaatimuksista modernien työskentelytapojen osalta on todettu tiedonhallintalain 15 §:ä täydentävänä suosituksena, että toimitilaturvallisuuden suunnittelussa olisi hyvä määritellä, ohjeistaa ja kouluttaa henkilöstöä, millä edellytyksillä eri tietoaineistoja voi käsitellä ja säilyttää etätöissä tai yhteiskäyttöisissä toimitiloissa[1076]. Tämä on selkeä parannus julkisen hallinnon tietoturvallisuuden vähimmäisvaatimuksissa modernien työskentelytapojen suhteen sekä hyvä esimerkki siitä, kuinka säännöstä voidaan täsmentää vielä soft law -tyyppisellä käytännesäännöllä.

[1074] Monipaikkaisella työskentelyllä tarkoitetaan tässä kohtaa kodin ja päätoimipisteen lisäksi vaihtoehtoisia työskentelypaikkoja, kuten toiset toimipisteet ja co-working-tilat, kahvilat, kirjastot, liikennevälineet sekä muu matkoilla tapahtuva työskentely esimerkiksi hotellissa.
[1075] Valtiovarainministeriön julkaisuja 2023:41: 24–25, 47.
[1076] Valtiovarainministeriön julkaisuja 2024:19: 28.

Teknologian kehittymisen myötä moderni työskentely on tullut jäädäkseen ja lainsäädännön tasolla tämäkin tulisi huomioida paremmin kaikkien organisaatioiden osalta. Organisaatioita tulisi vastuuttaa lainsäädännössä kattavammin ja proaktiivisemmin huomioimaan tiedon suojaaminen myös modernien työskentelytapojen osalta hallinnollisin, teknisin ja fyysisin tietoturvatoimenpitein. Käytännössä tällaisia toimenpiteitä ovat esimerkiksi työntekijöiden kouluttaminen ja ohjeistus sekä salakatselun ja -kuuntelun ehkäiseminen tarjoamalla työntekijöille näytönsuojia sekä kuulokkeet palavereja varten. Työnantajan velvollisuuksiin kuuluu varmistaa, että työolosuhteet ja tietoturva ovat kunnossa[1077]. Mikäli hallinnolliset, fyysiset ja tekniset suojakeinot eivät riitä tai toteudu sekä työntekijöiden osaaminen on alhaisella tasolla puutteellisten ohjeistuksien tai koulutuksien takia, organisaation pitäisi olla tästä vastuussa. Toki holtittomasta organisaation tietoaineistojen käsittelystä organisaation toimitilojen ulkopuolella tulee olla myös vastuu työntekijällä itsellään. Hyvä tietoturvan sääntelyjärjestelmä tulisi huomioida organisaatioiden ohella yksilöt tietoturvan toteuttajana ollakseen hyvä.

Tällä hetkellä tällainen työntekijöiden vastuuttaminen ulottuu esimerkiksi henkilötietojen suojaamiseen rikoslain 38 luvun 9 §:n mukaisen tietosuojarikoksen puitteissa, jolloin tietosuojarikoksesta voidaan tuomita se, joka tahallaan tai törkeästä huolimattomuudesta toimii vastoin tietosuojalainsäädännössä säädettyjä vaatimuksia henkilötietojen käsittelyn turvallisuudesta. Myös viranomaistoiminnan osalta tulee esimerkiksi huomioida rikoslain 40 luvun 5 §, jonka mukaan virkamiehiä voidaan tuomita tahallisesta tai huolimattomuuden takia johtuneesta virkasalaisuuden rikkomisesta. Virkasalaisuuden rikkominen ulottuu virkamiehen lisäksi rikoslain 40 luvun 12 §:n mukaisesti julkista luottamustehtävää hoitavaan henkilöön, julkista valtaa käyttävään henkilöön, julkisyhteisön työntekijään, tiettyihin ulkomaalaisiin virkamiehiin sekä niihin, joihin on muissa säädöksissä ulotettu koskemaan rikosoikeudellista virkavastuuta[1078]. Näin ollen edellä mainittujen säännöksien puitteissa vakavista tietoturvallisuuden laiminlyönneistä etätyössä, hybridityössä sekä monipaikkaisessa työssä on mahdollista langettaa seuraamuksia työntekijöille esimerkiksi tietosuojarikoksen sekä virkasalaisuuden rikkomisen puitteissa.

Täten onkin oleellista, että organisaatioilla olisi esimerkiksi monipaikkaisen työskentelyn osalta dokumentoituja sääntöjä, ohjeistuksia ja koulutuksia, jotta työntekijän tahallinen tai törkeästä huolimattomuudesta aiheutuva ohjeiden vastainen toiminta olisi helpompi todistaa. Myös tietoturvavastuiden ja

[1077] Etätyötä tehdään usein kotona tai muuten sellaisissa olosuhteissa, joiden turvallisuutta työnantajan on vaikea selvittää ja arvioida. Tietoturvallisuuden lisäksi sama koskee työterveyttä ja työturvallisuutta. Ks. EOAK 4542/2021, s. 4.
[1078] Viljanen 2023b: 943.

salassapitoklausaalien ulottaminen työ- ja toimeksiantosopimuksiin on tärkeää.[1079] Muuten työntekijä voisi vedota tietämättömyyteen tai osaamattomuuteen. Täten tulemme jälleen takaisin siihen seikkaan, miksi organisaatioita tulisi vastuuttaa lainsäädännössä huomioimaan tiedon suojaamisen riskit sekä toteuttamaan tietoturvatoimenpiteitä modernien työskentelytapojen osalta. Puutteet tällaisten toimenpiteiden osalta vaarantavat organisaation tietoturvan tasoa, ja sen myötä luottamuksellisten tietojen suojaa sekä yksilöiden perusoikeuksia.

4.4 Järjestelmien oikeudellisen suunnittelun vaatimukset sääntelyjärjestelmässä

4.4.1 Järjestelmien elinkaarimalli osana oikeudellista suunnittelua

Vaikkakin alkuperäistä NIS 1 -direktiiviä tituleerattiin ensimmäiseksi yleiseurooppalaiseksi kyberturvallisuutta käsitteleväksi oikeudelliseksi säädökseksi, jonka tarkoituksena oli lisätä verkko- ja tietojärjestelmien turvallisuutta, sen toimialakohtaiset järjestelmien tietoturvavelvoitteet kohdistuivat jo olemassa oleviin järjestelmiin. Näin ollen se ei niinkään ottanut kantaa tietojärjestelmien ja -palveluiden koko elinkaaren aikana huomioitaviin tietoturvavaatimuksiin. NIS 2 -direktiivissä elinkaariajattelu on otettu paremmin huomioon. Sen 21 artiklan kyberturvallisuusriskien hallintatoimenpiteiden yhtenä vähimmäisvaatimuksena on verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus (kohta 2e) eli kyseisen kohdan mukaan turvallisuus on otettava huomioon jo järjestelmien hankintavaiheessa eli elinkaaren alkupäässä.

Monesti järjestelmissä vahingon torjunta on halvempaa kuin vahingon korjaaminen. Lisäksi vahingon korjaaminen on haastavaa, sillä luottamuksen jälleenrakentaminen vie aikaa.[1080] Useasti esimerkiksi järjestelmien ja ohjelmistojen turvallisuuspuutteita korjataan osana ylläpitoa, versiopäivityksiä ja tuotteiden uusia julkaisuja. Tietoturvallisuus tulisikin huomioida jo järjestelmien, ohjelmistojen sekä muiden palveluiden elinkaaren alkupäästä alkaen, sillä jatkuvat korjauspäivitykset tai luottaminen turvaohjelmistoihin, kuten palomuureihin, ei ole riittävää.[1081] Näin ollen esimerkiksi jo järjestelmän tai palvelun hankintavaiheessa tulisi hankinnan tietoturvavaatimuksissa ottaa huomioon vaatimusten täyttyminen niiden

[1079] Ks. yksityiskohtaisemmin tästä aiheesta luvusta 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).
[1080] Andreasson, Koivisto & Ylipartanen 2013: 20.
[1081] Råman 2006b: 82–83, 411. Råman on myös kritisoinut (s. 67–69) ohjelmistosuunnittelun osalta sitä, että tietoturvaominaisuuksia helposti lisätään vasta jälkikäteen.

koko elinkaaren ajan[1082]. Yhtä lailla toimittajien tulisi olla vastuullisia ja huomioida turvallisuus tuotteensa elinkaaren jokaisessa vaiheessa (sisäänrakennettu turvallisuus, *”security-by-design”*) sekä varmistaa tuotteidensa ja palveluidensa perusturvallisuus (oletusarvioinen turvallisuus, *”security-by-default”*) siirtämättä sitä käyttäjien vastuulle[1083]. Sisäänrakennettu ja oletusarvoinen turvallisuus ovat ennakkoedellytys käyttäjien luottamukselle[1084].

Järjestelmien, ohjelmistojen ja palveluiden suunnitteluvaiheessa tulisi kiinnittää huomiota teknisten seikkojen lisäksi oikeudelliseen suunnitteluun, mikä on nykymuotoisen oikeusvaltiomme lähtökohta. Tämä ei tulisi unohtua keskittyessä suunnittelussa tehokkuuden kehittämiseen. Oikeudellinen suunnittelu tarkoittaa esimerkiksi järjestelmäsuunnittelussa yksilön perusoikeuksien suojaamista tietojärjestelmissä ja -verkoissa. Oikeudellinen suunnittelu sisältää muun muassa voimassa olevan lainsäädännön velvoitteiden tunnistamisen lisäksi uusien ja kehitteillä olevien lakiuudistusten selvittämisen sekä niiden vaikutusten arvioimisen, joiden pohjalta tietojärjestelmä rakennetaan lain mukaiseksi. Mikäli tietojärjestelmä tai -palvelu osoittautuisi lain vastaiseksi tai muuten oikeudellisesti puutteelliseksi, aiheutuu organisaatiolle ylimääräisiä kustannuksia. Todellisuudessa kuitenkin tietojärjestelmien ja -palveluiden suunnittelun edellytykset ja oikeudelliset näkökohdat tulevat huomioon vasta oikeudellisten ongelmien jo ilmetessä, esimerkiksi yhden tai useamman yksilön oikeuksien tultua loukatuiksi.[1085]

Tietojärjestelmäturvallisuuden osa-alueeseen kuuluu sekä ohjelmistoturvallisuus että laitteistoturvallisuus. *Ohjelmistoturvallisuus* sisältää muun muassa käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, pääsynvalvonta-, varmistus-, tarkkailu- ja eristämistoimet, lokimenettelyt, laadunvarmistamisen sekä ohjelmistojen ylläpito- ja päivitystoimet.[1086]

[1082] Valtiovarainministeriön julkaisuja 2023:57: 16, 20.
[1083] Esimerkiksi ***security-by-design*** sisältäisi digitaalisen turvallisuuden vähimmäistason ml. pääsynhallinnan menetelmät, haavoittuvuuksien hallinnan, tietosuojan huomioimisen sekä riskiperusteiset turvallisuusvaatimukset. ***Security-by-default***-vaatimuksen osalta olennaista on, että toimittaja määrittelisi perusominaisuutena riittävällä tasolla kovennetut oletuskonfiguraatiot ja -turvallisuusominaisuudet, jotka käyttäjä saisi halutessaan pois (mieluummin opt-out, kuin opt-in). Ks. OECD 2022, *Recommendation of the Council on the Digital Security of Products and Services,* OECD/LEGAL/0481, s. 8–9. Kyberturvallisuus ja yksityisyydensuoja tulisivat olla olennaisia vaatimuksia tuoteinnovoinnissa sekä tuotanto- ja kehitysprosesseissa, myös suunnitteluvaiheessa, ja ne olisi varmistettava tuotteen koko elinkaaren ja toimitusketjun ajan. Ks. Euroopan unionin neuvosto, Neuvoston päätelmät internetiin yhdistettyjen laitteiden kyberturvallisuudesta 2.12.2020, s. 3.
[1084] Euroopan unionin neuvosto, Euroopan digitaalisen tulevaisuuden rakentaminen - Neuvoston päätelmät 9.6.2020: 11.
[1085] Saarenpää 2016a: 96, 113–114, 119; Magnusson Sjöberg 1992: 479–480; Tornberg 2016: 299.
[1086] VAHTI 5/2004: 67.

Laitteistoturvallisuuteen puolestaan kuuluu tietokoneiden sekä muiden tietojärjestelmään kytkettyjen laitteiden mitoitus, testaus, huollot, laitteiden vanhentumiseen varautuminen sekä laitteiden käyttöturvallisuuden vaaratekijöiden minimointi[1087]. Tällä hetkellä kansallinen toimialakohtainen lainsäädäntö asettaa hajanaisesti velvoitteita verkko- ja tietojärjestelmäturvallisuuden elinkaaren osalta. Esimerkiksi sähköisen viestinnän palveluista annetun lain osalta huomioitava on kyseisen lain 243 §:n suunnitteluvelvoite tietoturvan osalta, jonka mukaan yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on *suunniteltava, rakennettava ja ylläpidettävä* taaten sähköisen viestinnän tietoturvallisuus. Tähän lisäten viestintäverkkojen ja -palveluiden tulisi kestää tietoturvauhat, ne eivät saisi aiheuttaa tietoturvauhkia ja niiden tulisi havaita niihin kohdistuvat merkittävät tietoturvauhat ja -loukkaukset. Lisäksi viestintäverkkojen ja -palveluiden tulee taata, ettei kenenkään tietoturva, tietosuoja tai muut oikeudet vaarannu. Näiden vaatimusten toteutuminen edellyttää toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, tietoaineistoturvallisuuden sekä laitteistoja ohjelmistoturvallisuuden varmistamiseksi. Lain mukaan toimenpiteet on suhteutettava huomioon ottaen uhan vakavuus, kustannukset sekä käytettävissä olevat tekniset mahdollisuudet torjua uhka. Jatkuvuuden osalta on myös säädetty lain 243 §:n kohdassa 14 niin, että viestintäverkkojen ja -palveluiden on toimittava mahdollisimman luotettavasti normaaliolojen häiriötilanteissa ja valmiuslaissa tarkoitetussa poikkeusoloissa. Näin muotoiltuna järjestelmien suunnitteluvaiheen tietoturva on otettu huomioon mahdollisimman teknologianeutraalisti kuitenkaan ottamatta kantaa spesifeihin, teknisiin toteuttamisvaatimuksiin.

Elinkaarimalliajattelua on huomioitu myös viranomaisia koskevassa lainsäädännössä. Esimerkiksi tiedonhallintalain 13 § mukaan tiedonhallintayksikön on varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Samoin tukipalvelulaissa on asetettu vaatimuksia tukipalvelujen elinkaaren suhteen: palveluntuottaja vastaa siitä, että sen tuottama tukipalvelu on suunniteltu, rakennettu ja ylläpidetty muun muassa siten, että palvelu on tekniseltä laadultaan hyvää ja tietoturvallista[1088].

Huomioitava on myös viranomaisia koskevan digipalvelulain (306/2019) 4 §, jonka mukaan viranomaisen on suunniteltava ja ylläpidettävä digitaaliset palvelunsa siten, että niiden tietoturvallisuus, tietosuoja, löydettävyys ja helppokäyttöisyys on varmistettu. Digipalvelulaissa ei ole kuitenkaan säädetty palvelun

[1087] Hakala, Vainio & Vuorinen 2006: 12.
[1088] Hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetussa lain (571/2016) 16 §.
Tällaisia tukipalvelulain mukaisia palveluita ovat tunnistuspalvelu, asiointivaltuuspalvelu, verkkomaksamisen kokoamis- ja hallinnointipalvelu sekä viestinvälityspalvelu. Ks. HE 63/2022 vp, s. 16.

suunnitteluvaiheessa huomioitavista tietoturvavaatimuksista, koska vaatimuksien oletetaan muuttuvan toimintaympäristön muutoksen ja teknisen kehityksen myötä. Tietoturvatoimenpiteiden riittävyys on pystyttävä toteennäyttämään tietoturvallisuutta koskevalla suunnitteludokumentaatiolla ja testausraporteilla, mikä on rinnastettavissa EU:n tietosuoja-asetuksen osoitusvelvollisuuteen.[1089] Tämän suunnitteluvaiheen sääntelemättömyyden taustalla on myös teknologianneutraalisuuden periaate. Kuitenkin vastakohtaisesti esimerkiksi NIS 2 -direktiivissä on todettu kohdassa 85 varsin teknologianeutraalisti, että keskeisiä ja tärkeitä toimijoita olisi erityisesti kannustettava sisällyttämään kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita ne tekevät välittömien toimittajiensa ja palveluntarjoajiensa kanssa. Lisäksi toimijoiden olisi otettava huomioon toimittajiensa tuotteiden ja palveluntarjoajiensa palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet ja toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt[1090]. Kyseinen NIS 2 -direktiivin vaatimus tulee lisäämään hankintavaiheen tietoturvavaatimuksia tulevaisuudessa, mutta myös mahdollisesti päivittämään nykyisiä tietoturvavaatimuksia sopimuksissa. Tällaiset toimenpiteet parantavat palveluiden tietoturvasuunnittelua jo hankinnan elinkaaren alkupäästä ja kuvastavat hyvin kattavampaa suunnitteluvaiheen teknologianeutraalia sääntelyä kuin mitä digipalvelulaissa on toteutettu.

Keskeinen järjestelmien elinkaaren tietoturvavaatimuksia parantava laki on tietosuoja-asetus. Tietosuoja-asetus asettaa vaatimuksia järjestelmien ja palveluiden turvallisuuden osalta jo näiden suunnitteluvaiheesta alkaen henkilötietojen suojaamiseksi. Tämä velvoite koskee kaikkia organisaatioita ja korostaa jälleen sitä, kuinka erinomaisesti tietosuojasääntelyn myötä on tullut hyviä ja relevantteja tietoturvavaatimuksia.

Henkilötietojen suojaamiseen liittyy periaate ”*Privacy by Design and Default*” eli tietojen käsittely tulisi perustua sisäänrakennettuun ja oletusarvoiseen tietosuojaan, jonka pohjana on ennakollinen, riskiperusteinen suunnittelu sekä sen myötä tehtävät tietosuojan takaavat toimenpiteet. Tietosuoja-asetuksen mukaiset tekniset ja organisatoriset toimenpiteet on tällöin toteutettava koko tiedon ja sen tallennusalustan elinkaaren ajan. Esimerkiksi tiedot on tuhottava säilytysajan päättymisen jälkeen ja tuhoaminen on tehtävä tietoturvallisesti.[1091] Aivan kuten Ahti Saarenpää kuvaa *tiedon tietä*: järjestelmien suunnittelussa tulee huomioida koko tiedon tie sen elinkaaren ajalta[1092]. Tietosuoja-asetuksen 25 artiklan tarkoituksena

[1089] HE 60/2018 vp: 62–63.
[1090] Ks. myös NIS 2 -direktiivin 21 artiklan kohta 2d ja 3.
[1091] Voutilainen 2019: 66, 194.
[1092] Saarenpää 2018: 26.

on varmistaa asianmukainen ja tehokas tietosuoja, joka on sekä sisäänrakennettu että oletusarvoinen koko henkilötietojen käsittelyn elinkaaren ajalta[1093].

Järjestelmän oikeasuhteisia suojatoimia suunniteltaessa ja toteuttaessa tulee ottaa huomioon henkilötietojen laatu eli minkälaista henkilötietoa järjestelmässä tulee olemaan, sekä henkilötietojen käsittelyn laajuus ja tarkoitukset. Esimerkiksi palvelun suunnittelu- ja kehitysvaiheessa varsinaisten tuotantopalvelinten lisäksi kehitystyössä käytetään usein testi- ja demotietokantoja, joissa kannattaa käyttää kuvitteellisia henkilötietoja oikeiden sijaan[1094]. Sisäänrakennetun tietosuojan vaatimukset sekä tietosuojan vaatimustenmukaisuutta koskevat arvioinnit tulisi sisällyttää osaksi tuotteiden ja palveluiden kehittämisprosesseja[1095]. Kirjoitan tässä tarkoituksella vaatimuksenmukaisuudesta enkä vaikutustenarvioinnista, sillä rekisterinpitäjän tulee lain mukaan tehdä tiettyjen kriteerien täyttyessä tietosuojan vaikutustenarviointi (*DPIA – Data Protection Impact Assessment*) ja tässä arvioinnissa keskitytään nimenomaan henkilötietojen käsittelyn vaikutuksiin rekisteröityjen oikeuksien ja vapauksien kannalta[1096]. Palveluntarjoajaorganisaation ei välttämättä tarvitse tehdä itse DPIA:a, mikäli he eivät käytä palvelua omassa toiminnassaan eli palveluntarjoajaorganisaatio ei ole rekisterinpitäjänä. Näin ollen osana palvelun kehittämistä olisi parempi tehdä sellainen tietosuoja-arviointi, jossa keskitytään enemmän GAP-analyysin tavoin tunnistamaan puutteita vasten tietosuojalainsäädäntöä ja vaatimustenmukaisuutta.

Järjestelmien suunnittelussa on pyrittävä henkilötietojen minimointiin[1097]. Sama periaate koskee ylipäätänsä henkilötiedon käsittelyä. Lisäksi henkilötietojen käsittelyn tulee perustua tarpeellisuuteen ja käyttötarkoitussidonnaisuuteen. Näin ollen uusia järjestelmiä tai järjestelmäintegraatioita kehittäessä tulee olla tarkkana, ettei henkilötietoja aleta käsittelemään ristiriitaisella tavalla alkuperäisen, laillisen käyttötarkoituksen ja käsittelyperusteen kanssa[1098].

[1093] Euroopan tietosuojaneuvoston (EDPB) ohje 4/2019, s. 5.
[1094] Ks. Järvinen 2022b, s. 27. Huom. Netissä on palveluita kuvitteellisten henkilötietojen luomiseen.
[1095] OECD 2022, *Recommendation of the Council on the Digital Security of Products and Services*, OECD/LEGAL/0481, s. 8: *"Integrate privacy impact assessments and privacy-by-design objectives and requirements in the development process of their products and services;"*.
[1096] GDPR kohta 84 ja 90.
[1097] Saarenpää 2018: 26.
[1098] Rekisterinpitäjä ei saa yhdistää tietueita tai tehdä jatkokäsittelyä uusia, yhteensopimattomia tarkoituksia varten. Kaikkien uusien tarkoituksien on oltava yhteensopivia alkuperäisen käyttötarkoituksen kanssa, ja sen on ohjattava myös käsittelyn rakenteeseen tehtäviä mahdollisia muutoksia. Ks. Euroopan tietosuojaneuvoston (EDPB) ohje 4/2019, s. 21.

> Jos henkilötietojen laillinen käsittelyperuste tunnistetaan muuttuvan esimerkiksi siirrettäessä tietoja järjestelmästä toiseen toisenlaista käsittelyä varten, tulisi henkilötiedot mahdollisesti anonymisoida.
>
> Kun henkilötietojen laillinen käsittelyperuste loppuu, henkilötiedot on myös tällöin poistettava tai anonymisoitava. Järjestelmien tulisi mahdollistaa helppo ja sujuva tiedon poistaminen sekä erilaisten säilytysaikojen määrittely. Joissain tapauksissa henkilötietojen poistaminen ei ole tarkoituksenmukaista, jolloin pseudonymisointi tulee kyseeseen[1099]. ”Mahdollisimman pian” toteutettu henkilötietojen pseudonymisointi on tietosuojaasetuksessa katsottu olevan yksi tekninen ja organisatorinen tietoturvatoimenpide osana sisäänrakennettua ja oletusarvioista tietosuojaa[1100]. Pseudonymisointi on nähty olevan myös merkittävä osa tietoturvallisuuden suunnittelua[1101]. Pseudonymisoitu tieto on kuitenkin lain mukaan edelleen yhdistettävissä luonnolliseen henkilöön käyttämällä lisätietoja, jolloin se on henkilötietoa ja tiedon käsittelyssä tulee noudattaa tietosuojalainsäädäntöä ja muun muassa samoja käyttötarkoitussidonnaisuuteen ja tietojen minimointiin liittyviä periaatteita. Näin ollen organisaatioiden käytännön työssä pseudonymisoinnin sijaan saattaa korostua erityisesti henkilötiedon keräämisen tai käsittelyn välttäminen osana tiedonkäsittelyn määrittelemistä järjestelmissä, taikka henkilötietojen mahdollisimman lyhyen säilytysajan määrittely sidottuna käsittelytarpeen minimointiin. Mikäli henkilötietojen käsittelyä ei pystytä minimoimaan ja välttämään, pseudonymisointi on kuitenkin huomion arvioinen tietoturvatoimenpide henkilötietojen suojaamiseksi järjestelmissä ja niissä luotavissa dokumenteissa.

Suhteellisuusperiaatteen mukaisesti henkilötietojen suojaamiseksi on otettava huomioon myös uusin tekniikka ja toteuttamiskustannukset sekä henkilötietojen käsittelyn aiheuttamat riskit luonnollisten henkilöiden oikeuksiin ja vapauksiin. Tietojärjestelmän tulisi perustua sellaiseen toiminta-analyysiin, jossa tietosuojariskit on kartoitettu[1102]. Esimerkiksi rekisterinpitäjän käyttäessä kolmannen osapuolen ohjelmistoa tai valmisohjelmistoa, rekisterinpitäjän on tehtävä tuotteelle riskienarviointi ja varmistettava, että toiminnot, joille ei ole laillista perustetta tai jotka eivät vastaa käsittelyn aiottuja tarkoituksia, poistetaan käytöstä[1103]. Jotta

[1099] Esimerkiksi EDPB:n ohjeistuksissa on määritelty, että varmuuskopiot ja lokit on pseudonymisoitava varotoimena, jotta minimoidaan mahdollisten tietoturvaloukkausten riskit, esimerkiksi käyttämällä tiivistämistä tai salausta. Ks. Euroopan tietosuojaneuvoston (EDPB) ohje 4/2019, s. 28.
[1100] GDPR kohta 78.
[1101] Saarenpää & Riekkinen 2023: 228.
[1102] Lehtonen 2001: 228–229.
[1103] Euroopan tietosuojaneuvoston (EDPB) ohje 4/2019, s. 12.

tällainen menettely olisi mahdollista, ohjelmistojen hankinta tulisi olla hallittua organisaatiossa ja hankinnan omistajien tulisi olla tietoisia tietosuojalainsäädännön vaatimuksista. Käytännön tasolla tämä ei aina toteudu. Lisäksi riskiperusteinen määrittely ja suunnittelu eivät tulisi olla kertaluontoisia vaan näiden tulisi olla jatkuva prosessi[1104]. Koska tietojen suojaamisen tulee olla tehokasta järjestelmän koko elinkaaren ajan, myös järjestelmäpäivitysten osalta tulee olla tarkkana uusien ominaisuuksien ja niiden sisältämän henkilötietojen käsittelyn riskiarvioinnin tarpeen osalta.

Loppujen lopuksi *Privacy by Design and Default* -periaate antaa aika lailla ”vapaat kädet” järjestelmien suunnitteluun ja ylläpitoon teknisten toteutusten osalta, kunhan henkilötietojen käsittely huomioidaan jo järjestelmää suunniteltaessa ja tietosuojaperiaatteet toteutuvat henkilötietojen käsittelyn osalta läpi järjestelmän elinkaaren. Sellaisia palveluita tai järjestelmiä, joiden toiminnallisuudet eivät vastaa rekisterinpitäjän tarpeita tai mahdollista tietosuojaa koskevien säännösten noudattamista, ei tulisi ottaa käyttöön[1105]. Huomioitava on osana *”Privacy by Design & Default”*-periaatetta se, että mahdollisuuksien mukaan järjestelmien ominaisuuksia suunniteltaessa, ottaessa käyttöön tai ylläpidettäessä henkilötietoja suojataan ensisijaisesti priorisoimalla teknisiä tietoturvatoimenpiteitä, koska se on tehokkainta[1106]. Järjestelmiä tulisi suunnitella niin, että ne minimoisivat inhimillisiä virheitä sekä näistä virheistä aiheutuvia riskejä, kuten tietovuotoja[1107].

EU:n kyberkestävyyssäädös[1108] (”CRA-asetus”) tulee voimaan tullessaan parantamaan tietoturvaan liittyvää elinkaarimalliajattelua. Asetuksena se tulee olemaan suoraan jäsenmaita velvoittava. Ehdotusluonnoksen ensimmäisen sivun taustaperusteluiden kohdan 1 mukaan asetuksen tavoitteena on luoda edellytykset digitaalisia elementtejä sisältävien tietoturvallisten tuotteiden[1109], kuten ohjelmistojen,

[1104] Voutilainen 2020: 69; Voutilainen 2023: 79.
[1105] Ks. tarpeettomien sijaintitietojen keräämistä koskeva päätös TSV 5.7.2021, dnro. 3843/163/20.
[1106] Tällöin dokumentointi ja ohjeistus on toissijaista.
[1107] Saarenpää 2018: 26.
[1108] COM (2022) 454 final.
[1109] Asetuksen 3 artiklan mukaan digitaalisia elementtejä sisältävällä tuotteella tarkoitetaan ohjelmisto- tai laitteistotuotetta ja siihen sisältyviä datan etäkäsittelyratkaisuja, mukaan lukien toisistaan erillään markkinoille saatettavat ohjelmisto- tai laitteistokomponentit. Ehdotetun kyberkestävyyssäädöksen liitteessä III (COM 2022 454 final) on määritelty kriittisiä digitaalisia elementtejä sisältäviä tuotteita, jotka on jaettu kahteen luokkaan. Luokkajaottelu perustuu ehdotetun asetuksen kohdan 26 mukaan kyberturvariskiin, jonka perusteella luokan II tuotteisiin liittyvä kyberturvapoikkeama voisi johtaa suurempiin kielteisiin vaikutuksiin kuin luokan I tuotteissa. Kriittisiin tuotteisiin on asetusehdotuksen mukaan sovellettava myös näin ollen tiukempia vaatimustenmukaisuuden arviointimenettelyjä. Luokkaan I kuuluvat muun muassa erinäiset ohjelmistot, järjestelmät, rajapinnat ja palvelut, kuten identiteetinhallintaohjelmistot, verkkoliikenteen seurantajärjestelmät ja salasanojen hallinnointipalvelut. Luokkaan II kuuluvat muun muassa

kehittämiselle varmistamalla, että laitteisto- ja ohjelmistotuotteet saatetaan markkinoille vähemmin haavoittuvuuksin ja että valmistajat suhtautuvat tietoturvaan vakavasti tuotteen koko elinkaaren ajan. Lisäksi esimerkiksi asetusluonnoksen 10 artiklan kohdan 2 mukaisesti valmistajien on arvioita digitaalisia elementtejä sisältävän tuotteen kyberturvariskit ja otettava arvioinnin tulokset huomioon tällaisen tuotteen suunnittelu-, kehitys-, tuotanto-, toimitus- ja ylläpitovaiheissa kyberriskien minimoimiseksi, tietoturvapoikkeamien ehkäisemiseksi ja tällaisten poikkeamien vaikutusten minimoiseksi, myös käyttäjien terveyden ja turvallisuuden osalta. Kyberkestävyyssäädöksen 11 artiklan mukaisesti valmistajan on myös ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluessa, kun se on tullut asiasta tietoiseksi, ilmoitettava ENISA:lle eli EU:n kyberturvallisuusvirastolle kaikista digitaalisia elementtejä sisältävän tuotteen sisältämistä aktiivisesti hyödynnetyistä haavoittuvuuksista sekä tällaisen tuotteen tietoturvaan vaikuttavista poikkeamista.

> Ehdotetun luonnosasetuksen liitteessä I ovat varsinaiset digitaalisia elementtejä sisältävien tuotteiden olennaiset vaatimukset. Liitteen I mukaan tällaiset tuotteet tulee suunnitella, kehittää ja tuottaa tavalla, joka huomioi asianmukaisen, riskeihin perustuvan kyberturvallisuuden tason. Aikaisemmin mainitun riskienarvioinnin perusteella ja soveltuvin osin digitaalisia elementtejä sisältävä tuote tulee a) olla tietoturvallinen oletuskonfiguraatioltaan, b) omata asianmukaiset valvontamekanismit luvattoman käytön estämiseksi, c) suojata datan luottamuksellisuutta, d) suojata datan eheyttä ja ilmoitettava poikkeamista, e) minimoida datan käsittelyä, f) suojata olennaisten toimintojen saatavuus sisältäen myös palvelunestohyökkäysten[1110] sietokyvyn ja niiden vaikutusten lieventämisen, g) minimoida muiden laitteiden ja tietoverkkojen käytöstä aiheutuvaa negatiivista vaikutusta palvelujen saatavuuteen, h) olla suunniteltu, kehitetty ja tuotettu rajoittaen hyökkäyspinta-aloja, i) olla suunniteltu, kehitetty ja tuotettu pienentäen poikkeamien vaikutusta, j) tuottaa turvallisuustietoa tallentaen ja seuraten relevanttia sisäistä toimintaa, sekä k) varmistaa, että haavoittuvuudet voidaan korjata (automaattisilla) turvallisuuspäivityksillä ja, että soveltuvin osin saatavilla olevista päivityksistä tulee ilmoitus käyttäjille[1111]. Liitteen I mukaan digitaalisia elementtejä sisältävät tuotteet on toimitettava ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia.

---

serverien, kannettavien tietokoneiden ja puhelimien käyttöjärjestelmät sekä teolliseen käyttöön tarkoitetut reitittimet, modeemit ja kytkimet.

[1110] DoS-hyökkäys (denial-of-service-attack) eli palvelunestohyökkäys on kyberhyökkäys, jolla pyritään ylikuormittamaan verkkosivuja ja estämään niiden käyttö useimmiten kohdistamalla suuren määrän liikennettä palveluun.

[1111] Digitaalisia elementtejä sisältävien tuotteiden ominaisuuksiin liittyvät tietoturvavaatimukset. Ks. COM (2022) 454 final, Liite I: 1.

> Liitteen I kohdassa 2 on painotettu haavoittuvuuksien hallintaa. Esimerkiksi digitaalisia elementtejä sisältävien tuotteiden valmistajien tulee tunnistaa ja dokumentoida haavoittuvuuksia sekä riskiperusteisesti viipymättä korjata niitä ja julkisesti informoida korjatuista haavoittuvuuksista. Haavoittuvuuksien ilmoittamista koskevat periaatteet tulee laatia ja valmistajien tulee toteuttaa toimenpiteitä helpottaakseen tiedon jakamista mahdollisista haavoittuvuuksista.[1112] Lisäksi valmistajien tulee tehdä tehokkaita ja säännöllisiä turvallisuustestejä ja -katselmointeja digitaalisia elementtejä sisältäville tuotteille. Valmistajien tulee myös mahdollistaa päivitysten turvallinen jako ja, että turvallisuuskorjaukset tai päivitykset ovat jaettu viipymättä ja ilmaiseksi sekä sisältäen mahdolliset ohjeistukset käyttäjien toimille.[1113]

CRA-asetuksen vaatimukset painottavat riskiperusteista lähestymistapaa, joka huomioi tietoturvallisuuden digitaalisia elementtejä sisältävien tuotteiden elinkaaren alkupäästä alkaen[1114]. Onkin mielenkiintoista huomata, miten ennen tekniikkaan taipuvaa tekstiä lähes välteltiin teknologianeutraalisuuden nimissä, mutta nykyään lainsäädännön kehityksessä on huomattavissa muutos, joka johtuu joko vanhojen periaatteiden ”löyhentämisestä” taikka lainsäätäjän osaamisen kehittymisestä. Esimerkiksi CRA-asetuksen aikaisemmin mainittu liite I ei ole luonteeltaan samalla tavalla teknologianeutraali kuin, mitä tietosuoja-asetuksessa ilmennyt ”*Privacy By Design and Default*” -periaate on ollut. CRA-asetuksen osalta onkin hyvin onnistuttu säätämään tietoturva-alan hyviä käytänteitä hyödyntämällä niin sanottuja vähimmäisvaatimuksia, jotka ovat myös mahdollisimman teknologianeutraaleita.

[1112] Vaatimuksella on paljon yhteistä vuonna 2019 päivitetyn kansallisen tunnistus- ja luottamuspalvelulain (617/2019, laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista) kanssa, jonka 16 §:n mukaan tunnistuspalvelun tarjoajan tulee ilmoittaa palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista ja häiriöistä. Lisäksi ilmoituksessa on kerrottava muun muassa niistä toimista, joilla eri tahoilla on käytettävissään näiden uhkien ja häiriöiden torjumiseksi (HE 264/2018 vp: 50).

[1113] COM (2022) 454 final, Liite I: 2. Haavoittuvuuksien käsittelyä koskevat vaatimukset.

[1114] Huomioon on myös otettava EU:n datasäädös (2023/2854/EU). Siinä missä kyberkestävyyssäädöksen (CRA) vaatimukset kohdistuvat digitaalisia elementtejä sisältäviin tietoturvallisiin tuotteisiin, EU:n datasäädöksessä keskitytään tuotteiden tai siihen liittyvän palvelun, esimerkiksi ohjelmiston, vaatimuksiin niiden sisältämän datan osalta. Tietoturvan kolmen ulottuvuuden (luottamuksellisuus, eheys ja saatavuus) osalta datasäädöksen vaatimukset keskittyvät lähinnä datan saatavuuteen ja keskiössä ovat kuluttajan oikeudet. Organisaationäkökulmasta datasäädös kuitenkin lisää oikeudellisen suunnittelun vaatimuksia datasäädöksessä tarkoitettujen tuotteiden ja palveluiden osalta.

On selkeästi huomattavissa, että uusimpien etenkin kyberturvallisuutta koskevien säädöksien tai säädösluonnoksien kohdalla niin sanottu teknisluontoinen käsitteistö on lisääntynyt. Esimerkiksi NIS 2 -direktiivin 21 artiklan mukaiset kyberturvallisuusriskien hallintatoimenpiteet ovat enemmän suoraviivaisia verrattuna tietosuoja-asetuksen 32 artiklan mukaisiin teknisiin ja organisatorisiin toimenpiteisiin. Tämä ilmenee kyseisissä pykälissä niin, että NIS 2 -direktiivissä on mainittu esimerkiksi suoraan varmuuskopiointi ja palautumissuunnittelu, kun taas tietosuoja-asetuksessa sama asia on laveammin kuvattuna *”kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa”*. Kuten aikaisemmin tässä tutkimuksessa on mainittu[1115], teknologianeutraalisuuden periaatteen mukaisesti lainsäätäjä pyrkii sääntelemään ensisijaisesti tekoja teknologian sijaan, jonka myötä säädöksissä on usein vältelty tietoteknisiä ilmaisuja. Teknologianeutraalisuuden periaate ei ole eikä sen tulisikaan olla ainoastaan tietoteknisten termien välttämistä lakitekstissä. Hyvä tietoturvan sääntelyjärjestelmä edellyttää sääntelyn ja teknologian yhteensovittamista teknologianeutraalisti. Nykyinen lainsäädäntö on kehittynyt teknologianeutraalisuuden osalta parempaan suuntaan, kun se ei ole enää niin ehdottoman neutraalia.

Yhteenvetona todettakoon, että järjestelmien elinkaarisuunnittelun vaatimukset lainsäädännössä ovat hajanaiset. Esimerkiksi NIS 2 -direktiivin 21 artiklan yhtenä vähimmäisvaatimuksena on verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus. Sähköisen viestinnän palvelulain 243 §:ssä elinkaari on huomioitu niin, että säännöksen mukaan yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä taaten sähköisen viestinnän tietoturvallisuus. Samoin tiedonhallintalain 13 § mukaan tiedonhallintayksikön on varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan sekä lisäksi digipalvelulain 4 §:n mukaan viranomaisen on suunniteltava ja ylläpidettävä digitaaliset palvelunsa siten, että niiden tietoturvallisuus ja tietosuoja on varmistettu. Näin ollen tietoturvallisuuden huomiointi organisaation järjestelmien koko elinkaaren osalta ulottuu vain tiettyihin toimijoihin. Huomioitava on se, että muihin organisaatioihin kohdistuu mahdollisesti tietoturvavaatimuksia välillisesti niiden toimijoiden kautta, joita voimassa olevan lainsäädännön elinkaarisuunnittelun vaatimukset suoraan velvoittavat ja vastuuttavat. Täten nykyinen tietoturvan sääntelyjärjestelmä ei näyttäydy kohtuullisena ja oikeudenmukaisena, sillä se ei velvoita kaikkia toimijoita hyvän tietoturvatavan mukaisiin tietoturvatoimenpiteisiin. Tulevan CRA-asetuksen myötä tietoturvavaatimuksien huomioiminen elinkaarimallin mukaan kehittyy parempaan, sillä CRA-asetus ulottuu näillä näkymin kaikkiin digitaalisia elementtejä sisältävien tuotteiden valmistajiin. Se ei

[1115] Ks. luku 2.4.2 (”Muut tietoturvalainsäädäntöön liittyvät keskeiset periaatteet”).

kuitenkaan yhtenäistä ja velvoita järjestelmien tietoturvallisuuden huomioimista niiden koko elinkaaren osalta kaikissa organisaatioissa. Järjestelmien tietoturvan elinkaarimalli on kytköksissä tiedon elinkaaren tietoturvavaatimuksiin. Mikäli järjestelmien tietoturvaa ei huomioida niiden koko elinkaaren ajalta, myöskään tiedon suojaaminen sen koko elinkaaren ajalta ei toteudu. Toisin sanoen Saarenpään kuvaama *"tiedon tie"* ei ole turvattu. Henkilötietojen suojan sekä muiden yksilöiden oikeuksien ja organisaation luottamuksellisten tietojen suojan toteutumisen takeena on tiedon tien turvaaminen koko järjestelmien elinkaaren ajalta. Tällöin luottamuksellisuuden takaaminen tiedon tiellä ei ole ainoastaan riittävää, vaan järjestelmien suunnittelussa on huomioitava myös tiedon eheyden ja käytettävyyden vaatimukset koko järjestelmän elinkaaren ajalta. Kyber- ja tietoturvallisuus kuin myös digitaalisten teknologioiden häiriönsietokykyinen toiminta ovat riippuvaisia sekä järjestelmän koko elinkaaresta että tietojen tiestä[1116].

4.4.2 Järjestelmien lokitusvaatimukset tietoturvan sääntelyjärjestelmässä

Osana monitasoista suojaamista on tärkeää pystyä jäljittämään turvallisuustapahtumia muun muassa keräämällä tarpeellisia lokitietoja ja säilyttämällä lokeja turvallisesti käyttötapauksen tarpeet huomioon ottaen. Monitasoiseen suojaamiseen liittyy myös poikkeamien havainnointi (ja palautuminen), joka saattaa toisinaan edellyttää automaattisia, ennakoivia, lokitietoja hyödyntäviä havainnointi- ja hälytystyökalujen käyttöä, mutta myös manuaalista lokien perkaamista.[1117]

Nykyisessä verkkoyhteiskunnassa tietojärjestelmäriippuvuuden kasvaessa olisi suotavaa kiinnittää huomiota tietojärjestelmien suunnittelussa tietojärjestelmän käytön ja toiminnan myöhempään todennettavuuteen, esimerkiksi erilaisten lokitoimintojen luomisella ja järjestelmässä käsiteltävän datan tallentamisella. Todennettavuus edesauttaa järjestelmän teknisen toimivuuden varmistamista ja häiriötilanteista palautumista. Kehitystyössä ei tule kuitenkaan unohtaa viranomaisohjeistuksia ja standardeja. Lokitoimintojen suunnittelussa korostuvat myös oikeudelliset vaatimukset etenkin tietosuojan ja luottamuksellisen viestin suojan turvaavan lainsäädännön kannalta.[1118] Tietojen säilytys (*data retention*) ja jälkikäteinen todennettavuus ovat myös olennaisia työkaluja toimivaltaisille tahoille tutkia

[1116] Pöysti 2023: 45.
[1117] Teknisin menetelmin toteutettua valvontaa on käsitelty aikaisemmin luvussa 3.5.4 ("Muu teknisin menetelmin toteutettu valvonta ja välitystiedot"), jossa keskeinen näkökulma on lokitiedon käyttö osana valvontaa. Tässä luvussa käsitellään ennemminkin lokien keräämistä ja järjestelmien lokitusvaatimuksia.
[1118] Riekkinen 2019: 147, 523–524.

tehokkaasti kansallisessa lainsäädännössä määriteltyjä rikoksia, kuten tietoverkkorikoksia[1119].

Lokitietojen kerääminen ja käsittely on katsottu olevan pääsääntöisesti henkilötietojen käsittelyä, jolloin henkilötiedot muodostavat rekisterin ja lokituksessa on otettava huomioon tietosuoja-asetuksen vaatimukset muun muassa tarpeellisuudesta, käyttötarkoitussidonnaisuudesta ja asiallisuudesta[1120]. Myös esimerkiksi kansallisen tietosuojalain 6 §:ssä korostetaan, että käsiteltäessä erityisiä henkilötietoryhmiä[1121] on tietoturvatoimenpiteinä tehtävä rekisteröidyn oikeuksien suojaamiseksi lokitusta eli toimenpiteitä, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty. Tällöin lokitusta tulisi ainakin tehdä terveydenhuollon ja henkilöstöhallinnon järjestelmissä, sillä näissä käsitellään useimmiten erityisiä henkilötietoja. Näin ollen tietosuojalainsäädäntö ikään kuin rajoittaa lokitusta tiettyjen tietosuojaperiaatteiden myötä, mutta yhtäaikaisesti myös velvoittaa tekemään sitä.

Tietosuoja-asetus huomioon ottaen, lokeja ei tulisi kuitenkaan henkilötietojen minimointiperiaatteen mukaisesti kerätä liian laajasti eikä säilöä liian kauaa. Tietosuojaperiaatteiden näkökulmasta lokien säilytysaika tulisi olla mahdollisimman lyhyt, kun taas tietoturvan näkökulmasta lokien säilytysaika tulee sitoa mahdollisuuksien mukaan rikosten vanhenemisaikoihin. Lokituksen aikarajoihin vaikuttaa myös rikostutkintojen lisäksi toki muualla lainsäädännössä asetetut vaatimukset säilyttää lokeja esimerkiksi vahingonkorvausvaatimuksien taikka kirjanpitolaista tulevien laskutustietojen säilytysvaatimusten takia. Vastakohtaisesti lokituksen säilytysaikoja rajaavat esimerkiksi kustannukset ja järjestelmän kapasiteetti tilan suhteen.

Rikoksen vanhenemisaika on sidoksissa lähtökohtaisesti rikoksesta säädetyn enimmäisrangaistuksen pituuteen ja ajan laskenta lähtee liikkeelle rikoksen tekopäivästä[1122]. Esimerkiksi rikoslain 38 luvun mukaisista tieto- ja viestintärikoksista pisin rangaistusaika eli 5 vuotta on törkeällä tietoliikenteen häirinnällä ja törkeällä tietojärjestelmän häirinnällä. Törkeästä viestintäsalaisuuden loukkauksesta sekä törkeästä tietomurrosta voidaan tuomita enintään 3 vuodeksi vankeuteen. Rikoslain 8 luvun 1 §:n mukaan syyteoikeus vanhentuu 10 vuodessa, jos ankarin

[1119] Euroopan unionin neuvosto, Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime 6.6.2019: 5. Neuvosto on myös todennut, että tietojen säilyttämisen ja vastaavien tutkintatoimenpiteiden käytössä olisi noudatettava perusoikeuskirjassa vahvistettuja suojattavia perusoikeuksia ja -vapauksia sekä käyttötarkoitussidonnaisuuden, tarpeellisuuden ja suhteellisuuden periaatteita.
[1120] Voutilainen 2020: 223; Voutilainen 2023: 290–291; HE 284/2018 vp: 149.
[1121] Esimerkiksi terveystieto, poliittinen mielipide, vakaumus, geneettiset ja biometriset tiedot, seksuaalinen suuntautuminen, rotu ja etinen alkuperä.
[1122] Ks. Rikoslain 8 luku 2 §.

rangaistus on yli 2 vuotta, eli kyseiset rikokset kuuluvat tämän piiriin. Niissä rikoksissa[1123], joissa ankarin rangaistus on yli vuosi ja enintään kaksi vuotta vankeutta, syyteoikeus vanhentuu 5 vuodessa.

Mitään yleistä, selkeää aikarajaa lokien säilytysajoille ei lähtökohtaisesti lainsäädännössä ole[1124], mutta käytännössä etenkin henkilötietojen ollessa kyseessä, rekisterinpitäjän on pystyttävä perustelemaan säilytysaika. Edellä mainitut vanhenemisajat, tietosuojan tarpeellisuusvaatimus ja tietojen minimoinnin periaatteet huomioon ottaen, ei ole perusteltua säilyttää lokeja 5–10 vuotta kaikkien järjestelmien osalta[1125]. Keskeisiä, kriittisimpiä lokeja törkeiden tieto- ja viestintärikosten osalta ovat esimerkiksi pääsynvalvontalokit ja tietoturvalokit, joiden osalta järjestelmästä ja toimialasta riippuen tuo 10 vuotta voisi olla perusteltua. Lokitusaika riippuu erityisesti järjestelmän kriittisyydestä, johon puolestaan vaikuttaa se, mitä kaikkea järjestelmään pääsy mahdollistaa ja kuinka kriittistä tietoa järjestelmässä on. Huomioitava on myös se, että usein törkeät tieto- ja viestintärikokset tulevat aikaisemmin ilmi kuin 10 vuodessa esimerkiksi tietovuodon tai kiristämisen kautta. Tämä fakta myös kaventaa tietosuojan näkökulmasta sitä, että 10 vuoden säilytysaika useiden lokien osalta olisi täysin käyttötarkoitussidonnaista. Useissa järjestelmissä 6kk – 2 vuoden lokitusaika on varsin riittävä.

Tietojen minimoinnin ja tarpeellisuuden periaatteiden lisäksi lokituksen osalta on huomioitava oikeasuhtaisuuden vaatimus, mikä liittyy esimerkiksi rekisterinpitäjän oikeutettuun etuun. Henkilötietojen käsittely on tietosuoja-asetuksen 6 artiklan mukaan lainmukaista, jos käsittely on tarpeen toteuttaakseen rekisterinpitäjän oikeutettua etua. Tällainen oikeutettu etu voi tietosuoja-asetuksen johdannon 49 kohdan mukaan liittyä esimerkiksi tietoturvaloukkauksiin varautumiseen sekä verkko- ja tietojärjestelmien suojautumiskyvyn takaamiseen, kun se on oikeasuhtaista ja rajoittuu ehdottoman välttämättömään käsittelyyn[1126]. Esimerkiksi sellainen sääntely on oikeasuhtaisuusvaatimuksen vastaista, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisen erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin[1127]. On sanomattakin selvää, että myös esimerkiksi tällaisten lokitietojen

[1123] Esimerkiksi tietomurto (38:8), tietojärjestelmän häirintä (RL 38:7a) ja viestintäsalaisuuden loukkaus (RL 38:3).
[1124] Pois lukien sähköisen viestinnän palveluista annetun lain 145 §, jonka mukaan keskeisiä välitystietoja sisältävien tietojärjestelmien käyttölokin säilytysaika 2 vuotta. Myös viranomaisen tukipalvelulain 20 §:ssä on säädetty lokirekisteristä, jonka säilytysaika on vähintään 2 vuotta.
[1125] Rekisterinpitäjän on pystyttävä perustelemaan objektiivisesti ja osoitusvelvollisuuden periaatteen mukaisesti se, että tietojen mahdollinen säilyttäminen on välttämätöntä. Ks. Euroopan tietosuojaneuvoston (EDPB) ohje 4/2019, s. 13.
[1126] Korpisaari & Toikkanen 2020: 472.
[1127] PeVL 18/2014 vp: 6.

säilyttäminen käytännön tasolla on ongelmallista jo pelkästään tietosuojaperiaatteiden kannalta.

Oikeasuhtaisuuden osalta huomioitava on myös henkilötietoja sisältäviin lokeihin ulottuva tietosuoja-asetuksen 15 artiklan vaatimus, jonka mukaan jokaisella rekisteröidyllä on oikeus saada pääsy henkilötietoihinsa sekä saada tiedot muun muassa käsittelyn tarkoituksista ja vastaanottajista[1128]. Rekisterinpitäjän on toimitettava jäljennös käsiteltävistä henkilötiedoista, mutta jäljennös ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin.

> *Jäljennöksellä tarkoitetaan sanamuodon mukaisesti alkuperäistä vastaavaa toisintoa rekisteröidyn henkilötiedoista, joihin kohdistetaan toimintoja ja jotka on luokiteltava rekisterinpitäjän suorittamaksi käsittelyksi. Jäljennöksen käsitteellä tarkoitetaan näin ollen alkuperäiskappaletta vastaavaa toisintoa tai transkriptiota, joten käsiteltävien tietojen puhtaasti yleinen kuvaus tai viittaus henkilötietojen ryhmiin ei vastaa tätä määritelmää. Se ei kuitenkaan liity asiakirjaan sellaisenaan vaan sen sisältämiin henkilötietoihin, jolloin toisinnon on sisällettävä kaikki henkilötiedot täydellisinä, tarkkoina ja kokonaisuudessaan.*[1129]

Lokitietojen luovuttaminen rekisteröidyn pyynnöstä tällaisena jäljennöksenä onkin varsin ongelmallista muiden oikeuksien kannalta, eikä myöskään tietoturvasyistä kaikenlaisia lokitietoja voida yksinkertaisesti luovuttaa. Esimerkiksi **ratkaisussa EUT 22.6.2023 C-579/21 Pankki S**[1130] on punnittu myös muiden oikeuksien toteutumista rekisteröidyn oikeuksien rinnalla:

> *Tapauksessa Pankki S oli kieltäytynyt ilmoittamasta rekisteröidyn tietoja tarkastelleiden työntekijöiden henkilöllisyyksiä käyttäjälokitiedoista, koska nämä tiedot olivat kyseisten työntekijöiden henkilötietoja. Suomen apulaistietovaltuutettu on katsonut ratkaisukäytännössään, että käyttäjälokitiedot eivät ole rekisteröityä koskevia henkilötietoja vaan niitä työntekijöitä koskevia henkilötietoja, jotka ovat käsitelleet rekisteröidyn henkilötietoja. Tuomioistuin pohtikin, kuuluuko käsittelytoimien yhteydessä*

[1128] Pääsy henkilötietoihin tarkoittaa sitä, että rekisterinpitäjän on etsittävä henkilötietoja kaikista tietoteknisistä järjestelmistä ja muista kuin tietoteknisistä rekistereistä sellaisten hakukriteerien perusteella, joissa huomioidaan se, miten tiedot on jäsennelty (esim. nimi ja asiakasnumero). Kaikki käsittelyä koskevat tiedot on toimitettava tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tältä osin tarkemmat vaatimukset määräytyvät tietojenkäsittelyn olosuhteiden ja sen mukaan, miten hyvin rekisteröity ymmärtää viestintää (esim. lapset). Ks. Euroopan tietosuojaneuvoston (EDPB) ohje 1/2022, s. 4.
[1129] Ks. Itä-Suomen HAO 22.12.2023 2891/2023 ja EUT 4.5.2023 C-487/21 Österreichische Datenschutzbehörde ja CRIF ratkaisun kohdat 21, 28, 32 ja 39.
[1130] Ratkaisun kohdat 73, 79–80 ja 83.

> *luotujen käyttäjälokitietojen, jotka sisältävät työntekijöiden henkilötietoja, luovuttaminen tietosuoja-asetuksen 15 artiklan piiriin, koska nämä tiedot saattavat osoittautua rekisteröidylle tarpeelliseksi tietojen käsittelyn lainmukaisuuden arvioinnissa. Tuomioistuin katsoi, että rekisterinpitäjän työntekijöitä ei voida pitää tietosuoja-asetuksen 15 artiklan 1 kohdan c alakohdan tarkoitettuna vastaanottajina heidän käsitellessään henkilötietoja rekisterinpitäjän alaisuudessa ja sen ohjeiden mukaisesti. Kuitenkin rekisterinpitäjän työntekijöiden henkilöllisyyttä koskevien tietojen antaminen rekisteröidylle, jonka henkilötietoja on käsittely, voi kuitenkin loukata näiden työntekijöiden oikeuksia ja vapauksia. Näin ollen tässä tapauksessa tuomioistuin antoi kyseisessä ristiriitatilanteessa enemmän painoarvoa työntekijöiden oikeuksille kuin rekisteröidyn tarkastusoikeudelle henkilötietojensa käsittelyn lainmukaisuuden suhteen edellyttäen kuitenkin sitä, että tämä ei saa johtaa siihen, ettei rekisteröidylle anneta mitään tietoa.*

EUT:n ratkaisu lisää organisaatioiden velvollisuutta tutkia tietopyynnön mukaisesti lokit varmistaakseen, ovatko rekisterinpitäjätyönantajan alaisuudessa toimivat työntekijät toimineet ohjeiden ja lain vastaisesti. Jos lokeista ei ilmenisi mitään poikkeavaa, työntekijöiden henkilöllisyyttä koskevien tietojen antaminen tietopyynnön tekijälle ei etenkään tällöin olisi perusteltua eikä sitä tarvitsisi tehdä. Mikäli väärinkäytöstä sen sijaan ilmenisi, tästä tulisi informoida tietopyynnön tehnyttä rekisteröityä, vaikka kyseessä ei välttämättä olisikaan korkea riskinen henkilötietojen tietoturvaloukkaus. Tällöin rekisteröidyn tiedonsaantioikeus toteutuisi ja rekisteröidyn olisi mahdollista käyttää myös muita oikeuksiaan paremmin. Tällöin EUT:n ratkaisun mukaisesti organisaation vastuulla olisi myös punnita, tulisiko tällaisessa väärinkäytöstapauksessa antaa työntekijän tai työntekijöiden henkilötietoja rekisteröidylle vai tulisiko rekisteröityä kehottaa tekemään asianomistajana rikosilmoitus tietosuojarikoksesta. Tällaisessakaan väärinkäytöstilanteessa organisaation ei tulisi rikkoa työntekijöiden henkilötietojen suojaa vaan informoida ensinnäkin tietopyynnön tehnyttä rekisteröityä toimenpiteistä, mitä seuraamuksia väärinkäytöksestä aiheutuu organisaation työntekijälle tai työntekijöille. Toiseksi organisaation tulisi informoida rekisteröidylle, onko kyseessä sen laatuinen henkilötietojen tietoturvaloukkaus, että organisaatio tekee asiasta lakisääteisen ilmoituksen tietosuojavaltuutetulle sekä mahdollisesti poliisille asianomistajana. Näiden seikkojen jälkeen rekisteröity voisi helpommin tehdä päätöksen, aikooko tehdä myös rikosilmoituksen asianomistajana. Poliisin tutkinnan yhteydessä organisaatio voisi luovuttaa lokitietoja ja työntekijän taikka työntekijöiden henkilötietoja lainmukaisesti poliisille.

Pankki S:n tapauksessa **Itä-Suomen hallinto-oikeuden ratkaisun 22.12.2023 2891/2023** perusteella pankki oli antanut selvityksen rekisteröidylle lokitietoihin liittyen. Tästä selvityksestä ilmeni sisäisen tarkastajan lausunnon perusteella, että käsittely oli ollut asianmukaista. Selvitys itsessään ei ollut kuitenkaan riittävä ajankohtien ilmaisujen osalta vaan varsin lavea siihen nähden, että lokitiedoista on saatavissa tarkat aikaleimat lokitettaville tapahtumille. Muuten ratkaisu vastasi EUT:n aikaisempaa linjausta siitä, että käsittelijöiden henkilöllisyyksiä ei tarvitse luovuttaa rekisteröidyn lokitietopyynnössä heidän ollessa rekisterinpitäjän alaisuudessa toimivia henkilökuntaan kuuluvia henkilöitä:

> *Ratkaisun mukaan asiassa ei ollut ilmennyt, etteivätkö valittajan henkilötietoja käsitelleet henkilöt olisi olleet Pankki S:n työntekijöitä ja toimineet pankin ohjeistuksen mukaisesti. Mikäli valittaja katsoisi, että hänen henkilötietojaan oli käsitelty ilman lainmukaista perustetta, hänellä olisi mahdollisuus saattaa asia tältä osin valvontaviranomaisen käsiteltäväksi. Hallinto-oikeus kuitenkin katsoi, ettei pankin ilmoitus siitä, kuinka monena päivänä tietoja oli pyydetyllä aikavälillä käsitelty, ollut riittävä toisinto kyselytietojen sisältämistä valittajan pyytämistä henkilötietojen käsittelytoimien ajankohdista. Käyttäjälokitiedoista oli luovutettava käsittelytoimien tarkemmat ajankohdat. Tällöin tietojen luovuttaminen ei kuitenkaan edellyttänyt tietojen luovuttamista hallinto-oikeudelle toimitetun lokitietotulosteen muodossa, mikäli se ei olisi tarpeen valittajalle luovutettavien tietojen ymmärrettävyyden varmistamiseksi.*

Tietosuojalainsäädännön lisäksi järjestelmien lokitusvaatimuksia ilmenee myös muualla kansallisessa lainsäädännössä. Tiedonhallintalain 17 §:n mukaan viranomaisten tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista on kerättävä tarpeelliset lokitiedot, mikäli järjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Muissa tapauksissa lokituksen tarpeellisuus jää viranomaisen harkintaan. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Jos lokitietoja on tarpeellista käsitellä laajemmin, tulisi käsittelyn perustua johonkin toiseen säännökseen tai muuhun käsittelyn oikeusperusteeseen huomioon ottaen etenkin tietosuoja-asetuksen käyttötarkoitussidonnaisuuden, asiallisuuden ja tarpeellisuuden vaatimukset.[1131]

Tiedonhallintalain 17 §:ä täydentävänä suosituksena on myös määritelty, että sellaisissa järjestelmissä, joissa on salassa pidettäviä tietoja ja henkilötietoja, tulisi kerätä käyttölokitiedot. Muissa tapauksissa käyttölokituksen tarpeellisuutta tulee arvioida sillä perusteella, onko käyttölokituksella merkitystä esimerkiksi

[1131] Voutilainen 2020: 223–224; Voutilainen 2023: 290–291; HE 284/2018 vp: 149.

henkilötietojen suojaamisen näkökulmasta.[1132] Tiedonhallintalain 17 § on hyvä esimerkki teknologianeutraalista säätämisestä lokituksen osalta, jota on myös tarkennettu soft law -tyyppisellä käytännesäännöllä. Kyseinen vaatimus koskee myös välillisesti esimerkiksi viranomaisten järjestelmien toimittajia, jotka suunnittelevat järjestelmiä.

Huomioitava on myös se, että sähköisen viestinnän palveluista annetussa laissa on säädetty välitystietojen käsittelystä, jotka voivat olla myös lokitietoja[1133]. Sähköisen viestinnän palvelulain vaatimukset kohdistuvat kuitenkin lähinnä välitystietoja sisältävien lokien käsittelyyn, eli ei niinkään velvollisuuteen toteuttaa lokitusta järjestelmissä - lukuun ottamatta 145 §:n käsittelylokivaatimusta. Sähköisen viestinnän palvelulain 145 §:n mukaan viestinnän välittäjän, eli esimerkiksi myös yhteisötilaajana toimivan työnantajan, on tallennettava yksityiskohtaiset tapahtumatiedot luottamuksellisuuden ja yksityisyyden suojan kannalta keskeisiä välitystietoja sisältävissä tietojärjestelmissä tapahtuvasta välitystietojen käsittelystä. Kyseessä on siten eräänlainen audit trail -loki, johon tallennetaan lain mukaan, kuka on katselmoinut lokeja ja siihen liittyvä aikaleima kestotietoineen. Lisäksi tapahtumatiedot on säilytettävä 2 vuotta, mutta huomioitava on, että tämä on vähimmäisaika[1134].

Liikenne- ja viestintäministeriön ohjeessa[1135] linjataan, että edellä mainittu lokitusvelvollisuus koskee vain sähköisiä tietojärjestelmiä. Lokitusvelvollisuus syntyy, kun välitystietojen käsittely tapahtuu luonnollisten henkilöiden toimesta ja käsittelytoimet kohdistuvat tietyn tunnistettavissa olevan viestinnän osapuolen viestintään. Yhteisötilaajien osalta tallennusvelvoitteen alaista välitystietojen käsittelyä

[1132] Valtiovarainministeriön julkaisuja 2024:19: 39.
[1133] Ks. aiheen tarkempi käsittely luvuista 3.5.4 (”Muu teknisin menetelmin toteutettu valvonta ja välitystiedot”) sekä 3.5.5 (” Väärinkäytösten ehkäiseminen ja selvittäminen organisaatioissa”). Esimerkiksi lokeista välitystietojen käsittely on sallittua vain käsittelyn vaatimassa laajuudessa ja käyttötarkoitussidonnaisuus huomioon ottaen esimerkiksi tietoturvasta huolehtimiseksi (137 § ja 138 §). Yhteisötilaajana toimivalla työnantajalla on oikeus käsitellä välitystietoja väärinkäytöstapauksien ehkäisemiseksi ja selvittämiseksi, ja käsittelyoikeus on vain yhteisötilaajan viestintäverkon ja viestinpalvelun ylläpidosta ja tietoturvasta sekä turvallisuudesta huolehtivilla henkilöillä (146 § ja 148 §). Yhteisötilaajan automaattisesta ja manuaalisesta välitystietojen käsittelystä maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön sekä liikesalaisuuksien paljastamisen selvittämiseksi on säädetty myös erikseen (149 § - 154§). Yhteisötilaajan lisäksi sähköisen viestinnän palvelulaissa säädetään viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuudesta huolehtia tietoturvasta (247 §).
[1134] Viranomaisen on määriteltävä lokitietojen säilytysajat tarpeellisuuden perusteella, mutta yleisesti lokitietojen säilytysaika on vähintään viisi vuotta viranomaistoiminnassa rikosoikeudellisten vanhenemisaikojen vuoksi. Lisäksi lainsäädännön perusteella voi olla pidempiäkin säilytysaikoja. Ks. Valtiovarainministeriön julkaisuja 2024:19, s. 39.
[1135] Huomioitava on, että kyseessä on nimenomaan ohje. Sähköisen viestinnän palveluista annetun lain 145 §:n 2 momentissa lukee, että Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä 1 momentissa tarkoitetun tallentamisen ja säilyttämisen teknisestä toteuttamisesta. Näin ollen kyseistä ohjetta ei voida pitää velvoittavana.

tapahtuu erityisesti sähköpostijärjestelmien hallinnoinnin yhteydessä.[1136] Lain mukaisia keskeisiä välitystietojärjestelmiä ovat sellaiset, joissa välitystietoja säilytetään muutoin kuin lyhytaikaisesti, esimerkiksi tikettivarastot ja laskutusjärjestelmät[1137]. Pilvipalvelut voivat olla myös tällaisia järjestelmiä, jolloin näitä käyttäessä on syytä sopia käsittelylokin käytännön toteutuksesta viestinnän välittäjän alihankkijana toimivan pilvipalveluntarjoajan sekä oikeudellista vastuuta kantavan viestinnän välittäjän kesken. Keskeisiä välitystietoja sisältäviksi järjestelmiksi ei sen sijaan katsota kytkimiä ja reitittimiä, joihin välitystieto tallentuu lyhytaikaisesti ja niissä olevien välitystietojen käsittely on lähinnä manuaalista vianselvittelyä.[1138]

Vaikka laissa määritellään, että tapahtumatiedoista on käytävä ilmi käsittelyn ajankohta, kesto ja käsittelijä, Liikenne- ja viestintäministeriö ohjeistaa myös, että luonnollisesti tulee myös tallentaa mitä ja mihin tallennettuja välitystietoja käsittely on koskenut. Käsittelyllä tarkoitetaan samaa kuin tietosuoja-asetuksessakin, eli siihen liittyy välitystietojen kaikenlainen haku, käyttö ja muuttaminen. 145 §:n käsittelylokivaatimuksesta on mahdollista poiketa, jos lokittaminen ei ole teknisesti ja ilman kohtuuttomia kustannuksia mahdollista. Liikenne- ja viestintäministeriön ohjeen mukaan poikkeus voi kohdistua koko lokitusvelvollisuuden toteuttamisen sijasta myös yksittäisten tapahtumatietotyyppien tallentamiseen, eli esimerkiksi käsittelyn kestotieto voidaan jättää tallentamatta, jos se on teknisesti mahdotonta. Lokitusvelvollisuuden poikkeamisen perusteet ja tekniset rajoitteet on suotavaa dokumentoida. Käsittelylokeihin kohdistuu myös tietoturvasuosituksia, sillä Liikenne- ja viestintäministeriön ohjeen mukaan käsittelylokien sisältämien tietojen tulisi olla saatavilla kohtuullisessa ajassa ja mahdollisuuksien mukaan varmuuskopioituna, käsittelyloki tulee tallentaa tietoturvallisesti ja käsittelylokin tietojen seuranta, analysointi sekä automatisoidut hälytykset poikkeamista tulee määritellä asianmukaisessa laajuudessa.[1139]

Tuoreesta lainsäädännöstä NIS 2 -direktiivi ei ota ollenkaan suoraan lokitukseen kantaa. Esimerkiksi NIS 2 -direktiivin mukaisiin 21 artiklan kyberturvallisuusriskien hallintatoimenpiteisiin ei ole nostettu lokitusta, vaikka käytännön näkökulmasta sen kuuluisi olla osana tuota listausta. Yksi vaihtoehto on se, että se katsotaan kuuluvaksi kyseisessä artiklassa ilmeneviin perustason kyberhygieniakäytäntöihin. Näin ei kuitenkaan suoraan ole, sillä NIS 2 -direktiivin 49 kohdan mukaan

[1136] Liikenne ja viestintäministeriön ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta 2022: 3.
[1137] HE 221/2013 vp: 154–155.
[1138] Liikenne ja viestintäministeriön ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta 2022: 3, 8.
[1139] Liikenne ja viestintäministeriön ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta 2022: 4–6.

kyberhygieniaperiaatteisiin kuuluvat perustason käytännöt, kuten ohjelmisto- ja laitteistopäivitykset, salasanojen vaihtaminen, uusien asennusten hallinta, ylläpitäjän käyttöoikeuksia edellyttävien tilien rajoittaminen ja tietojen varmuuskopiointi. NIS 2 -direktiivin 89 kohdassa on myös mainittu, että perustason kyberhygieniakäytäntöihin kuuluvat nollaluottamuksen periaate, ohjelmistopäivitykset, laitteiden konfigurointi, verkon segmentointi, identiteetin- ja pääsynhallinta ja käyttäjien tietoisuuden lisääminen. Näin ollen perustason kyberhygieniakäytännöt eivät välttämättä sisällä lokitusta, sillä suoranaista viittausta lokitukseen tai esimerkiksi ”jälkikäteiselle todentamiselle ja varmistamiselle tietojen muutosten tai käyttäjätoimien osalta” ei kuitenkaan ole.[1140] Tämä on erikoista, sillä lokitus on tärkeä elementti osana poikkeamien tunnistamista ja lokitus lisää organisaatioiden havainnointikyvykkyyttä väärinkäytösten osalta. Toisaalta lokitietojen kerääminen ja analysointi on useamman havainnointi- ja valvontatyökalujen perusta, jotka ovat oletusarvoisia työkaluja osana NIS 2 -direktiivin mukaisia tietoturvatoimenpiteitä poikkeamien vaikutuksen estämiseksi ja minimoimiseksi. Ilman lokitietoja, organisaatioiden olisi mahdotonta näiden työkalujen avulla tunnistaa uhkia ja reagoida niihin reaaliajassa, tutkia tietoturvaloukkauksia taikka estää uhkia proaktiivisemmin. Hyvät käytänteet huomioon ottaen, tietoturvan sääntelyjärjestelmässä tulisi huomioida järjestelmien lokitusvaatimukset paremmin. Tästä näkökulmasta NIS 2 -direktiivi ei huomioi riittävästi ja selkeästi järjestelmälokitusta oleellisena osana kyberhygieniakäytäntöjä tai kyberriskien hallintatoimenpiteitä.

Aikaisemmin käsitellyssä ehdotuksessa kyberkestävyyssäädökseksi (”CRA-asetus”) on huomioitu lokitukseen liittyviä vaatimuksia paremmin kuin NIS 2 -direktiivissä. CRA:n luonnosliitteen I turvallisuusvaatimusten 3 j-kohdan mukaan digitaalisia elementtejä sisältävä tuote tulee tuottaa tietoturvaan liittyvää tietoa tallentamalla ja seuraamalla asiaan liittyvää sisäistä toimintaa, kuten tietojen, palvelujen tai toimintojen käyttöä tai muutoksia. Näin ollen voidaan päätellä, että digitaalisia elementtejä sisältävän tuotteen, kuten ohjelmiston, tulisi omata toiminnallisuutena lokien muodostaminen.

Yhteenvetona voidaan todeta, että yleisesti ottaen järjestelmien lokituksesta ei ole säädetty täsmällisesti kaikkia organisaatioita velvoittavana vähimmäisvaatimuksena, vaikka lokitus on yksi tärkeimmistä teknisistä tietoturvatoimenpiteistä poikkeamien ja väärinkäytösten havaitsemisen osalta. Karkeasti ilmaistuna eri säädöksien mukaan lokitusta tulee tehdä, mikäli järjestelmässä käsitellään erityisiä henkilötietoja, kyseessä on viranomaisen tunnistautumista tai muuta kirjautumista

[1140] Kyberturvallisuuslain 9 §:n 9 kohdan riskienhallinnan toimenpiteiden osalta todettu, että (poikkeamien) havainnointi- ja analysointikyvyn kannalta on välttämätöntä, että toimijalla on kerättynä ja käytettävissä riittävät lokitiedot esimerkiksi ylläpidosta, muutoksista, käytöstä ja virheistä. Itse 9 §:n luonnoksessa ei ole kuitenkaan suoranaista viittausta lokitukseen. Ks. HE 57/2024 vp, s. 166.

vaativa järjestelmä taikka viestinnän välittäjän keskeisiä välitystietoja sisältävissä tietojärjestelmissä käsitellään välitystietoja. Näin ollen organisaatioiden tietoturvan sääntelyjärjestelmä näyttäytyy järjestelmien lokitusvaatimuksien osalta epäjohdonmukaisena eikä se nykyisellään edistä riittävästi yksilöiden perusoikeuksia henkilötietojensa suojaan.

Myöskään lokitietojen säilytysajoista ei ole säädetty täsmällisesti lukuun ottamatta sähköisen viestinnän palveluista annetun lain 145 §:ä, jonka mukaan viestinnän välittäjän käyttölokitietoja on säilytettävä 2 vuotta niiden tallentamisesta. Lähinnä tietosuojaperiaatteet, kuten tietojen minimointi, tarpeellisuus ja käyttötarkoitussidonnaisuus rajaavat lokien säilytysaikoja, mutta toisaalta myös rikosoikeudelliset vanhentumisajat. Käytännön työssä lokitietojen säilyttämisen rajauksia ei kuitenkaan arvioida ja toteuteta riittävällä tasolla, vaikka a) rekisterinpitäjän velvollisuuteen kuuluu määritellä henkilötietojen säilytysajat; sekä b) tietoturvan näkökulmasta tiedon omistajan velvollisuuksiin kuuluu tiedon elinkaaren hallinta. Organisaation järjestelmissä syntyvä tieto (*system generated data*), kuten lokitieto, voidaan katsoa kuuluvan sekä organisaation omistajuuden että rekisterinpitäjyyden alle.

Liiallinen lokitus ja lokien säilöminen on organisaatioissa usein tunnistettu ongelma, eli joissain organisaatioissa kerätään ja säilötään liikaa lokeja vain varmuuden vuoksi. Näin ollen lainsäädännön ei tulisi kannustaa keräämään turhia lokeja. Edellä mainittu ongelma kuitenkin indikoi sitä, että tarvittaisiin lisää raameja lokien säilytysaikojen suhteen. Vastakohtaisesti on myös organisaatioita, joissa on puutteellista järjestelmien lokitusta, jolloin ne eivät tue väärinkäytösten selvittämisessä esimerkiksi henkilötietojen tietoturvaloukkausten osalta. Täten nykyisessä tietoturvan sääntelyjärjestelmässä ilmenevä hajanainen ja puutteellinen sääntely ei välttämättä edesauta organisaatioita lokitusvelvollisuuden tunnistamisessa, mutta ei myöskään tietojen minimoimisessa: suoraa vaatimusta järjestelmien lokitietojen säilytysajan määrittelemisestä ja dokumentoinnista ei ole. Lainsäädännössä tulisi korostaa paremmin lokituksen tarpeellisuuden reunaehtoja esimerkiksi huomioon ottaen henkilötietojen minimointi, tiedon salassa pidettävyys ja järjestelmien kriittisyysluokittelu. Näin ollen tietoturvalainsäädännön yhtenäistämiseksi ja tarpeellisen vähimmäistason luomiseksi olisi suotavaa säätää lokituksen osalta kaikkia organisaatioita velvoittavat vähimmäisvaatimukset, joissa myös täsmennettäisiin lokien säilytysaikoja.

4.4.3 Pääsynhallintavaatimukset tietoturvan sääntelyjärjestelmässä

Pääsynhallinta[1141] on yksi tärkeimmistä tietoturvakontrolleista, koska sen avulla konkreettisesti suojataan organisaation järjestelmissä olevaa tietoa. Hyvien käytäntöjen mukaisesti pääsyoikeuksia tulisi hallinnoida vähimpien oikeuksien periaatetta noudattaen, eli käyttöoikeudet tulisi määritellä ja niitä tulisi myöntää vain käsittelyoikeuksien osalta varmistetuille henkilöille. Lisäksi käyttöoikeudet ja valtuudet tulisivat olla tehtävien suorittamiseksi välttämättömiä, jolloin puhutaan myös *need-to-know*-periaatteesta.[1142] Tarkoituksenmukaista olisi välttää vaarallisten työ- ja rooliyhdistelmien syntyminen. Käyttöoikeudet tulisi pitää myös ajantasaisina.

Esimerkiksi ratkaisua **KKO 2013:20** on tulkittu niin, ettei yritysvakoilua koskevaa säännöstä ole perusteltua ulottaa sellaiseen työntekijän tietojen hankkimiseen, joka tapahtuu työntekijän työhön kuuluvien tiedonhankkimisoikeuksien rajoissa:

> *Tapauksessa A ja B olivat kopioineet ennen työsuhteensa päättymistä työnantajansa Y Oy:n tietojärjestelmistä käytössään olleille tietokoneille ja muistitikuille laajasti yrityssalaisuuksia sisältäneitä tietoja. Tietojen kopiointia ei ollut erikseen kielletty organisaation ohjeilla. A ja B olivat siirtyneet pian työsuhteidensa päättymisen jälkeen Y Oy:n kanssa kilpailevan yhtiön palvelukseen. KKO:n tuomiosta ilmenevillä perusteilla A ja B eivät kuitenkaan syyllistyneet yritysvakoiluun vaan heidät tuomittiin yrityssalaisuuden rikkomisen yrityksestä.*

Jos yrityssalaisuuksia sisältävät aineistot ovat ”työntekijän työhön kuuluvien tiedonhankkimisoikeuksien” piirissä, työntekijä on lähtökohtaisesti yritysvakoilusäännöksen soveltamisalan ulkopuolella, mutta toisaalta kuitenkin saatettavissa sen piiriin erikseen annettavalla kopiointikiellolla. Työnantajien tulisi erityisesti kiinnittää huomiota siihen, että työntekijöiden tekniset käyttöoikeudet on rajattu niin, että niiden piirissä on lähtökohtaisesti vain sellainen tieto, mitä asianomainen työntekijä tosiasiallisesti tarvitsee tai voi tarvita työtehtävissään. Hyvin hoidettuun tietohallintoon kuuluu yhtenä osana se, että kunkin työntekijän tekniset käyttöoikeudet on rajattu sen mukaan, millaisia tehtäviä työntekijän toimenkuvaan sisältyy.[1143] Ratkaisu korostaa hallinnollisena tietoturvatoimenpiteenä

[1141] Tässä tutkimuksessa pääsynhallinta sisältää myös identiteetinhallinnan (IAM – Identity and Access Management), koska tutkimuksen tehtävä ja rajaukset huomioon ottaen ei ole ollut tarvetta eritellä sitä omaksi osa-alueekseen.
[1142] Tähän riittäisi evidenssiksi esimerkiksi dokumentoitu peruste työsuhteesta tai sopimus suoritettavasta työstä. Myös Katakri 2020 T13 -vaatimuksessa on ohjeistettu, että organisaation tulisi muun muassa määritellä käsittelyoikeuksien menettelytapaohjeet sekä periaatteet, joiden pohjalta organisaation henkilöstö pääsee käsiksi turvallisuusluokiteltuihin tietoihin.
[1143] Nyblin 2016: 212–213

ohjeistuksien[1144] tärkeyttä, mutta myös teknisten keinojen käyttämistä liikesalaisuuksien suojaamiseksi.

Hyvien käytänteiden mukaisesti tietojenkäsittely-ympäristön toimijat tulisi tunnistaa esimerkiksi yksilöllisillä ja henkilökohtaisilla käyttäjätunnuksilla. Salasanoille tulisi olla riskitason mukaiset laatuvaatimukset[1145] ja vaihtovälit järjestelmässä. Mikäli tunnistus epäonnistuisi monta kertaa peräkkäin, järjestelmä lukittuisi. Myös järjestelmien ja sovellusten ylläpitotunnusten olisi suositeltavaa olla henkilökohtaisia. Tunnistus ja todennus tulisi järjestää luotettavalla menetelmällä. Esimerkiksi suositeltavaa on nykyään käyttää monivaiheista tunnistautumista (*Multi-factor Authentication, ”MFA”*) eli perinteisen käyttäjätunnus- ja salasanayhdistelmän lisäksi yksilöivää tietoa[1146] tilimurtojen estämiseksi (tai hidastamiseksi). MFA ei kaikissa tapauksissa kuitenkaan ole täysin varma keino estää tilimurtoja etenkin, esimerkiksi jos käyttäjä kalastelusivuilla syötettyään tunnuksensa rikolliselle kuittaa puhelimellaan MFA-kirjautumisen. Nykyisin kalastelutrendeissä on havaittavissa yhä enemmän AiTM-automatiikkaa (*adversary-in-the-middle*), joka mahdollistaa rikollisen ohittamaan monivaiheisen tunnistautumisen kaappaamalla AiTM-palvelimen kautta istuntoevästeen[1147].

Käytännössä edellä mainitut hyvät käytänteet ovat juuri niitä teknisiä ja organisatorisia toimia, joilla turvataan henkilötietoja ja toteutetaan tietosuojalainsäädännön periaatteita, kuten esimerkiksi käyttötarkoitussidonnaisuutta ja luottamuksellisuutta. Inhimillisten riskilähteiden vaikutusten pienentämiseksi tai ehkäisemiseksi olisi suositeltavaa käyttää sellaisia henkilötietojen hallintaan liittyviä

[1144] Ratkaisussa **KKO 2015:42** on vastaavanlaisesti tulkittu, että työntekijän irtisanoutumisen jälkeenkin lomalla tapahtunut tietokantojen kopiointi ei ollut yritysvakoilua, koska tietojen kopiointi on tapahtunut tiedonhankkimisoikeuksien rajoissa eikä se ole siten ollut yritysvakoilun (RL 30:4) tavoin oikeudetonta. Tässäkin tapauksessa henkilökunnan riittävillä ohjeistuksilla tällainen kopiointi olisi ollut ”oikeudetonta”. Esimerkiksi hyvien tietoturvakäytänteiden mukaisesti tiedon käsittelyn ohjeistuksissa tulisi mainita, että työntekeminen ja aineistojen käsittely on sallittua vain työnantajan laitteilla. (Vrt. Nyblin 2016, s. 214: Ratkaisua KKO 2013:20 voidaan tulkita siten, että työnantaja voi saattaa kaikki työntekijänsä yritysvakoilusäännöksen soveltamisalan piiriin vain antamalla heille kiellon kopioida aineistoja muille kuin työnantajan omistamille tai hallinnoimille tietovälineille.) Työntekijöiden ohjeistamisen ja vastuuttamisen tärkeyttä on käsitelty yksityiskohtaisemmin luvussa 3.5.7 (”Henkilöstöturvallisuus: työntekijöiden osaaminen ja vastuut”).

[1145] Toisin sanoen salasanojen tulee olla tarpeeksi ennalta-arvaamattomia, pitkiä ja monimutkaisia sisältäen erikoismerkkejä, numeroita sekä isoja ja pieniä kirjaimia. Tällä hetkellä Kyberturvallisuuskeskuksen suosittelema salasanapituus on vähintään 15 merkkiä. Usein salasanojen sijaan suositellaan käyttämään salalauseita, joiden myötä merkkipituusvaatimus on helpompi täyttää.

[1146] Monivaiheinen tunnistaminen perustuu kolmelle periaatteelle, joista 2/3 on toteudutettava riittävän tunnistuksen toteuttamiseksi: 1. Jotain mitä tiedän (esim. salasana); 2. jotakin mitä omistan (esim. matkapuhelimeen lähetettävä mobiilivarmenne); sekä 3. jotakin mitä olen (esim. sormenjälki). Ks. Traficom, kyberturvallisuuskeskus 2023c.

[1147] Ks. lisää AiTM-kalasteluista: Traficom, kyberturvallisuuskeskus 2024a.

järjestelmiä, joissa sovelletaan asianmukaisia pääsynvalvontamekanismeja ja joilla estetään inhimilliset virheet: esimerkiksi EDPB on todennut, että laskentataulukoiden ja muiden toimistoasiakirjojen käyttö asiakastietojen hallitsemiseksi ei ole asianmukaista[1148]. Kansallisen tietosuojalain 6 §:ssä edellytetään erityisiä henkilötietoryhmiä sallivan käsittelyn osalta tietoturvatoimenpiteenä rekisterinpitäjän ja käsittelijän sisäisiä toimenpiteitä, joilla estetään pääsy henkilötietoihin. Tällä tarkoitetaan käytännön tasolla pääsynhallinnan ja käyttöoikeuksien hallinnan kontrolleja. Tähän liittyen **apulaistietosuojavaltuutetun ratkaisussa 15.11.2022 (dnro 4022/171/22)** on ilmaistu kanta, jossa kannettavalle tietokoneelle tallennettujen erityisten henkilötietojen suojaaminen pelkällä salasanalla ei ole riittävä suojausmenetelmä:

> *Tapauksessa terveydenhuollon toimijan kannettava tietokone ja ulkoiset kiintolevyt päätyivät varkauden takia sivulliselle. Tietokone oli suljettu ja rekisterinpitäjän mukaan kirjautuminen tapahtui salasanalla. Lisäksi laukussa oli muutakin arkaluontoista, paperista dokumentaatiota. Varkaus oli tapahtunut, kun tietokonelaukku oli jätetty kadun varteen pysäköidyn auton viereen tavaroiden purkamisen ajaksi ilman valvontaa. Tietosuoja-asetuksen 32 artiklan mukaan rekisterinpitäjän tulee toteuttaa riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten henkilötietojen salaus, muun muassa estääkseen asiattomien pääsyn henkilötietoihin. Apulaistietosuojavaltuutetun mukaan ensinnäkin henkilötietoja sisältäviä paperiasiakirjoja tulisi käsitellä niin, että ne eivät ole ulkopuolisten saatavilla eli niitä ei tule viedä ulkotiloihin ilman asianmukaista suojaamista ja valvontaa. Toiseksi tietokoneen massamuisti tai sen sisältämät henkilötiedot eivät olleet salattuja, jolloin tietokoneessa vahvakaan salasanasuojaus ei ole riittävä keino suojata tietokoneelle tallennettuja henkilötietoja. Salasanasuojaus ei yksin estä pääsyä tietoihin, jos sivullinen saa fyysisen pääsyn tietokoneelle, jonka sisältämiä tietoja ei ole salattu.*

Tämä on mielenkiintoinen kannanotto tietoturvan kannalta, sillä ratkaisussa linjataan, että tietosuoja-asetuksen mukaista asianmukaista henkilötietojen suojaamista, etenkin erityisten henkilötietojen kohdalla, ei ole pelkkä salasanakirjautuminen laitteissa. Näin ollen salasanasuojaus yksistään on ollut selkeästi puutteellinen keino suojata tietokoneelle tallennettuja rekisteröityjen erityisiä henkilötietoja. Etenkin korkeariskiset henkilötiedot tulisi suojata riittävän vahvasti, esimerkiksi salausohjelmistoilla. Tietokoneiden kovalevyjen salaukseen on useissa organisaatioissa käytetty esimerkiksi BitLocker -suojausta. Tällainen apulaistietosuojavaltuutetun päätös on varsin ajankohtainen ja toivottu tietoturvan näkökulmasta

[1148] Euroopan tietosuojaneuvoston (EDPB) ohje 1/2021, s. 26–27.

ottaen huomioon etenkin nykyisin suositun hybridi- tai monipaikkatyöskentelyn riskit[1149].

Ratkaisun näkökulmasta on huomioitava kuitenkin se, kuinka monipuolista tietojen käsittely nykyisessä digitalisoituneessa verkkoyhteiskunnassa on[1150]. Luottamuksellista tietoa käsitellään herkästi monenlaisissa järjestelmissä ja palveluissa, mutta myös erilaisilla laitteilla. Esimerkiksi tietosuojavaltuutetun ratkaisusta johdettuna erityisten tai muuten luottamuksellisten tietojen käsittely ei ole lain vaatimalla tasolla suojattua, mikäli tietojen käsittely on mahdollista sellaisissa palveluissa, joissa on SSO (*Single Sign-On[1151]*) käytössä ja palvelua pystyy suoraan käyttämään mobiililaitteella ilman MFA-kuittausta. Tällöin esimerkiksi puhelimen varkaustapauksessa hyökkääjä pääsee käsiksi palveluun ja sen sisältämiin luottamuksellisiin tietoihin vain tietämällä puhelimen PIN-koodin tai suoraan, jos mobiililaitteen näytönlukitus ei ole päällä. Tietoturva- ja tietosuojariskien arvioinneissa tuleekin huomioida riskiperusteisesti riittävät pääsynhallinnan kontrollit eri laitteiden näkökulmasta. Myös laitteiden käyttökonteksti on huomioitava, sillä riskit ovat täysin eritasoisia sellaisissa mobiililaitteissa, jotka työnantaja on kustantanut työntekijälle sekä työ- että henkilökohtaiseen, vapaa-ajan käyttöön. Erityisen ongelmallisia ovat BYOD-laitteet (*Bring your own device),* jolloin työntekijät käyttävät töiden tekemiseen omia laitteitaan, joissa on alhaisempi tietoturvataso.

Tietosuojalainsäädännön ohella lainsäädännöstä löytyy myös muita pääsynhallinnan vaatimuksia, mutta ne ovat lokivaatimusten tavoin hajaantuneita eri säädöksiin. Esimerkiksi aikaisemmin käsitellyssä[1152] sähköisen viestinnän palveluista annetun lain 147 §:ssä edellytetään ennen välitystietojen käsittelyn aloittamista yhteisötilaajana toimivalta, esimerkiksi työnantajaorganisaatiolta, tietoturvatoimenpiteitä maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman käytön ehkäisemiseksi. Tähän kuuluu pääsyn rajoittaminen yhteisötilaajan viestintäverkkoon ja viestintäpalveluun. Samassa lain pykälässä säädetään myös vastaavasti liikesalaisuuksien paljastamisen ehkäisystä. Lain mukaan yhteisötilaajan on ennen välitystietojen käsittelyn aloittamista liikesalaisuuksien

[1149] Nykyään koronapandemian jälkeen on varsin yleistä, että työntekijät suosivat vieläkin etätyöskentelyä. Työnteosta onkin tullut monipuolisempaa ja on alettu puhumaan hybridityöskentelystä, joka yhdistää etä- ja lähityöskentelyä, taikka monipaikkaisesta työskentelystä, jossa työtä tehdään varsinaisten työpaikkojen lisäksi välillä esimerkiksi kotona, kahvilassa tai co-working-tiloissa. Etenkin julkisissa tiloissa työskentelyyn liittyy aina tietoturvariskejä. Ks. myös luku 4.3.4 (”Fyysinen tietoturvallisuus osana riskienhallintaa”).
[1150] Ks. pohdintaa myös luvusta 3.2.2 (”Henkilötietojen käsittely ja henkilörekisteri”).
[1151] SSO-ratkaisulla tarkoitetaan kertakirjautumista, jolla käyttäjät pääsevät turvallisesti kirjautumaan useisiin palveluihin yhdellä kirjautumissessiolla, jolloin erilaisia salasanoja ei tarvitse keksiä joka palveluun erikseen. Nykyisin monessa organisaatioissa pyritään ottamaan käyttöön SSO-ratkaisuja työntekijöiden salasana-ahdistuksen lieventämiseksi.
[1152] Ks. luku 3.5.5 (” Väärinkäytösten ehkäiseminen ja selvittäminen organisaatioissa”).

paljastamisen ehkäisemiseksi rajoitettava pääsyä liikesalaisuuksiin. Täten organisaatiossa tulisi käytännössä vain tiettyjä tehtäviä hoitavien käyttäjien päästä liikesalaisuuksiin käsiksi, jolloin pääsyä voidaan rajoittaa muun muassa tietohallinnollisin toimenpitein, kuten käyttäjätunnuksin ja salasanoin tai muuten käyttäjäoikeuksia hallinnoimalla[1153].

Lähes jokainen työnantajana toimiva organisaatio tarjoaa työntekijöilleen sähköpostin ja pikaviestintäsovelluksia työvälineiksi, joten kyseinen sähköisen viestinnän palvelulain 147 § koskee erittäin montaa yhteisötilaajaorganisaatiota. Matalan tietoturvan maturiteettitason omaaville organisaatioille kyseinen pykälä ei välttämättä ole kuitenkaan niin tavoitettava ja ymmärrettävä, koska kyseisen säädöksen tietoturvavaatimukset ikään kuin hukkuvat sen sisään eikä säädöksen nimi itsessään kuvaa riittävällä tasolla sitä, että se sisältää tärkeitä, huomioitavia tietoturvavaatimuksia organisaatioille. Esimerkiksi jo pelkästään käsitteenä yhteisötilaaja saattaa olla haasteellinen ymmärtää. Näillä perustein nykyinen organisaatioiden tietoturvan sääntelyjärjestelmä tarvitsisi selkeytystä, jotta se näyttäytyisi kohtuullisena ja oikeudenmukaisena myös sellaisille yrityksille, joilla ei välttämättä ole niin hyvää säädös- ja tietoturvaosaamista tai edes kunnollista tietohallintoa. Toki käytännesääntöjen kautta hyvät perustietoturvakäytänteet saattavat olla jalkautuneet paremmin. Korostettakoon kuitenkin sitä, että hyvä tietoturvan sääntelyjärjestelmä tulisi olla helposti tavoitettava ja ymmärrettävä kaikille. Näin suojattaisiin myös luonnollisten henkilöiden perusoikeuksia paremmin.

Pääsynhallinnan vaatimuksia löytyy myös viranomaisia koskevan tiedonhallintalain 16 §:stä. Säännöksessä on vähimmäisvaatimuksena esitetty, että käyttöoikeuksien on oltava määriteltyjä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina. Käytännön tasolla näin varmistetaan tarpeellinen tietoihin pääsy ja toisaalta estetään vanhentuneiden käyttöoikeuksien perusteella tiedonsaanti laajemmin kuin käyttäjän tehtävät edellyttävät[1154]. Lisäksi tiedonhallintalain 14 §:ssä on säädetty, että viranomaisen tiedonsiirto on järjestettävä niin, että salassa pidettävän tiedon vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään näitä salassa pidettäviä tietoja. Kyseisen 14 §:n 2 momentin mukaan käyttäjän tunnistamisesta yleisölle tarjottavissa digitaalisissa palveluissa säädetään digitaalisten palvelujen tarjoamisesta annetussa lain (306/2019) eli digipalvelulain 6 §:ssä. Käytännössä siis salassa pidettävän tiedon siirto viranomaisen digitaalisissa palveluissa vaatii vastaanottajan vahvaa sähköistä tunnistamista.

[1153] HE 48/2008 vp: 22.
[1154] Ks. yksityiskohtaisemmin Valtiovarainministeriön julkaisuja 2024:19, s. 37–38.

Pääsynhallintaan liittyvän sääntelyn osalta on relevanttia huomioida myös rikoslaki, vaikka kyseisessä laissa ei suoraan velvoitetakaan organisaatioita tekemään pääsynhallinnan toimenpiteitä tietojensa suojaamiseksi kuten sähköisen viestinnän palveluista annetussa laissa tai tiedonhallintalaissa. Kuitenkin esimerkiksi rikoslain mukaisen oikeudettoman tietojärjestelmään tunkeutumisen[1155] rangaistavuuden edellytyksenä on, että tietojärjestelmässä on tekniset turvallisuusjärjestelyt kunnossa. Tällöin kyse olisi tietomurrosta[1156]. Lain esitöissä mainitaan turvajärjestelynä jo pelkästään käyttäjätunnus, joka tietojärjestelmään pyrkivän on osattava päästäkseen käsiksi järjestelmän tietoihin. Rikoksen tunnusmerkistö täyttyy heti, kun tunnistuskontrolli on läpäisty.[1157] Menettelyä ei rangaista tietomurtona, jos asianosainen onnistuu pääsemään järjestelmään turvajärjestelyn epäkunnon vuoksi tai saatuaan luvallisesti käyttäjätunnuksen[1158]. Tunnusmerkistö tosin täyttyy, jos rikoksentekijä keksisi salasanan tai koodin sattumanvaraisesti, jos tekijän tarkoituksena on ollut tunkeutua tietojärjestelmään. Näin ollen rikoksen tunnusmerkistön kannalta ei ole merkitystä, miten asianosainen on saanut salasanan tai koodin tietoonsa, esimerkiksi tunnistautumistieto voi olla urkittu.[1159] Tämä korostaa sitä, että vaatimatonkin pääsynhallinnan turvakontrolli on hyvä olla, mutta vielä olennaisempaa on tietojen turvaamisen osalta se, että turvakontrolli toimii.

Tietomurron tunnusmerkistö täyttyy heti tunnistuskontrollin läpäisyn jälkeen eli jos turvajärjestely on monivaiheinen, rikoksen tunnusmerkistön täyttyminen edellyttää myös viimeisen vaiheen läpäisemistä[1160]. Myös tietomurron yritys on rangaistava, esimerkiksi mikäli asianomainen yrittää selvittää tietojärjestelmää suojaavan käyttäjätunnuksen tai murtaa muun turvajärjestelyn. Tämä kuitenkin

---

[1155] Ks. Korpisaari, Pitkänen & Warma-Lehtinen 2022: 656; Pitkänen, Tiilikka & Warma 2013: 233. Oikeudettomassa tietojärjestelmään tunkeutumisessa voi olla esimerkiksi kysymys salasana murtamalla tapahtuneesta oikeudettomasta tunkeutumisesta toisen tietokoneella oleviin tietoihin.

[1156] Rikoslain 38 luvun 8 §:n mukaan tietomurrosta voidaan tuomita sakkoon tai vankeuteen enintään kahdeksi vuodeksi se, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka tunkeutuu sellaisen järjestelmän erikseen suojattuun osaan. Kyseisen lain toisen momentin mukaan tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta 1) teknisen erikoislaitteen avulla tai 2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta.

[1157] HE 94/1993 vp: 155–156.

[1158] Pihlajamäki 2004: 123; Korpisaari, Pitkänen & Warma-Lehtinen 2022: 656; Melander & Rautio 2022: 1306; HE 94/1993 vp: 155–156.

[1159] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 656–657; Pitkänen, Tiilikka & Warma 2013: 233.

[1160] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 657; Melander & Rautio 2022: 1306; HE 94/1993 vp: 156.

edellyttää, että menettelyn tarkoituksena on ollut oikeudeton tunkeutuminen tietojärjestelmään. Yrityksen rangaistavuuden tarkoituksena on ollut helpottaa puuttumista järjestelmien käyttäjätunnusten tai muiden turvajärjestelyjen järjestelmälliseen selvittämiseen.[1161] Tällaista käyttäjätunnusten järjestelmällistä selvittämistä on esimerkiksi rikollisten tekemät kalastelusivustot, joissa tarkoituksena on huijata käyttäjää syöttämään tunnuksensa aidonnäköisille sivustoille ja niitä hyödyntäen kirjautumaan esimerkiksi käyttäjän organisaatiotilille tai verkkopankkiin.

Tietomurtosäännöksiä sovelletaan toissijaisesti[1162] eli ensisijaisesti sovelletaan esimerkiksi säännöksiä liittyen viestintäsalaisuuden loukkaukseen, tietojärjestelmään tai siihen tallennettuun tietoon kohdistuvaan vahingontekoon sekä yritysvakoilua varten tapahtuvaan tietojärjestelmään tunkeutumiseen[1163]. Myös esimerkiksi valtiollisesta (kyber)vakoilusta voidaan tuomita jopa 10 vuodeksi vankeuteen tai törkeänä muotona elinkautiseen, jolloin normikollisiossa toissijaisuuslausekkeen puuttuessakin on selvää, että törkeä tietomurto väistyisi vakoilusyytteen tieltä. Lisäksi tietomurto voidaan nähdä vakoilussa valmisteluluontoisena tekona, jossa vakoilu kattaa pidemmälle edenneenä kaiken vääryyden, joka sisältyy tietomurtoon.[1164]

Siinä missä tietomurron tunnusmerkit sisältävät oikeudettoman tietojärjestelmään tunkeutumisen, myös viestintäsalaisuuden loukkaus [1165] sisältää

[1161] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 658–659; Melander & Rautio 2022: 1307; HE 94/1993 vp: 156; Pihlajamäki 2004: 124; Pitkänen, Tiilikka & Warma 2013: 233.

[1162] Tietomurtoa voidaan pitää valmisteluluontoisena tekona. Erityinen tekotapa, suojattava oikeushyvä, säännöksen luonne erityissäännöksenä tai valmisteluluonteisten tekojen väistymistä koskeva periaate johtaa siihen, että muu kriminalisointi tulee sovellettavaksi. Tietomurtoa koskevan pykälän osalta on lisäksi huomattava sen sisältämä toissijaisuuslauseke. Ks. HE 232/2014 vp, s. 11–12.

[1163] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 660; Pitkänen, Tiilikka & Warma 2013: 236; HE 94/1993 vp: 156.
Yritysvakoilua koskevassa säännöksessä tietojärjestelmän tulisi olla ulkopuolisilta suojattu, jolloin tunkeutuminen edellyttäisi jonkin turvajärjestelyn murtamista tai käyttäjäkontrollin läpäisemistä. Ks. HE 66/1988 vp, s. 83. Oikeuskirjallisuudessa (Viljanen 2023a: 734) on kuitenkin todettu, että yritysvakoilusäännös on tulkinnanvarainen sen osalta, milloin paikka tai tietojärjestelmä voidaan katsoa olevan ulkopuolisilta suljettu. Esimerkkinä on tulkittu, että mikäli organisaatio on aidattu ja portit lukittu, mutta oikeudettomasti aidan yli kiipeävä henkilö tunkeutuessaan suljettuun paikkaan ja kopioidessaan salasanasuojaamattomista tietokoneista liikesalaisuuksia, syyllistyy hän todennäköisesti yritysvakoiluun.

[1164] Lohse 2015: 765; HE 232/2014 vp: 12.
Vakoilu on siirtynyt merkittävästi tietoverkkoihin, sillä kybervakoilu on esimerkiksi ulkomaisille tiedustelupalveluille kustannustehokas ja lähes riskitön tapa hankkia tietoa kohdemaan päätöksenteosta ja yrityksistä. Ks. Lohse, Honkanen & Meriniemi 2019, s. 34.

[1165] Rikoslain 38 luvun 3 §:n mukaan viestintäsalaisuuden loukkauksesta voidaan tuomita sakkoon tai enintään kahdeksi vuodeksi vankeuteen henkilö, joka oikeudettomasti 1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii

tunnusmerkistössä oikeudettoman suojauksen murron. Viestintäsalaisuuden loukkauksen osalta on täsmennetty lain esitöissä, että rangaistavuuden edellytyksenä on se, että sähköinen viesti on teknisin keinoin suojattu ulkopuolisilta ja että tiedon hankkiminen viestistä tapahtuu tämän suojaus murtaen. Suojauksen murtaminen voisi tapahtua vastaavalla tavalla kuin tietomurtoa on kuvattu rikoslain 38 luvun 8 §:n 1 momentissa.[1166] Tämän tietomurtoa koskevan 8 §:n 1 momentin mukaan tietomurrosta tuomitaan se, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään. Keskeistä viestintäsalaisuuden loukkauksessa on kuitenkin kajoaminen viestintään eli henkilö avaa toiselle kuuluvan suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuolisesta suojatusta viestistä.

Esimerkiksi ratkaisussa **KKO 2022:32** viestintäsalaisuuden loukkauksen tunnusmerkistö on täyttynyt suojauksen murtamisen suhteen samoin kuin tietomurrosta säädetyn rikoslain 38 luvun 8 §:n 1 momentissa eli silloin, kun toiselle kuuluvaa käyttäjätunnusta on käytetty luvatta:

> *Työnantajan edustaja A syyllistyi viestintäsalaisuuden loukkaukseen, kun hän oli B:n työsuhteen päättymisen jälkeen pitänyt auki tämän työsähköpostiosoitetta ja antanut muiden työntekijöiden tehtäväksi seurata sähköpostia.*

KKO:n ratkaisun mukaan toiselle kuuluvaa sähköpostiosoitetta on pidettävä käyttäjätunnuksena. Käyttäjätunnuksen luvaton käyttäminen on jo itsessään riittävää, sillä se mahdollistaa tiedon hankkimisen suojatusta viestistä, jolloin esimerkiksi erillisen salasanan kirjaamistointa ei tarvita tunnusmerkistön täyttymiseksi. Lisäksi B ei ollut antanut A:lle työelämän tietosuojalain mukaista suostumusta työsähköpostiosoitteen käyttöön työsuhteen päättymisen jälkeen. KKO katsoi myös, että rikoksen tunnusmerkistön täyttymisen kannalta ei ole kriittistä sähköisen viestin avaaminen, vaan riittävää on jo viestin otsikkoa tai osapuolia koskevan tiedon hankkiminen.[1167] KKO:n lavea tulkinta viestintäsalaisuuden loukkauksen tunnusmerkistön täyttymisen suhteen on katsottu olevan kritiikille altis[1168]. KKO:n

---

tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka; 2) hankkii tiedon televerkossa tai tietojärjestelmässä välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta. Myös yritys on rangaistava. Rikoslain 38 luvun 4 §:n mukaan törkeä viestintäsalaisuuden rikos voi tulla kyseeseen esimerkiksi silloin, kun rikoksen kohteena on ollut erityisen luottamuksellinen viesti taikka teko huomattavasti loukkaa yksityisyyden suojaa.

[1166] HE 94/1993 vp: 149.

[1167] KKO 2022:32 kohta 8 ja 11–14.

[1168] Luoto 2022: KKO:n ratkaisut kommentein 2022:I.

tulkinta on kuitenkin varsin paikkaansa pitävä, sillä usein esimerkiksi jo otsikkotasolla viesteistä on mahdollista saada paljon tietoa myös viestin sisällöstä. Sama koskee osapuolia koskevia tietoja eli esimerkiksi lähettäjäosoitetta, jossa sähköpostiosoite voi koostua nimen lisäksi organisaation nimestä tai tunnuksesta.

NIS 2 -direktiivin myötä pääsynhallinnan vaatimukset parantuvat kansallisella tasolla. Esimerkiksi 21 artiklan kyberturvallisuusriskien hallintatoimenpiteiden osaksi kuuluu pääsynhallintaperiaatteiden ja kyberhygieniakäytäntöjen käyttöönotto. Direktiivin mukaan kyberhygieniaperiaatteisiin kuuluu perustason käytännöt, kuten salasanojen vaihtaminen ja käyttöoikeuksia edellyttävien tilien rajoittaminen sekä identiteetin- ja pääsynhallinta.[1169] Huomioitava kuitenkin on, että NIS 2 -direktiivin mukaiset pääsynhallinnan vaatimukset koskevat vain kriittisiä toimialoja.

Yhtä lailla esimerkiksi tulevan EU-lainsäädännön ehdotus kyberkestävyyssäädökseksi (CRA) sisältää luonnosliitteessä I pääsynhallintaan liittyvän vaatimuksen digitaalisia elementtejä sisältävälle tuotteelle: liitteen I kohdan 3 b mukaan digitaalisia elementtejä sisältävässä tuotteessa, esimerkiksi ohjelmistossa, tulee soveltuvin osin olla asianmukaiset valvontamekanismit esimerkiksi käyttäjien tunnistamista ja käyttöoikeuksien hallintaa varten, jotta luvaton käyttö estyy. Tämä vaatimus on tärkeä lisäys pääsynhallintaa koskevaan lainsäädäntöön, mutta se kohdistuu lähinnä tuotteisiin eikä organisaatioiden hyvien käytänteiden mukaisiin vähimmäisvaatimuksiin. Näin ollen se ei poista kaikkiin organisaatioihin kohdistuvaa vähimmäissääntelyn tarvetta pääsynhallinnan osalta.

Yhteenvetona todettakoon, että nykyisen tietoturvan sääntelyjärjestelmän vaatimukset pääsynhallinnan osalta ovat edellisessä alaluvussa kuvatun lokisääntelyn tavoin kovin hajanaisia. NIS 2 -direktiivin implementoinnin jälkeen pääsynhallinnan vaatimuksia tulee esiintymään kansallisessa lainsäädännössä tietosuojalain, sähköisen viestinnän palvelulain sekä tiedonhallintalain lisäksi myös kyberturvallisuuslaissa, jolla toimenpannaan NIS 2 -direktiivin vaatimuksia keskeisille ja tärkeille toimijoille. Useaan säädökseen hajaantuneet pääsynhallinnan vaatimukset eivät kuitenkaan riittävällä tasolla kuvaa sitä, kuinka tärkeästä ja perustavanlaatuisesta kontrollista on kyse tietojen turvaamisen osalta. Lähes joka organisaatiossa on vähintään jotain pääsynhallinnalla suojattavia tietoja, esimerkiksi henkilötietoja, liikesalaisuuksia, lokitietoja ja varmuuskopioita. Näin ollen lainsäädännössä tulisi korostaa kattavammin riskiperustaisia pääsynhallinnan kontrolleja henkilötietojen ja muiden luottamuksellisten tietojen suojaamiseksi sekä järjestelmien ja palveluiden luvattoman käytön ehkäisemiseksi. Riskiperusteisesti arvioitavat riittävät pääsynhallinnan kontrollit tulisi huomioida myös eri laitteiden

[1169] Ks. myös NIS 2 -direktiivin kohdat 49 ja 89.

näkökulmasta, sillä nykyisessä digitalisoituneessa verkkoyhteiskunnassa tietojen käsittely on laajaa ja monipuolista. Esimerkiksi rikoslaissa ilmaistun oikeudettoman tietojärjestelmään tunkeutumisen rangaistavuuden edellytyksenä on se, että tietojärjestelmässä on tekniset turvallisuusjärjestelyt kunnossa. Tämä edellytys ei välttämättä täyty ja menettelyä ei rangaista tietomurtona, jos asianosainen pääsee järjestelmän tietoihin käsiksi puutteellisen turvajärjestelyn vuoksi. Esimerkiksi tällainen tapaus voisi tulla kyseeseen tilanteessa, jossa työpuhelimessa ei ole automaattista näytönlukitusta päällä, puhelimessa oleviin sovelluksiin ja työtiedostoihin pääsee SSO:n avulla käsiksi suoraan ja tämä puhelin joutuu rikollisen käsiin. Pääsyn- ja käyttöoikeuksienhallinnan velvoitteet tulisi ulottaa kaikkiin toimijoihin niin sanottuna vähimmäisvaatimuksena, koska se parantaisi myös organisaatioiden sidosryhmissä esiintyvien henkilöiden perusoikeuksia.

Tämä näkökulma huomioon ottaen, NIS 2 -direktiivin implementointi kansalliseen lainsäädäntöön kyberturvallisuuslailla ei yhtenäistä ja kehitä pääsynhallinnan sääntelyä riittävällä tasolla, sillä useita toimijoita jätetään sääntelyn ulkopuolelle.

4.4.4 Varmuuskopioinnin ja toipumisen vaatimukset sääntelyjärjestelmässä

Osana järjestelmien suunnittelua tulee huomioida myös järjestelmien toipuminen[1170] ja niiden tietosisällön palauttaminen varmuuskopioista[1171], sillä toipuminen ja palautuminen ovat olennaisia toiminnan jatkuvuuden kannalta. Lisäksi suunnitteluvaiheessa tulisi huomioida myös varmuuskopioiden elinkaarisuunnittelu eli esimerkiksi, kuinka kauan varmuuskopioita säilytetään ennen niiden tuhoamista.

Vain ajan tasalla olevat varmuuskopiot suojaavat inhimillisiltä virheiltä ja kiristyshaittaohjelmilta[1172]. Hyvien käytäntöjen mukaisesti varmuuskopiot tulee suojata koko elinkaaren ajalta ja varmuuskopioiden palautusta tulee testata säännöllisesti dokumentoidun palautusprosessin avulla. Suositeltavaa olisi, että varmistusten taajuus olisi mitoitettu tiedon kriittisyyteen nähden ja selvitetty, kuinka paljon tietoa voidaan menettää (*RPO, Recovery Point Objective)*. Lisäksi suositeltavaa olisi

[1170] Valtiovarainministeriön julkaisuja 22/2017b: 5; VAHTI 2/2016: 24; Andreasson & Koivisto 2013: 100–101. Järjestelmähäiriöistä toipumisen tueksi laaditaan toipumissuunnitelma. Ne ovat yleensä järjestelmäkohtaisia ja niissä kuvataan järjestelmän toipuminen häiriöstä normaalitoimintaan.
[1171] Varmuuskopio tarkoittaa tiedoston, ohjelman tai taltion kopiota, joka on tarkoitettu käytettäväksi, jos alkuperäinen menetetään vian tai vahingon takia. Ks. ATK-sanakirja 1 2008, s. 376.
[1172] Järvinen 2022b: 43.

mitoittaa palautumisprosessin nopeus toimintavaatimuksiin nähden ja selvittää, kuinka kauan palautuminen saa kestää (*RTO, Recovery Time Objective*).

Varmuuskopiot voivat olla yksinkertaisia kopioita tiedostoista, tietokantadumppeja taikka kokonaisia järjestelmäkuvia tai snapshotteja riippuen järjestelmän kriittisyydestä. Niitä voi tallentaa paikalliselle tallennusvälineelle tai esimerkiksi pilveen *"off-site"*. Varmuuskopiointi voidaan suorittaa täydellisenä *"full"* varmuuskopiona, inkrementaalisena[1173] taikka differentiaalisena[1174].

Esimerkiksi tietokannoista olisi suotava tehdä myös varmuuskopio fyysiselle tallennusvälineelle, sillä pilvipalvelut eivät ole täysin varmoja varastoja varmuuskopioille. Lisäksi varmuuskopiot tulisi säilyttää huolellisesti, sillä ne turvaavat tiedon saatavuuden (käytettävyyden), mutta voivat olla riski tiedon luottamuksellisuudelle. Näin ollen esimerkiksi, mikäli fyysiset tallenteet eivät ole salattuja, niitä tulisi säilyttää lukitussa, paloturvallisessa kaapissa. Jos varmuuskopiot ovat omassa verkossa tai pilvessä, ne tulisi suojata haitta- tai kiristysohjelmien varalta niin, ettei edes ylläpito omilla tunnuksillaan pääse niitä poistamaan.[1175]

Organisaation tulisi järjestää tietokantojen ja käyttäjien työtiedostojen varmuuskopiointi vaivattomasti tai kokonaan automaattisesti[1176]. Varmuuskopiointia tehdään yleensä isommissa organisaatioissa säännöllisesti, tietyissä aikaikkunoissa, riippuen järjestelmien tai niissä olevan tiedon kriittisyydestä. Vaikka varmuuskopioita käytetään ensisijaisesti nopeaan operatiiviseen palautukseen ottamalla jaksottaisia kuvia aktiivisista tiedoista, joita säilytetään vain muutama päivä tai viikko, arkistot on yleensä suunniteltu tarjoamaan jatkuva ja nopea pääsy yritystietoihin vuosien taakse tallentamalla versioita tiedoista, jotka eivät ole enää käytössä, eivät muutu usein ja eikä niitä tarvita säännöllisesti.[1177]

Suoraan jäsenmaita velvoittavassa tietosuoja-asetuksen 32 artiklassa on teknisiin ja organisatorisiin toimenpiteisiin lueteltu vaatimukseksi muun muassa *teknisen tai fyysisen vian sattuessa kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin*, mikä viittaa varmuuskopiointiin[1178]. Samaa on todettu myös

[1173] Inkrementaalinen varmuuskopio sisältää edellisen varmuuskopioinnin jälkeen muuttuneet tiedot.
[1174] Differentiaalinen varmuuskopio sisältää vain edellisen "full" eli täydellisen varmuuskopioinnin jälkeen muuttuneet tiedot.
[1175] Järvinen 2022b: 43–45.
[1176] Ibid.: 42.
[1177] Alepis, Michota, Patsakis, Pocs & Politou 2018: 1249–1250.
[1178] Ks. myös tietosuojalain 6 § erityisiä henkilötietoryhmiä koskevasta käsittelystä ja siihen liittyvistä suojatoimenpiteistä. Nämä sisältävät mm. suojatoimenpiteet, joilla käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, ja näihin mukaan luetaan myös kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa.

apulaistietosuojavaltuutetun päätöksessä 7.12.2021 (dnro 1150/161/2021) koskien Vastaamon tietomurtoa:

> *Tietosuoja-asetuksen 32 artiklan 1 kohdan c alakohdan mukaan eräänä henkilötietojen asianmukaisen turvallisuuden varmistavana toimenpiteenä voidaan pitää kykyä palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa. Tietojen saatavuuden ja tietoihin pääsyn palauttaminen edellyttävät, että henkilötiedoista ja niiden käsittelystä tallennetaan riittävät varmuuskopiot.*

Vastaamon tapauksessa todettiin olevan monta ongelmaa varmuuskopioihin liittyen. Esimerkiksi tietomurron yhteydessä hävinneitä tietoja jouduttiin palauttamaan puoliautomatisoidusti käsittelemällä, koska varmuuskopiointi- ja lokiasetukset ovat olleet varmuuskopiointisuunnitelman vastaiset. Myös monet dokumentit, kuten vaikutustenarviointi, omavalvontasuunnitelma ja tietosuojaseloste, olivat puutteellisia tiedoiltaan varmuuskopioinnin osalta. Henkilötietojen käsittelyä, jossa rekisterinpitäjä ei toteuta toimenpiteitä, joiden avulla se kykenee muun muassa huolehtimaan riittävistä varmuuskopiointiin ja lokitietojen säilyttämiseen liittyvistä menettelytavoista tietojen saatavuuden ja tietoihin pääsyn palauttamiseksi, ei voida pitää sellaisena henkilötietojen käsittelynä, jossa henkilötiedot olisi tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdassa edellyttämällä tavalla suojattu muun muassa vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla.[1179] Näillä perusteilla voi todeta, että kaikkien henkilötietojen käsittelyä tekevien organisaatioiden tulisi suojata henkilötiedot vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta huolehtimalla riittävästä varmuuskopioinnista. Asia ei ole kuitenkaan niin yksiselitteinen: organisaatioissa on erilaisia järjestelmiä, joissa on eri tasoista luottamuksellista tietoa, jotkut järjestelmät eivät välttämättä edes ole niin kriittisiä tai niiden fokus ei ole henkilötietojen käsittelyssä. Varmuuskopioinnin kriittisyys on pitkälti kiinni myös järjestelmän kriittisyysarviosta. Vastaamon tapauksessa koko organisaation tiedon käsittely perustui käytännössä luottamuksellisten ja erityisesti suojattavien henkilötietojen käsittelyyn.

Samalla kun tietosuoja-asetuksen 32 artiklan tekniset ja organisatoriset toimenpiteet kannustavat varmuuskopiointiin, tietosuoja-asetuksen *Right to be forgotten* -vaatimus eli *oikeus tulla unohdetuksi* herättää kysymyksiä varmuuskopioiden tietosisällöstä ja henkilötietojen säilytysajoista. Tietosuoja-asetuksen 17 artiklan

[1179] TSV 7.12.2021, dnro 1150/161/2021. Ks. myös tietomurrosta annettu ratkaisu Länsi-Uudenmaan käräjäoikeus 30.4.2024 R 23/3965.

mukaan oikeus tulla unohdetuksi tarkoittaa oikeutta tietojen poistamiseen[1180] rekisteristä ilman aiheetonta viivästystä, mikäli esimerkiksi henkilötietoja ei enää tarvita alkuperäiseen tarkoitukseen nähden, rekisteröity peruuttaa suostumuksensa taikka vastustaa käsittelyä eikä käsittelyyn ole tällöin laillista perustetta. Lisäksi tietosuoja-asetuksen säilytyksen rajoittamisen periaatteen mukaan, henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn toteuttamista varten. Pidempi aikainen säilytys on sallittua, jos kyseessä on yleisen edun mukainen arkistointi taikka tieteellinen, historiallinen tai tilastollinen tutkimustarkoitus ja tietosuoja-asetuksessa vaaditut tekniset ja organisatoriset vaatimukset on pantu täytäntöön. Näin ollen säilytysaika on hyvinkin sidoksissa myös käyttötarkoitussidonnaisuuden perusteeseen.

Kun henkilötietoja ei enää tarvita, ne ovat poistettava tai anonymisoitava[1181]. Arkistoinnin osalta huomioitava on, että se kattaa muutakin aineiston käsittelyä kuin säilyttämistä, kuten esimerkiksi aineistojen järjestämistä ja tietojen yhdistelyä. Näin ollen arkistointitarkoituksen luonteeseen kuulunee passiivinen käsittely, kuten säilytyksen lisäksi tietojen löytämisen edellyttämä järjesteleminen. Jatkuva tai tilapäinen aktiivinen käsittely on kuitenkin muuta toimintaa kuin arkistointia.[1182] Huomioitava onkin, että varmuuskopiointi ja arkistointi ovat kaksi eri asiaa, vaikka usein varmuuskopiointien yhteydessä puhutaan varmuuskopioiden arkistoinnista tai varmuuskopioarkistoista. Varmuuskopioinnin perimmäinen tarkoitus on mahdollistaa tietojen nopea palauttaminen tarvittaessa, kun taas arkistointi tähtää pitkäaikaiseen säilyttämiseen. Varmuuskopiointia ei voi myöskään yhdistää tietosuoja-asetuksen mukaiseen yleisen edun mukaiseen arkistointiin, jolloin pidempi säilytysaika on sallittua.

Tietosuojalainsäädännön *oikeus tulla unohdetuksi* -vaatimusta on käytännön tasolla kritisoitu siitä, että tietosuoja-asetuksen vaatimukset ei tulisi koskea varmuuskopioita ja niihin liittyviä arkistoja. Kritiikki johtuu siitä, että henkilötietojen etsiminen ja poistaminen varmuuskopioista olisi kallista, aikaa vievää, vaikeaa ellei jopa mahdotonta. Varmuuskopioiden datamuutokset todennäköisesti vaikuttaisivat koko varmuuskopioon, joka yleisten standardien mukaisesti edustaa ainutlaatuista esiintymää tietyllä aikaleimalla. Varmuuskopioiden ensisijaisena tavoitteena on ennemminkin nopea palautus, kuin tietojen säilytys, jolloin niitä

[1180] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 247. Tietojen poistamisen osalta ei ole riittävää siirtää tietoja roskakoriin, josta ne on helppo hakea takaisin. Tiedot on poistettava niin, että rekisterinpitäjä, henkilötietojen käsittelijä tai kolmas puoli eivät saa niitä enää käsiinsä. Tällöin poistotekniikalla ei ole merkitystä.
[1181] Korpisaari & Toikkanen 2020: 476.
[1182] HE 9/2018 vp: 82; Korpisaari, Pitkänen & Warma-Lehtinen 2022: 128–129

tulisi käsitellä vain harvoin eli esimerkiksi silloin, kun asiat menevät pieleen.[1183] Kritiikki on aiheellista. Huomioitava on myös se, että erityisesti kriittisten järjestelmien varmuuskopioiden palautusta tulee myös aika ajoin hyvien käytänteiden mukaisesti testata, jotta asioiden mennessä pieleen ei tulisi yllätyksiä.

Oikeuskirjallisuudessa on katsottu, että tietosuoja-asetuksessa ei ole poikkeusta *oikeus tulla unohdetuksi* -vaatimukselle. Näin ollen onkin ristiriitaista poistaa dataa varmuuskopioarkistoista, jotka on luotu alun perin suojaamaan täsmällisesti tiettyjä tietoja tiettynä ajankohtana. Se ei ole myöskään yksinkertaista huomioon ottaen, että varmuuskopiot voivat sijaita erilaisilla välineillä, eri lokaatioissa ja ne sisältävät runsaasti dataa. Ristiriita ilmenee myös yleisimpien hyviä käytänteitä ilmentävien standardien ja ohjeistuksien kohdalla, jolloin nämä pitäisi kritiikin mukaan päivittää vastaamaan lainsäädäntöä.[1184] Esitetty kritiikki huomioon ottaen mielestäni lainsäädännön kehitystyössä ja lain tulkinnassa tulisi nimenomaan tukeutua enemmän hyviin käytänteisiin, sillä ne ovat nimensä mukaisesti hyväksi todettu ja toteutuskelpoisia. Toki hyviä käytänteitä ilmentävät standardit ja ohjeistukset eivät ole todellisesti hyviä, mikäli ne rikkovat yksilöiden oikeuksia. Toisesta näkökulmasta varmuuskopioinnilla nimenomaan parannetaan tietoturvaa ja mahdollistetaan siten myös muita yksilöiden oikeuksia, joten aivan mustavalkoisesti *oikeus tulla unohdetuksi* -periaatteen pohjalta ei ole syytä lähteä muuttamaan hyvien käytänteiden mukaisia standardeja ja ohjeistuksia.

Lisäksi *oikeus tulla unohdetuksi* -periaatteen osalta on huomioitava tietosuoja-asetuksen 17 artiklan 2 momentti. Tämän mukaan rekisterinpitäjän velvollisuuteen poistaa tiedot liittyy myös kohtuullisesti toteutettavat toimenpiteet, joissa tulee huomioida käytettävissä oleva teknologia ja toteuttamiskustannukset. Henkilötietojen etsimistä ja poistoa varmuuskopioista ei todennäköisesti voida katsoa sen monimutkaisuudesta johtuen ainakaan edellä kuvaillun momentin mukaisesti kohtuulliseksi toimenpiteeksi, joten tähän vedoten varmuuskopioihin kajoaminen ei olisi tarpeellista.

Rekisteröidyn oikeudet eivät myöskään ole absoluuttisia, eli niin kauan kuin rekisterinpitäjällä on kumoava peruste käsitellä tietoa, rekisteröity ei voi vaatia tietojensa unohtamista. Tästä esimerkkinä oikeudellisen vaateen laatiminen, esittäminen tai puolustaminen. Tietosuoja-asetuksessa on myös mainittu, että rekisteröidyn oikeuksia voidaan tietyissä tapauksissa myös rajoittaa lainsäädäntötoimenpiteillä. Rajoituksen on kuitenkin noudatettava keskeisiltä osin perusoikeuksia ja – vapauksia sekä rajoituksen on myös oltava oikeasuhteinen ja välttämätön toimenpide, jotta yhteiskunnassa voitaisiin taata muun muassa yleinen ja kansallinen

[1183] Alepis, Michota, Patsakis, Pocs & Politou 2018: 1249, 1251–1253.
[1184] Alepis, Michota, Patsakis, Pocs & Politou 2018: 1249, 1251–1253.

turvallisuus sekä puolustus, rikosten ennaltaehkäiseminen ja tutkinta, rikosten paljastaminen ja niihin liittyvät syytetoimet sekä seuraamusten täytäntöönpano, oikeudellisen riippumattomuuden ja oikeudellisten menettelyjen suojelu, muut asetuksessa tarkemmin määriteltyjen julkiseen etuun liittyvät tärkeät tavoitteet sekä rekisteröidyn suojelu tai muiden oikeuksien ja vapauksien suojelu.

Yhden ihmisen henkilötietojen poistaminen varmuuskopioista ei välttämättä ole mahdollista ilman, että samalla vaarannetaan muiden ihmisten henkilötietojen varmuuskopiot. Näin ollen punnitsemalla eri henkilöiden etuja voidaan päätellä, ettei varmuuskopioita voida lähteä muuttamaan tai poistamaan, koska siitä aiheutuisi muiden henkilöiden oikeuksille ja vapauksille vielä suurempi riski kuin yhden rekisteröidyn unohdetuksi tulo -oikeuden rajoittamisesta.[1185]

Oleellista on myös varmistua siitä, etteivät käytöstä poistetut tiedot koskaan palaudu käyttöön varmuuskopioilta, josta niitä ei ole erikseen poistettu. Rekisterinpitäjän tulee esimerkiksi kirjata erikseen lokitiedosto poistetuista tiedoista ja huolehtia myöhemmin, että mahdollisen palautuksen yhteydessä lokiin kirjatut poistamiset toistetaan varmuuskopiosta palautettaville tiedoille ennen niiden käyttöönottoa.[1186] Tällainen tehostettu prosessisuositus johtuu siitä, että varmuuskopioiden palauttamisen yhteydessä henkilötietojen käsittelyn tietojen minimoinnin ja käyttötarkoitussidonnaisuuden periaatteiden osalta on ristiriitaista, jos palautettu varmuuskopiokanta sisältää vanhoja, tarpeettomia henkilötietoja. Riippuen tietokannasta, vanhentuneiden tietojen poistaminen voi olla kuitenkin kovinkin työlästä.

Tietosuoja-asetusta säädettäessä on pyritty teknologianeutraalisuuteen, jotta tietosuoja-asetus sopeutuisi teknisiin innovaatioihin mahdollisimman nopeasti. Tässäkin kohtaa nousee tosin jälleen ongelmaksi teknologianeutraalisuuden yleinen heikkous: lainsäädännön velvoite jää hyvinkin tulkinnanvaraiseksi. Loppujen lopuksi kuitenkin pääasia on, että henkilötietoja suojataan asianmukaisesti. Henkilötietojen suojaamisen lisäksi varmuuskopioimisella suojataan myös muita tärkeitä organisaation tietoja. Varmuuskopiot ovatkin erittäin oleellinen osa organisaation tietoturvaa ja toiminnan jatkuvuutta.

Tietosuojalainsäädäntöä lukuun ottamatta kansallisessa lainsäädännössä varmuuskopioinnin vaatimukset ovat olleet varsin puutteellisia. Kuitenkin varautumiseen liittyvässä lainsäädännössä velvoitteet toiminnan jatkuvuuden

[1185] Korpisaari, Pitkänen & Warma-Lehtinen 2022: 248.
[1186] Ibid: 248.

varmistamiselle sekä normaaliolojen häiriötilanteisiin[1187] varautumiselle sisältävät oletusarvoisesti hyvien tietoturvallisten käytänteiden mukaisesti varmuuskopioinnin, sillä varmuuskopiointi on oleellinen osa jatkuvuuden varmistamista ja etenkin häiriöistä toipumista.

NIS 2 -direktiivin myötä kansalliset tietoturvavaatimukset paranevat myös varmuuskopioinnin osalta: NIS 2 -direktiivin 21 artiklan 2 c kohdan kyberturvallisuusriskien hallintatoimenpiteisiin on sisällytetty *"toiminnan jatkuvuudenhallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu"*. Lisäksi NIS 2 -direktiivissä varmuuskopiointi on myös katsottu osaksi kyberhygieniaperiaatteiden perustason käytäntöjä[1188]. NIS 2 -direktiivissä ei sen sijaan oteta kantaa muihin hyviin käytänteisiin liittyen varmuuskopiointiin, esimerkiksi säännölliseen varmuuskopioista palautumisen testauksiin kriittisten järjestelmien osalta.

Yhteenvetona voidaan todeta, että järjestelmien toipuminen häiriöistä (mukaan lukien kyberhyökkäykset) ja niiden tietosisällön palauttaminen varmuuskopioista ovat olennaisia toimia organisaation palveluiden jatkuvuuden kannalta. Nämä ovat myös tärkeitä toimia rekisteröityjen oikeuksien kannalta, sillä tällöin tietojen saatavuus ja henkilöiden pääsy tietoihin on varmistettu. Näin ollen järjestelmien toipuminen ja palauttaminen varmuuskopioista ovat osa henkilötietojen asianmukaista turvallisuutta varmistavia toimenpiteitä. Tietosuojan näkökulmasta eräänlainen ristiriita varmuuskopioiden osalta syntyy kuitenkin *oikeus tulla unohdetuksi* -periaatteesta, jota on käytännössä perusteetonta toteuttaa huomioon ottaen varmuuskopioiden perimmäinen tarkoitus, eikä sitä voi välttämättä katsoa tietosuoja-asetuksen 17 artiklan 2 momentin mukaiseksi kohtuulliseksi toimenpiteeksi. Tietojen saatavuuden ja tietoihin pääsyn palauttaminen edellyttävät, että henkilötiedoista ja niiden käsittelystä tallennetaan riittävät varmuuskopiot[1189]. Varmuuskopioiden riittävä suojaus, elinkaaren hallinta sekä kriittisten varmuuskopioiden säännöllinen palautusharjoittelu ovat oleellisia hyvien käytänteiden mukaisia toimenpiteitä tietoturvan näkökulmasta, mutta näitä toimenpiteitä ei ole juurikaan huomioitu tietoturvan sääntelyjärjestelmässä. Varmuuskopioinnin tärkeydestä

[1187] Normaaliolojen häiriötilanteita, jolloin jatkuvuus- ja toipumissuunnitelmat aktivoidaan, ovat yleensä laajavaikutteisia, merkittäviä tai vakavia häiriöitä organisaation toiminnassa, palvelussa tai prosesseissa.
Laajavaikutteiset häiriöt ovat sellaisia, jotka vaikuttavat suureen joukkoon toiminnan, palvelun tai prosessin sidosryhmiä, esimerkiksi käyttäjiin, ja ne voivat johtaa toiminnan keskeyttämiseen tai merkittävään alenemiseen. Ks. VAHTI 2/2016, s. 25.
Tällaisia häiriötilanteita voivat olla esimerkiksi tulipalo, vesivahinko sekä tietotekniikan laajat häiriöt, esimerkiksi verkkohyökkäykset. Ks. Andreasson & Koivisto 2013, s. 99–100.
[1188] NIS 2 -direktiivin kohta 49.
[1189] Ks. myös TSV 7.12.2021, dnro 1150/161/2021.

huolimatta varmuuskopioinnin vaatimukset näyttäytyvät lisäksi hajanaisina organisaatioiden tietoturvan sääntelyjärjestelmässä.

4.4.5 Tietoturvan vähimmäisvaatimukset ja tietoturvatason arviointi

Kuten lienee jo selvää, järjestelmän suunnittelu ei ole ainoastaan teknistä tekemistä, vaan siinä tulee ottaa huomioon myös oikeudelliset seikat. Järjestelmissä olevan tiedon osalta keskeinen huomioitava lainsäädäntö on tietysti tietosuojalainsäädäntö, sillä lähes kaikissa järjestelmissä käsitellään jossain määrin henkilötietoja. Osa järjestelmän suunnitteluvaatimuksista liittyvät puolestaan puhtaasti sopimuksilla sovittuihin asioihin, esimerkiksi palvelutasojen[1190] suhteen. Etenkin tietosuoja-asetus asettaa paljon vaatimuksia hankintasopimuksien sisällölle henkilötietojen turvaamisen suhteen[1191]. Lainsäädännön vaatimusten lisäksi tietoturvallisuusvaatimusten määrittelyssä ja järjestelmien kehittämisessä voidaan hyödyntää jo olemassa olevia tietoturvallisuuden standardeja ja muita viitekehyksiä[1192].

Tietoturvallisuuden viitekehykset toimivat parhaiten hyvien käytänteiden lisääjänä sekä organisaatioiden tietoturvan kehittäjänä ja suunnannäyttäjänä. Tunnettujen tietoturvastandardien noudattaminen ja sertifiointi ovat luottamusta lisääviä tekijöitä sopimusosapuolten ja muiden toimijoiden kesken, sillä tällöin pystytään osoittamaan tiettyjen tietoturvatoimien toteutuminen organisaatiossa. Toteutumisen osoittaminen on mahdollista tehdä tietoturva-auditoinnilla, mikä tarkoittaa puolueetonta ja riippumatonta tutkintaa siitä, ovatko tutkittavan kohteen tietoturvallisuuden loukkaamattomuuteen liittyvät toiminnot ja niihin liittyvät tulokset suunniteltujen järjestelyiden mukaisia, tehokkaita ja sopivia tavoitteiden saavuttamiseksi[1193]. Esimerkiksi ISO 27001-auditoinnit usein tähtäävät sertifiointiin, jonka avulla organisaatio voi osoittaa sidosryhmilleen, että sillä on käytössä tietoturvallisuuden hallintajärjestelmä ja se on sitoutunut jatkuvaan tietoturvallisuuden tason ylläpitoon, arviointiin ja kehittämiseen[1194]. Kansallisten viitekehysten todentamisen osalta esimerkiksi virallisessa Katakri-auditoinnissa tavoitteena on saada arviointilaitostodistus vaatimusten toteutumisen todistamiseksi.

[1190] SLA – Service Level Agreement
[1191] Ks. luku 3.3.2 (”Henkilötietojen käsittelyn ja tietoturvan huomioiminen sopimuksissa”).
[1192] Ks. lisää luku 2.7 (”Tietoturvan sääntelyjärjestelmä ja hyvät käytänteet”).
[1193] Porvari 2012: 47.
[1194] Esimerkiksi tällaisen ISO 27001 -sertifiointiauditoinnin läpäisseen yrityksen tulee myös ylläpitää sertifiointiansa säännöllisten seuranta-auditointien kautta, jotta voidaan varmistaa tietoturvallisuuden tason ylläpitäminen ja vaatimuksenmukaisuus sertifioinnin kohteena olevassa yrityksessä.

Kyberturvallisuuskeskuksen (Traficomin) hyväksymät arviointilaitokset arvioivat auditoimalla toimeksiannossa sovitun arviointikriteeristön pohjalta organisaation tietoturvallisuustasoa. Toisinaan virallisten auditointien sijaan tehdään tietoturva- ja tietosuoja-arviointeja eri viitekehyksiä vasten, jotka eivät tähtää sertifiointiin tai todistukseen vaan pätevän arvioijan tekemään arviointiraporttiin. Tällaista arviointiraporttia voidaan käyttää esimerkiksi ohjenuorana järjestelmän tai toiminnan kehittämisessä, taikka selkänojana rahoituksen lisäämiseksi tietoturvabudjetissa. Huomioitava on myös, että Suomessa virallisia auditointeja ei tehdä PiTuKria tai Julkria käyttäen, koska ne eivät kuulu tällä hetkellä Kyberturvallisuuskeskuksen (Traficomin) hyväksymien arviointilaitoksien pätevyysalueeseen[1195]. Eli näiden osalta on kyseessä arviointi, jonka lopputuotos on arviointiraportti.

Viranomaisten tietoturvallisuuden arviointi perustuu lakiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)[1196]. Lain 3 §:n mukaan valtiohallinnon viranomaiset saavat käyttää tietoturvallisuutensa arvioinnissa vain laissa (1406/2011) tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, arviointilaitoslaki) mukaan[1197]. Muiden toimijoiden osalta tietoturvallisuuden arvioinnista ei ole samalla tavalla säädetty kuin viranomaisten vaatimuksista. Poikkeuksena on asiakastietolain (703/2023, Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä) 87 §:n mukainen tietoturvallisuuden arviointi, eli niin kutsuttu Kanta-auditointi, joka ulottuu muun muassa Kanta-palveluihin liittyviin järjestelmiin, hyvinvointisovelluksiin sekä Kanta-välityspalveluihin[1198].

Huomioitava kuitenkin on, että kaikkiin organisaatioihin ulottuvassa EU:n yleisessä tietosuoja-asetuksessa on korostettu, että käytännesääntöjen ja sertifiointimekanismin noudattamista voidaan pitää yhtenä todisteena asetuksen vaatimusten osoitusvelvollisuuden toteutumisesta [1199] . Näin ollen tietoturvan

[1195] Ks. Traficom, kyberturvallisuuskeskus 2023a. Tällaisia hyväksyttäjä tietoturvallisuuden arviointilaitoksia ovat KPMG IT Sertifiointi Oy, Nixu Certification Oy sekä Inspecta Sertifiointi Oy

[1196] Huomioitava on myös tiedonhallintalain 13 §, jossa on säädetty, että viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

[1197] Kyberturvallisuuskeskus hyväksyy arviointilaitokset (ks. Traficom, kyberturvallisuuskeskus 2023b). Kansallinen akkreditointielin FINAS (Finnish Accreditation Service) pätevyydentoteamispalveluna arvioi tietoturvallisuuden arviointilaitoksien toimintaa sekä työntekijöiden pätevyyttä ja riippumattomuutta (ks. Finnish Accreditation Service 2018).

[1198] Ks. myös Kanta 2024.

[1199] Esimerkiksi tietosuoja-asetuksen kohta 81. Lisäksi asetuksen 42 artiklan mukaan tietosuojaa koskevia sertifiointimekanismeja kannustetaan ottamaan käyttöön, mutta sen on oltava myös vapaaehtoista.

käytännesääntöjen, eli esimerkiksi kansallisten viitekehyksien, arvioinnit eivät ole lähtökohtaisesti organisaatioiden osalta pakollisia, mutta ne voivat toimia tietosuojan osoitusvelvollisuuden toteutumisen yhtenä todisteena. Samaa ajatusta on noudatettu NIS 2 -direktiivin ja tulevan kyberturvallisuuslain osalta: Hallinnollisen seuraamusmaksun määräämisessä on huomioitava hyväksyttyjen käytännesääntöjen tai hyväksyttyjen sertifiointimekanismien noudattaminen[1200].

EU:n kyberturvallisuusasetus (2019/881/EU) vaikuttaa tietoturvasertifiointeihin liittyvään toimintaan. Asetuksessa tarkoitetaan sertifiointijärjestelmällä kattavaa sääntöjen, teknisten vaatimusten, standardien ja menettelyjen muodostamaa kokonaisuutta. Näiden sertifiointijärjestelmien tarkoituksena on sertifioida tieto- ja viestintätekniikan tuotteita, palveluita ja prosesseja tai kohdistaa niihin vaatimuksenmukaisuuden arviointia, jolloin ne ovat yhtenäisten turvallisuusvaatimusten mukaisia.

Ensinnäkin on huomioitava, että kyberturvallisuusasetuksen nojalla sellaiset kansalliset kyberturvallisuuden sertifiointijärjestelmät tai –menettelyt, joiden kattamat tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit kuuluvat jonkin eurooppalaisen kyberturvallisuussertifioinnin soveltamisalaan, lakkaavat asetuksen mukaan tuottamasta oikeusvaikutuksia. Näin ollen jäsenmaat eivät voi enää laatia kansallisia sertifikaatteja siltä osin, kun ne olisivat päällekkäisiä asetuksen nojalla laadittujen EU-sertifikaattien kanssa. Esimerkiksi kansallinen pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) ja sen avulla tehtävä pilvipalveluiden turvallisuuden arviointi lakkaa, mikäli pilvipalveluiden sertifioinnista tulee tulevaisuudessa eurooppalainen sertifiointijärjestelmä.[1201] Toinen huomioitava seikka on se, että kyberturvallisuusasetuksen mukainen arviointilaitosten akkreditointi- ja valtuuttamisprosessi vastaa pääosin arviointilaitoslaissa (1405/2011) tarkoitettua samanlaista prosessia, mutta sisällölliset vaatimukset ovat erilaiset. Näin ollen arviointilaitoslain mukainen arviointilaitos ei voi suoraan saada kyberturvallisuusasetuksessa tarkoitettua vaatimuksenmukaisuuden arviointilaitoksen asemaa, jolloin asetuksen mukainen akkreditointi ja valtuuttaminen on tehtävä erikseen.[1202] Kolmanneksi on huomioitava, että myös kyberturvallisuussertifiointi on 56 artiklan mukaan vapaaehtoista, jollei muualla kansallisessa tai unionin lainsäädännössä toisin säädetä. Kyberturvallisuusasetuksen artiklassa 51 on täsmennetty yksityiskohtaisemmin sertifiointijärjestelmien turvallisuustavoitteiden vähimmäistasosta. Sertifioidut tuotteet, palvelut ja prosessit voitaisiin jakaa kolmeen varmuustasoon, jotka vastaavat käyttötarkoitukseen liittyvää riskin tasoa

[1200] NIS 2 -direktiivin 32 artikla kohta 7 (Keskeisiin toimijoihin liittyvät valvonta- ja täytäntöönpanotoimenpiteet); HE 57/2024, s. 290 (kyberturvallisuuslain 37 §, seuraamusmaksun määrittäminen).
[1201] HE 98/2020 vp: 108.
[1202] HE 98/2020 vp: 109.

perustuen mahdollisen poikkeaman todennäköisyyteen ja vaikutuksiin. Varmuustasot ovat perustaso, korotettu ja korkea. Näiden perusteella sertifiointijärjestelmässä tulee täsmentää omat vastaavat turvallisuusvaatimukset. Tavoitteena on, että sertifikaatin myötä tuotteiden ja palvelujen tarjoajien ei tarvitsisi hankkia useita kansallisia sertifikaatteja.

Kyberturvallisuusasetuksen 51 artikla on olennainen järjestelmien turvallisuuden kannalta, sillä siinä on säädetty sertifiointijärjestelmien vähimmäisturvallisuustavoitteista. Eli toisin sanoen kyseisessä artiklassa on säädetty vähimmäistaso turvallisuusvaatimuksien osalta sertifioiduille kohteelle. Huomioitava on, että kyberturvallisuusasetuksen vähimmäisturvallisuusvaatimuksilla on paljon yhtäläisyyksiä luonnoksena olevan EU:n kyberkestävyyssäädöksen (”CRA-asetus”) vaatimuksien kanssa. Molemmissa asetuksissa toistuvat osittain samankaltaiset tietoturvavaatimukset, jotka korostavat muun muassa tiedon turvaamista koko sen elinkaaren ajalta, todennettavuutta lokitoiminnon avulla, pääsynhallintaa sekä haavoittuvuusien hallintaa.

> Esimerkiksi kyberturvallisuusasetuksen 51 artiklan elinkaariajattelua huomioivan kohdan mukaan tallennetut, siirretyt ja muulla tavoin käsitellyt tiedot tulisi suojata vahingossa tapahtuvalta tai luvattomalta tallentamiselta, käsittelyltä, käytöltä, luovuttamiselta, tuhoamiselta, katoamiselta, muuttamiselta taikka puutteelliselta saatavuudelta tieto- ja viestintätekniikan tuotteen, palvelun tai koko prosessin elinkaaren ajalta.
>
> Asetuksen artiklassa 51 on myös huomioitu luvattoman pääsyn ehkäiseminen salassa pidettäviin tietoihin. Esimerkiksi kohdassa c on täsmennetty, että ainoastaan valtuutettujen henkilöiden, ohjelmien tai koneiden saatavilla on vain ne tiedot, palvelut tai toiminnot, joihin näillä on käyttöoikeudet. Näin ollen tämä vaatimus viittaa pääsynhallinnan kontrolleihin.
>
> Mitä tulee järjestelmän käytön ja toiminnan myöhempään todennettavuuteen, siitä on säädetty 51 artiklan e ja f -kohdissa. Asetuksen mukaan järjestelmään tulisi tallentua tietoja siitä, mitä tietoja, palveluja tai toimintoja on käytetty, hyödynnetty tai muutoin käsitelty, sekä näiden toimien ajankohta ja tekijä. Lisäksi kyseiset tiedot pitäisi olla mahdollista tarkastaa. Tämä vaatimuksen kohta viittaa puolestaan lokien keräämiseen riittävällä tasolla.
>
> Artiklassa 51 on myös säädetty yhtenä sertifioinnin vähimmäisvaatimuksena, että kaikki tunnetut riippuvuudet ja haavoittuvuudet tulisi tunnistaa ja dokumentoida. Lisäksi tieto- ja viestintätekniikan tuotteiden, palveluiden ja prosessien ei tulisi sisältää tunnettuja haavoittuvuuksia ja niihin

> sisältyy ajantasainen ohjelmisto ja laitteisto, jotka eivät sisällä julkisesti tiedossa olevia haavoittuvuuksia. Lisäksi tuotteisiin, palveluihin ja prosesseihin tulisi sisältyä mekanismit, joilla varmistetaan turvalliset päivitykset, ja näiden suojaus tulisi olla oletusarvoista ja sisäänrakennettua. Tietojen, palvelujen ja toimintojen saatavuus ja käytettävyys tulisi olla mahdollista palauttaa mahdollisimman pian fyysisen tai teknisen poikkeaman sattuessa. Tämä viittaa tietojen varmuuskopiointiin.

Tällaiset 51 artiklan vaatimukset kuvastavat hyvin teknologianeutraalia sääntelyä samojen teemojen osalta, joita on käsitelty tässä luvussa aiemmin: elinkaarimallin, lokituksen, pääsynhallinnan ja varmuuskopioinnin vaatimuksia. Huomioitava on, että itse kyberturvallisuussertifiointi on kuitenkin toistaiseksi vapaaehtoista, jollei muualla kansallisessa tai unionin lainsäädännössä toisin säädetä.

Yhteenvetona todettakoon, että toistaiseksi käytännesääntöjen ja standardien noudattaminen perustuu pitkälti vapaaehtoisuuteen, mutta etenkin tietoturvatasoltaan kypsemmissä tuotteita ja palveluita tarjoavissa organisaatioissa tietoturva-auditoinnit ja -arvioinnit saattavat olla hyvinkin arkipäiväisiä. Käytännesääntöjen ja tietoturvastandardien noudattamisella saavutetaan ennen kaikkea asiakasluottamusta organisaatioiden tietoturvatasoon, mutta myös ylläpidetään ja kehitetään organisaation ja järjestelmien tietoturvaa. Kyberturvallisuusasetuksen 51 artiklan sekä tulevan CRA-asetuksen vähimmäistietoturvavaatimukset ovat hyviä esimerkkejä teknologianeutraalista sääntelystä ja ne ovat oleellista huomioida osana järjestelmien kehittämistä ja tietoturvavaatimusten määrittelyä. Vapaaehtoinen käytännesääntöjen ja standardien noudattaminen ja sertifiointi eivät kuitenkaan välttämättä ole riittäviä tietoturvallisuuden edistämisen osalta yhteiskunnassa. Tarvitaan enemmän tietoturvaan liittyvää vähimmäissääntelyä niin henkilötietojen, henkilöiden perusoikeuksien kuin myös muiden organisaatioiden luottamuksellisten tietojen suojelemiseksi.

5 KESKEISET TUTKIMUSTULOKSET

5.1 Hyvä tietoturvan sääntelyjärjestelmä ja toimintaympäristön vaatimukset

Viime vuosikymmenen aikana teknologinen kehitys, digitalisoituminen ja globalisoituminen ovat olleet nopeaa. Informaatioyhteiskuntamme on muuttunut *verkkoyhteiskunnaksi*, jota voidaan kutsua myös *oikeudellistuneeksi riski- ja valvontayhteiskunnaksi*[1203]. Muuttuva ympäristö on luonut organisaatioille uusia mahdollisuuksia, mutta myös uusia uhkia ja riskejä. Tietojärjestelmien ja -verkkojen varassa toimiva yhteiskuntamme on siksi kohdannut uusia lainsäädännöllisiä muutostarpeita ja uutta oikeudellista sääntelyä, oikeusperiaatteiden ja oikeudellisten kysymysten muotoilua sekä oikeuskäsitteiden määrän lisääntymistä[1204]. Laitteet ja palvelut kehittyvät todennäköisesti nopeasti myös jatkossa, ja tietoa käsitellään entistä automaattisemmin osana digitalisaatiota ja robotisaatiota. Myös tiedon määrä kasvaa palveluiden digitalisoituessa[1205]. Nykyinen oikeudellistunut verkkoyhteiskuntamme voi muuttua jopa *automaatioyhteiskunnaksi*. Kehityksen myötä oikeudellistuminen, riskienhallinta ja valvonta tulevat olemaan pysyviä piirteitä muuttuvassa yhteiskunnassamme. Tietoturvallisuuden merkitys on kasvanut teknologian kehittymisen, digitalisoitumisen ja globalisaation myötä: tämä heijastuu nykyiseen, järjestelmäriippuvaiseen verkkoyhteiskuntaamme, organisaatioiden toimintaan, yhteiskunnan toimivuuteen sekä yksilöiden oikeuksiin. Toimintaympäristön muutokset asettavat vaatimuksia myös tietoturvan sääntelyjärjestelmälle. Yhteiskunnan digitalisoituessa ja ottaessa uusia teknologisia ratkaisuja käyttöön **hyvä tietoturvan sääntelyjärjestelmä edellyttää teknologian huomioon ottamista sekä sääntelyn ja teknologian yhteensovittamista teknologianeutraalisti**[1206].

Tulevaisuudessa organisaatioihin kohdistuvat tietoturvariskit liittyvät suurella todennäköisyydellä uuden teknologian omaksumiseen ja digitalisoitumiseen.

[1203] Ks. lisää luku 2.3 (”Kehitys informaatioyhteiskunnasta oikeudellistuneeksi verkkoyhteiskunnaksi”).
[1204] Saarenpää 2016a: 79, 103–109; Saarenpää 2016b: 63–66; Saarenpää 2015: 203; Wiatrowski 2016: 109, 116; Korja 2016a: 197–198.
[1205] Tähän liittyy oleellisesti myös IoT (Internet of Things eli esineiden internet) -laitteiden lisääntyvä käyttö. Tällaisista laitteista esimerkkinä mm. älykkäät kodinkoneet. Internetiin liitettyjen kulutustavaroiden ja teollisuuden laitteiden lisääntynyt käyttö lisää yksityisyydensuojaan, tietoturvaan ja kyberturvallisuuteen liittyviä uusia riskejä. Ks. Euroopan unionin neuvosto, Neuvoston päätelmät internetiin yhdistettyjen laitteiden kyberturvallisuudesta 2.12.2020, s. 3.
[1206] Ks. lisää teknologianeutraalisuuden periaatteesta luvusta 2.4.2 (”Muut tietoturvalainsäädäntöön liittyvät keskeiset periaatteet”).

Jatkossakin ihminen on kuitenkin inhimillisine piirteineen suurin tietoturvauhka[1207]. Ihminen uhkana on kuitenkin samalla mahdollisuus: tietoisuuden lisäämisellä, helppokäyttöisillä tietoturvaratkaisuilla ja johdon sitoutumisella tietoturvan edistämiseen, ihmisistä voi tulla tietoturvan voimavara organisaatioissa. Erityisiä mahdollisuuksia liittyy etenkin poikkeamien varhaiseen havainnointiin ja reagointiin. Tietoisuuden ja osaamisen merkitystä tietoturvariskien hallinnassa tukee käsite *risk homeostasis*: yksilöt ylläpitävät sellaista riskin tasoa, minkä he itse hyväksyvät[1208]. **Hyvä tietoturvan sääntelyjärjestelmä ottaa siksi teknologian ohella huomioon ihmisen**. **Näin ollen hyvä tietoturvan sääntelyjärjestelmä vastuuttaa viranomaisten ja organisaatioiden johdon lisäksi yksilöitä huomioimaan tietoturvan toiminnassaan**.

Toimintaympäristön vaihtelut lisäävät ja muuttavat organisaatioihin kohdistuvia riskejä osin ennakoimattomasti, jolloin organisaatioiden tietoturvariskien määrää ja muotoa tulevaisuudessa on vaikea täysin ennustaa. Lainsäätäjä on siksi usein toimintaympäristön kehitystä jäljessä. Tästä hyvänä esimerkkinä on tekoälyn hyödyntäminen niin kansalaisten ja organisaatioiden kuin rikollisten toiminnassa. Tekoäly uutena teknologiana on muodostanut täysin uusia riskejä organisaatioiden toimintaympäristöön ja kyberturvallisuuteen jo jonkin aikaa[1209], ja vastauksena huomattuun sääntelytarpeeseen on EU:lta viimein julkaistu lopullinen versio tekoälysäädöksestä (2024/1689/EU). Uutta tietoturvaan, tietosuojaan ja riskienhallintaan liittyvää lainsäädäntöä on tullut paljon viime vuosina, mutta yhteiskunnan kehitykseen verrattuna lainsäädäntö on ollut pikemminkin reaktiivista kuin proaktiivista. Nykyisen toimintaympäristön kehitystahti vaatii todella paljon lainsäätäjiltä osaamista, mikä osaltaan saattaa vaikeuttaa kehityksessä mukana olemista ja proaktiivista toimintaa[1210]. Tämä tuo esiin tietoturvan sääntelyjärjestelmän *lainsäätäjäriskin*: lainsäätäjä ei aina havahdu lainsäätämistarpeeseen ajoissa tai oikealla tavalla[1211]. Lainsäätäjäriski ilmenee myös siten, että kansainvälisen sääntelyn muutoksista huolimatta olemme edelleen Suomessa vailla yhtenäisiä käsityksiä tietoturvallisuuden merkityksestä ja siten myös ilman yleistä

[1207] Vanha sanonta ”ihminen on suurin tietoturvauhka” viittaa siihen, että monet tietoturvatapahtumat ovat seurausta joko tahallisesta toiminnasta, esimerkiksi sabotaasista, tai inhimillisistä virheistä. Sanontaan linkittyy myös eräänlainen riski siitä, että yhteiskunnan digitalosoinnin myötä tietoturvallisuuden taso on suuresti riippuvainen yksilöistä ja heidän tietoturva- ja digiosaamisestaan. Ks. Salminen 2022, s. 57–60 ja myös 131–139.
[1208] Porvari 2012: 143–144.
[1209] Esimerkiksi ks. tekoälyn mahdollistamien kyberhyökkäysten turvallisuusuhasta Traficomin julkaisusta 30/2022.
[1210] On huomioitava se, että lait valmistellaan virkamiesten asiantuntemuksen puitteissa, jolloin myös lain sisältö rajoittuu lakia valmistelevan tahon hallussa olevaan tietoon: yleensä lain valmisteluvaiheessa käytettävissä oleva tieto on määrältään pienempi kuin lain soveltamiseen tarvittava tieto, mikä ilmentää lainsäätäjän dilemmaa (ks. Häyhä 1997: 17).
[1211] Saarenpää 2016a: 82–83, 87–88, 239.

tietoturvallisuuslakia [1212] . **Hyvä tietoturvan sääntelyjärjestelmä tukee proaktiivisuutta niin, että tyypillinen lainsäätäjäriski tiedostetaan. Näin ollen vastakohtaisesti hyvä tietoturvan sääntelyjärjestelmä ei voi olla reaktiivinen, vaan sen tulee voida sopeutumisen ohella myös ohjata muuttuvaa teknologista toimintaympäristöä ja huomioida varhaisessa vaiheessa uudet riskit**.

Teknologian kehitys, digitalisoituminen ja globalisoituminen muuttavat sekä yhteiskunnan toimintatapoja että oikeutta. Oikeuden muuttuminen on tältä osin ilmennyt erityisesti oikeusjärjestyksen eli oikeusnormien koonnoksen muuttumisena[1213], sillä esimerkiksi uutta tietoturvaan liittyvää lainsäädäntöä on säädetty kiihtyvällä tahdilla. Tietoturvan sääntely on kuitenkin kohdistunut erityisesti kriittisiin toimialoihin ja viranomaisiin, mikä on johtanut nykyisen tietoturvasääntelyn heterogeenisuuteen ja hajanaisuuteen. Sääntelystä ei ole näin ollen muodostunut kattavaa. **Tietoturvan sääntelyjärjestelmän tulisi olla sisällöltään johdonmukainen ja yhtenäinen kokonaisuus ollakseen hyvä, mutta sen edellytyksenä on samalla kohtuullisuuden ja oikeudenmukaisuuden kriteerit**. Esimerkiksi henkilötietojen ohella myös muita luottamuksellisia tietoja tulee suojata asianmukaisesti ja riittävällä tietoturvatasolla muissakin organisaatioissa kuin kriittisillä toimialoilla: tietoturvan sääntelyjärjestelmässä tulee huomioida hyvä tietoturvatapa ja sen mukainen tietoturvan vähimmäistaso.

Toimintaympäristön uhkiin vastannut tietoturvasääntely on vaikuttanut laajasti oikeusjärjestykseen johtaen lukuisiin yksittäisiin säännöksiin, mutta myös sitovuudeltaan erilaiseen sääntelyyn. Tietoturvaan liittyvä sääntely muodostuu sekä perinteisestä, oikeudellisesti sitovasta sääntelystä että soft law -tyyppistä sääntelyä tuottavista myötä- ja itsesääntelymalleista ja muista ei-sitovista ohjeistuksista[1214]. Tietoturvallisuutta koskevaa sääntelyä sisältyy useisiin niin julkista hallintoa kuin erilaisten palveluiden tarjoamista koskeviin säädöksiin. Osa säännöksistä koskee tietosuojaa ja luokiteltujen asiakirjojen käsittelyä, osa taas toiminnan riskienhallintaa ja jatkuvuutta.[1215] Erityisesti tietoturvaa ja tietosuojaa koskevia yleisiä velvollisuuksia on henkilötietoja turvaavassa lainsäädännössä ja viranomaisia

[1212] Saarenpää & Riekkinen 2023: 201–202.
[1213] Aarnio 2006: 108–109. Oikeuden muuttuminen voi tapahtua a) oikeusjärjestyksen eli oikeusnormien koonnoksen muuttumisena; b) oikeusjärjestelmän eli systeemin muuttumisena; taikka c) molempien muuttumisena. Oikeusnormit voivat muuttua lainsäätäjän toimesta eli esimerkiksi uusien soveltamiskäytäntöjen tai uusien säädösten myötä. Oikeusjärjestelmän muuttuminen on puolestaan paljon monimutkaisempi prosessi kuin yksittäiset normimuutokset ja se vaatii enemmän aikaa. Tällaisina muutoksen aiheuttajina yleensä pidetään muun muassa yhteiskunnallisia, taloudellisia, kulttuurillisia taikka arvojen ja moraalin muutoksiin liittyviä tekijöitä.
[1214] Ks. Voutilainen 2009: VIII.
[1215] HE 192/2017 vp: 9.

koskevissa yleislaeissa. Useilla toimialoilla on myös sektorikohtaisia velvoitteita huolehtia palveluiden ja järjestelmien tietoturvasta ja -suojasta.[1216] Muuttuvan toimintaympäristön uhkiin vastaamiseksi on mahdollistettava sitovuudeltaan ja hierakialtaan erilaisten normistojen toisiaan täydentävä ja johdonmukainen vuorovaikutus, jonka myötä **hyvän tietoturvan sääntelyjärjestelmän tulee olla helposti tavoitettava ja ymmärrettävä.**

Oikeuden muutos voidaan huomata oikeusjärjestyksen muuttumisen ohella oikeusjärjestelmän muuttumisena, joka ilmenee tämän tutkimuksen toteutuksen kautta: oikeusjärjestelmän muutoksessa tarvitaan tutkimusta. Oikeusjärjestelmän muuttuminen on havaittavissa myös osana suurempaa yhteiskunnallista ja arvopohjaista muutosta, jossa keskiössä on tietojen turvaaminen digitalisoituneessa, verkottuneessa ympäristössä. Tietoturva nähdään yhä vahvemmin metaperiaatetasoisena oikeutena (*”oikeus tietoturvaan”*), jolloin se heijastuu myös perusoikeustason periaatteisiin: yksilöillä tulisi olla oikeus kyberturvaan nykyisessä järjestelmäriippuvaisessa verkkoyhteiskunnassa[1217]. **Hyvä tietoturvan sääntelyjärjestelmä huomioi yhteiskunnan arvoja ilmentävät perusoikeudet.**

Organisaation tietoturva toteutuu lopulta hyvien käytänteiden myötä. Organisaation arjessa toteutuvat hyvät käytännöt tai käytännesäännöt saattavat kuitenkin poiketa lainsäädännössä ilmenevistä tietoturvan toteuttamisvaatimuksista. Toisaalta käytännesäännöissä voi konkretisoitua uuden teknologian tuottamien riskien ja mahdollisuuksien tunnistaminen. **Hyvä tietoturvan sääntelyjärjestelmä mahdollistaa organisaatioiden hyvät käytänteet ja käytännesäännöt tietoturvan toteuttajana.**

Tämän tutkimuksen päätehtävänä on ollut muodostaa organisaatioiden tietoturvan sääntelyjärjestelmä kokoamalla yhteen ja systematisoimalla organisaatioiden tietoturvaa käsitteleviä säädöksiä. Samalla tavoitteena on ollut esittää hyvän tietoturvatavan muodostama kokonaisuus, joka on tapahtunut arvioimalla organisaatioita velvoittavia tietoturvasäännöksiä sekä käytännesääntöjä ja hyviä käytänteitä. Lainsäädännöstä ilmenevää hyvää tietoturvatapaa on myös vertailtu organisaatioiden hyviin, olemassa oleviin käytäntöihin. Tutkimustehtävän toteuttaminen on edellyttänyt nykyisen tietoturvalainsäädännön sisällön ja tehokkuuden

[1216] Liikenne- ja viestintäministeriön julkaisuja 2021:1: 17–18. Eri sektoreiden kyvykkyydet vastata kasvaviin tietoturva- ja tietosuojahaasteisiin vaihtelevat kuitenkin suuresti. Esimerkiksi lokakuussa 2020 julkisuuteen nousseen Vastaamon tietomurtoon liittyvä selvittäminen on osoittanut, että Suomessa on tietojärjestelmiä, joiden tietoturvan ja tietosuojan taso ei ole EU:n tietosuojalainsäädännön ja toimialan erityislainsäädännön edellyttämällä tasolla. Näin ollen on todettu, että etenkin yhteiskunnan kannalta kriittisten toimialojen tietojärjestelmien sääntelyä ja valvontaa on vahvistettava.
[1217] Ks. luvut 2.4.1 (”Oikeus tietoturvaan periaatteena”) sekä 2.5 (”Tietoturva perusoikeutena osana tietoturvan sääntelyjärjestelmää”).

sekä yleisen tietoturvalain säätämistarpeen tarkastelua ja arviointia. Uusien säädöksien synnyttämästä oikeusjärjestyksestä on tunnistettu aikaisemmin tässä luvussa kuvatut elementit hyvälle tietoturvan sääntelyjärjestelmälle, jotka samalla toimivat tässä tutkimuksessa normikeskeisinä kriteereinä sääntelyjärjestelmän hyvyydelle. Täten tutkimuksen tavoitteena on ollut myös määritellä oikeusjärjestyksen pohjalta organisaatioiden hyvä tietoturvan sääntelyjärjestelmä.

Tutkimuksen toteuttamiseksi on erotettu kaksi olennaista tutkimuskysymystä, joista ensimmäisen tutkimuskysymyksen vastausta käytetään perustana määritettäessä toisen tutkimuskysymyksen vastausta:

1) ***Onko nykyinen organisaatioiden tietoturvan sääntelyjärjestelmä hyvä?***

2) ***Onko Suomessa tarpeen kansallinen tietoturvalaki?***

Tutkimuskysymysten vastauksien arvioinnin taustalla vaikuttavat hyvän tietoturvan sääntelyjärjestelmän elementit, joita on aikaisemmin tässä luvussa korostettu. Näin ollen tutkimuskysymysten vastauksiin vaikuttavia kriteerejä ovat tunnistettujen tietoturvan sääntelyjärjestelmän elementtien osalta muun muassa *teknologianeutraalisuus, proaktiivisuus, hyvien käytänteiden huomioiminen, kohtuullisuus ja oikeudenmukaisuus, tavoitettavuus ja ymmärrettävyys, johdonmukaisuus ja yhtenäisyys sekä yksilöiden ja perusoikeuksien huomioiminen:*

> *Teknologianeutraalisuuden* vaatimus edellyttää teknologian huomioimista ja yhteensovittamista lainsäädännön kanssa. Teknologianeutraalisuus on yksi informaatio-oikeuden oikeusperiaatteista, joka on heijastunut lainvalmisteluun: pyrkimyksenä on säännellä ensisijaisesti tekoa teknologian sijaan. Näin ollen teknologianeutraalisuus kuuluu osaksi hyvää tietoturvan sääntelyjärjestelmää.[1218]

> Teknologianeutraalisuus auttaa lainsäädäntöä pysymään paremmin ajan tasalla. Tällainen ajan tasainen lainsäädäntö mahdollistaa sääntelyjärjestelmän pysymisen proaktiivisempana. *Proaktiivisuus* on yksi hyvän tietoturvan sääntelyjärjestelmän elementti. Proaktiivisuutta tarvitaan, jotta lainsäätäjäriskiä saataisiin pienennettyä. Tällöin lainsäätäjä ei olisi yhteiskunnan kehitykseen verrattuna jäljessä vaan lainsäädännön kehittämisen reaktiivisuus olisi minimoitu.[1219]

[1218] Ks. teknologianeutraalisuudesta yksityiskohtaisemmin luvusta 2.4.2 (”Muut tietoturvalainsäädäntöön liittyvät keskeiset periaatteet”).
[1219] Ks. yhteiskunnan kehityksestä ja proaktiivisuuden vaatimuksesta luvusta 2.3 (”Kehitys informaatioyhteiskunnasta oikeudellistuneeksi verkkoyhteiskunnaksi”) sekä

Lainsäädännön proaktiivisuutta edistää *hyvien käytänteiden huomioiminen,* joka on myös hyvän tietoturvan sääntelyjärjestelmän elementti. Muuttuva toimintaympäristö ja sen uudet uhat vaativat lainsäädännön rinnalle hyviä käytänteitä, jotka tulevat ilmi erilaisten tietoturvan viitekehysten ja ohjeistuksien kautta. Käytännesäännöt soft law -tyyppisenä aineistona ovat osa organisaation tietoturvaa, mutta ne tulisi huomioida myös lainsäädännössä. Standardien noudattaminen oikeusnormiston osana tulisi tarvittaessa huomioida hyvässä tietoturvan sääntelyjärjestelmässä, mikä mahdollistaisi hyvien käytänteiden huomioimisen paremmin. Käytännesääntöjen ja standardien avulla lainsäädäntö pysyy muuttuvassa järjestelmäriippuvaisessa toimintaympäristössä teknologianeutraalina ja ajankohtaisena.[1220]

Hyvän tavan mukainen toiminta on usein se tapa toimia, mikä katsotaan vakiintuneeksi tavaksi tai käytännöksi toimia. Useimmiten vakiintuneet tavat ovat alalla kohtuullisia ja oikeudenmukaisia. Lisäksi hyvän tavan oikeusperiaatteella on ominaista, että se tarkoittaa kaikille samaa.[1221] Hyvä tietoturvatapa tulee ilmi täsmällisten sääntöjen puuttuessa hyvinä käytänteinä tietyllä alalla eli osana tavanomaista oikeutta. Hyvä tietoturvan sääntelyjärjestelmä on oltava hyvän tietoturvatavan mukaisesti *kohtuullinen ja oikeudenmukainen*, mutta lisäksi yhtä lailla *tavoitettava ja ymmärrettävä* tarkoittaakseen kaikille samaa.[1222] Näiden elementtien pohjalta rakentuvat hyvän tietoturvan sääntelyjärjestelmän kriteereiksi myös *johdonmukaisuuden ja yhtenäisyyden* vaatimukset. Esimerkiksi johdonmukaisella ja yhtenäisellä tietoturvasääntelyllä parannetaan tietoturvasäännöksien tavoitettavuutta ja ymmärrettävyyttä.[1223]

Hyvän tietoturvan sääntelyjärjestelmän oleellisena elementtinä on perusoikeuksien huomioiminen, sillä ne ilmentävät yhteiskunnan arvoja ja mahdollistavat yksilöiden oikeuksien turvaamisen. Oikeuksien myötä syntyy vastuita ja näin ollen hyvä tietoturvan sääntelyjärjestelmä huomioi yksilöt perusoikeustasolla, mutta myös vastuuttamalla yksilöt huomioimaan

esimerkki proaktiivisuuden puutteesta luku 4.3.2 (”Eri toimijoiden tietoturvariskien hallintavelvoitteet”).

[1220] Ks. lisää hyvistä käytänteistä luku 2.7 (”Tietoturvan sääntelyjärjestelmä ja hyvät käytänteet”).

[1221] Kaasalainen 2008: 79, 84; Ämmälä 1993: 19; Saarnilehto 1992: 15–16.

[1222] Ks. lisää perusteluita luvusta 1.5 (”Hyvä tapa tietoturvan sääntelyjärjestelmän elementtinä”).

[1223] Johdonmukaisuuden ja yhtenäisyyden vaatimuksista mm. luvussa 2.6.2 (”Kansallisen lainsäädännön tietoturvavelvoitteet”).

tietoturva riittävällä tasolla toiminnassaan. Täten *yksilöiden ja perusoikeuksien huomioiminen* on hyvän tietoturvan sääntelyjärjestelmän kriteeri.[1224]

Näiden tunnistettujen hyvän tietoturvan sääntelyjärjestelmän elementtien ja kriteerien pohjalta vastataan ensimmäiseen tutkimuskysymykseen, jota käsitellään seuraavaksi.

5.2 Onko nykyinen organisaatioiden tietoturvan sääntelyjärjestelmä hyvä?

Organisaatioiden tietoturvan sääntelyjärjestelmän kuvaaminen on tapahtunut kokoamalla yhteen organisaatioita velvoittavia säädöksiä, joiden myötä on tunnistettu elementtejä hyvän tietoturvan sääntelyjärjestelmän määrittelemiseksi. Näin ollen keskeiseksi kysymykseksi tämän tehtävän pohjalta muodostuu se, onko nykyinen tietoturvan sääntelyjärjestelmä hyvä? Hyvyyttä tässä oikeudellisessa tutkimuksessa tarkastellaan normikeskeisesti. Tunnistettujen hyvän tietoturvan sääntelyjärjestelmän elementtien tavoitteena on edistää samoja tavoitteita lainsäädännössä kuin tietoturvan tavoitteena on: suojata tietojen lisäksi yhteiskunnan ja organisaatioiden toimintaa ja jatkuvuutta sekä henkilöiden oikeuksia ja vapauksia[1225].

Eräs tässä tutkimuksessa tehty havainto on se, että tietoturvaan liittyvä lainsäädäntö on hajaantunut useaan eri säädökseen. Hajaantuminen synnyttää monia erilaisia ongelmia, jotka ovat sekä organisaatioiden käytäntöihin liittyviä, sisällöllisiä että oikeussystemaattisia. Tietoturvaa koskevien säädösten etsijän tulee osata etsiä tietoa eri lähteistä ja hahmottaa tietoturvaan liittyvän säädösjärjestelmän kokonaisuus, mikä aiheuttaa haasteita sen *tavoitettavuuden* ja *ymmärrettävyyden* osalta. Tietoturvaa koskevien säännösten sijoittuminen eri säädöksiin on omiaan johtamaan sisällöllisesti heterogeeniseen

[1224] Yksilöiden ja perusoikeuksien huomioimisen sisällyttämistä osaksi hyvän tietoturvan sääntelyjärjestelmän kriteerejä on käsitelty luvuissa 1.5 (” Hyvä tapa tietoturvan sääntelyjärjestelmän elementtinä”) sekä 2.5 (”Tietoturva perusoikeutena osana tietoturvan sääntelyjärjestelmää”). Ks. lisää yksilöiden vastuuttamisesta esimerkiksi luvuista 3.4.4 (” Tietoturvatoimenpiteiden käsitteistön yhdenmukaisuus”) ja 4.3.4 (”Fyysinen tietoturvallisuus osana riskienhallintaa)”.

[1225] Tietoturvallisuudella on moniulotteisia vaikutuksia, minkä takia myöskään sääntelyjärjestelmän näkökulmaa hyvyyden osalta ei ole nähty hyödylliseksi rajata vain tiettyyn näkökulmaan, kuten kuluttajan, juristin tai pienyrityksen näkökulmaan. Esimerkiksi kansallista kyberturvallisuuslakia koskevassa hallituksen esityksessä HE 57/2024 (s. 121) on todettu, että kyseisellä lakiesityksellä arvioidaan olevan yhteiskunnan häiriöttömän toiminnan edistämisen kautta välillisesti myönteisiä vaikutuksia kansalaisten turvallisuudelle. Tämä kuvastaa myös tietoturvallisuuden moniulotteisia vaikutuksia.

tietoturvasääntelyyn. Hajaantunut sääntely vaikeuttaa myös säännösten yhteensovittamista ja systemaattisen sääntelykokonaisuuden muodostamista, mikä lisää erityisesti tietoturvan sääntelyjärjestelmän *epäjohdonmukaisuutta ja epäyhtenäisyyttä*.

> Ensinnäkin hajaantumista koskevat ongelmat ilmenevät siinä, että tietoturvasääntely on osittain toteutettu muun sääntelyn osana. Esimerkiksi keskeisimmät organisaatioita koskevat tietoturvavaatimukset sisältyvät tietosuojalainsäädäntöön, sillä henkilötietoja suojataan tietoturvatoimenpiteillä. Näin ollen tietoturva ja tietosuoja toteutuvat käytännön toiminnassa rinnakkain, jolloin lainsäädännön tietosuojavaatimukset nostavat organisaatioiden tietoturvatasoa. Tietosuoja-asetus on suoraan sovellettava EU:n jäsenvaltioissa ja lisäksi henkilötietojen suoja on perusoikeutena perustuslaissa turvattu. Täten tietosuojalainsäädännön velvoittamat tietoturvatoimenpiteet ovat myös yhtenäisempiä ja kattavampia kohdistuessa kaikkiin organisaatioihin, mikä on erityisen positiivinen asia. Organisaatioiden tietoturvan kannalta työntekijöiden yksityisyyttä suojaava työelämän tietosuojalaki on yhtä lailla tärkeä säädös, joka on huomioitava tiettyjä tietoturvatoimia toteuttaessa. Lisäksi muun muassa kansallisen tietosuojalain 6 § velvoittaa organisaatioita toteuttamaan vähimmäistietoturvatoimenpiteitä, mikäli organisaatio käsittelee erityisiä henkilötietoryhmiä. Henkilötietolainsäädännön ohella on huomioitava sähköisen viestinnän luottamuksellisuutta ja yksityisyyttä suojaava sähköisen viestinnän palveluista annettu laki, jossa on tietoturvasäännöksiä tietoturvasta huolehtimiseksi sekä väärinkäytösten ehkäisemiseksi ja selvittämiseksi. Henkilötietoja ja yksityisyyttä suojaavan lainsäädännön hajaantuneiden tietoturvavaatimuksien tunnistaminen vaatii tietoturvan sääntelyjärjestelmän kokonaisvaltaista tuntemista, mikä saattaa vähentää säännöksien *tavoitettavuutta* etenkin maturiteettitasoltaan kypsymättömien organisaatioiden osalta.

> Toiseksi tietoturvan hajaantunut sääntely ilmenee siten, että se on toteutettu osittain toimialakohtaisesti. Esimerkiksi tietosuoja-asetuksen kanssa yhtä aikaa valmistellun, alkuperäisen NIS 1 -direktiivin asettamat verkkoja tietojärjestelmien tietoturvariskien hallintavaatimukset sekä tietoturvapoikkeamien ilmoittamisvelvoitteet implementoitiin kansalliseen lainsäädäntöön toimialakohtaisesti. Toimialakohtaiset tietoturvavaatimukset ovat kuitenkin epäyhtenäisiä, sillä riippuen toimialan yleisestä maturiteettitasosta turvallisuuden suhteen, joillekin keskeisten palvelujen tarjoajille on asetettu jo ennestään yksityiskohtaisempia turvallisuuden ja riskienhallinnan vaatimuksia. NIS 2 -direktiivin implementointi kumoaa NIS 1 -

direktiivin myötä tulleet toimialakohtaiset tietoturvariskien hallintavelvoitteet[1226], mutta tietoturvasääntely tulee edelleen olemaan hajaantunutta ja *epäyhtenäistä*, sillä joitain tietoturvavaatimuksia jäänee silti voimaan toimialakohtaisiin säädöksiin. Tämä lisää tietoturvan sääntelyjärjestelmän osalta *epäjohdonmukaisuutta* sekä vaikeuttaa *proaktiivisuutta* toimintaympäristön muutosten osalta. Lisäksi huomioitava on se, että NIS 2 -direktiivillä ja sen implementoivalla lainsäädännöllä asetetaan tietoturvavaatimuksia ”vain” keskeisille ja tärkeille toimijoille. Kuitenkin yhtä lailla NIS 2 -direktiivin vaatimukset heijastuvat näiden toimijoiden sopimuskumppaneihin eli mahdollisesti moneen ei-kriittiseen toimialaan, jotta keskeiset ja tärkeät toimijat voivat noudattaa lain vaatimuksia[1227]. Tällainen epäsuora vaikutus tekee tietoturvan sääntelyjärjestelmästä ristiriitaisen, jolloin sääntelyjärjestelmä ei näyttäydy niin *kohtuullisena* ja *oikeudenmukaisena*.

Kolmanneksi sääntelyn hajaantuminen ilmenee siten, että julkishallinnon ja yksityisen sektorin organisaatioiden sääntely poikkeaa toisistaan. Verrattuna toimialakohtaiseen tietoturvasääntelyyn, viranomaisia koskevat tietoturvavelvoitteet ovat kattavampia ja yksityiskohtaisempia. Viranomaisen tietoturvasta on säädetty muun muassa tiedonhallintalaissa, joka on tullut voimaan vuoden 2020 alussa. Julkisen hallinnon verkottuneen toimintaympäristön osalta on todettu tärkeäksi se, että tietoturvallisuuden toteuttaminen perustuu yhdenmukaisiin vaatimuksiin[1228]. Tämä edistää myös *yksilöiden ja perusoikeuksien huomioimista*. Tiedonhallintalain 4 luvun tietoturvavaatimukset ovat vähimmäiskriteereitä tietoturvan toteuttamiselle julkishallinnossa. Ne ovat samalla hyvä esimerkki riittävästä *teknologianeutraalista* sääntelystä, mutta on harmillista, että tällainen teknologianeutraali vähimmäissääntely kohdentuu vain julkishallintoon tietoturvan hyvien peruskäytänteiden osalta.

[1226] HE 57/2024 vp: 1, 61.

[1227] NIS 2 -direktiivin kohdan 83 ja 85 mukaisesti keskeisten ja tärkeiden toimijoiden tulisi arvioida ja ottaa huomioon toimittajiensa tuotteiden ja palveluntarjoajiensa palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet ja toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt. Saman tyyppinen vaatimus esiintyy myös hallituksen esityksessä 57/2024 kyberturvallisuuslain 9 §:n 4 kohdassa (s. 278, 302). On myös huomioitava HE 57/2024 (s. 93 ja 164), jonka mukaan keskeisiä ja tärkeitä toimijoita olisi erityisesti kannustettava sisällyttämään kyberturvallisuusriskien hallintatoimenpiteitä välittömien toimittajiensa ja palveluntarjoajiensa sopimusjärjestelyihin. Lisäksi nämä toimijat voisivat käsitellä myös alemman tason toimittajistaan ja palveluntarjoajistaan johtuvia riskejä.

[1228] HaVM 38/2018 vp: 17.

Neljänneksi sääntelyn hajaantuneisuus ilmenee siinä, että lainsäädännön tietoturvavaatimukset eivät täysin huomioi organisaatioiden *hyvien käytänteiden* muodostamaa kokonaisuutta. Tämä vaikuttaa suuresti säädösten väliseen *johdonmukaisuuteen* sekä siihen, että lainsäädäntö ei suojaa riittävän tehokkaasti tietoa sekä *yksilöiden perusoikeuksia*. Sääntelyn näkökulmasta tietoturvallisuus on laaja ja vaativa kokonaisuus, sillä se ulottuu ohjelmisto-, alusta- ja verkkoturvallisuudesta pääte- ja päätekäyttäjäturvallisuuteen asti: näin ollen vain osaa tästä kokonaisuudesta on pyritty sääntelemään tai ohjaamaan, mikä johtuu suureksi osaksi siitä, että tietoturvaa ei ole tunnistettu asianmukaisesti yleisenä oikeusperiaatteena[1229]. Lisäksi monet tietoturvavaatimukset painottavat tiettyä näkökulmaa, esimerkiksi järjestelmien tietoturvallisuutta, henkilötietojen suojaa tai viranomaisten asiakirjojen suojaa. Nämä näkökulmat ovat kuitenkin vain pieniä osa-alueita organisaation tietoturvasta. Esimerkiksi fyysisen tietoturvallisuuden osa-alueesta on hyvin vähän mainittu sellaisenaan voimassa olevassa lainsäädännössä. Toisena esimerkkinä fyysisten tietoturvakontrollien, kuten kameravalvonnan[1230], painotus kohdistuu tietosuojanäkökulmaan. Fyysisen tietoturvallisuuden huomioiminen lainsäädännössä on kuitenkin parantunut, sillä NIS 2 -direktiivin mukaisten toimijoiden on otettava huomioon myös verkko- ja tietojärjestelmien fyysinen turvallisuus[1231]. Tosin velvoittavuus rajautuu tällöinkin vain tiettyyn, laissa määriteltyyn toimijajoukkoon – ei kattavasti kaikkiin organisaatioihin.

Viimeiseksi tietoturvan hajaantunut sääntely ilmenee käsitteiden epäyhtenäisyytenä ja epäjohdonmukaisuutena eri säädöksien välillä, joka voi vähentää säännöksien *ymmärrettävyyttä*. Ainoastaan täsmällinen ja ristiriidaton käsitteistö mahdollistaa säädöstulkinnan, joka on luotettava[1232]. Esimerkiksi tietoturvatoimenpiteitä kuvaavat käsitteet vaihtelevat eri säädöksissä: tietosuojalainsäädännössä käytetään käsitettä tekniset ja organisatoriset toimenpiteet, yksityisyyttä suojaavassa sähköisen viestinnän palvelulaissa käytetään käsitettä hallinnolliset ja tekniset toimenpiteet, viranomaisen tiedonhallintalaissa käytetään käsitettä hallinnolliset, toiminnalliset ja tekniset toimenpiteet eli tietoturvallisuustoimenpiteet ja NIS 2 -

[1229] Saarenpää & Riekkinen 2023: 178.
[1230] Ks. työelämän tietosuojalaki, jonka 5 luvussa on koottuna yksityiskohtaiset säännökset liittyen kameravalvontaan työpaikalla. Tässä tutkimuksessa aihetta on käsitelty luvussa 3.5.2 (”Kameravalvonta”).
[1231] Alkuperäinen NIS 1 -direktiivi otti huomioon tilaturvallisuuden, mutta vaatimus rajautui suppeammin vain rajattuun toimijajoukkoon. Fyysisen turvallisuuden vaatimuksia on käsitelty tarkemmin luvussa 4.3.4 (” Fyysinen tietoturvallisuus osana riskienhallintaa). Ks. myös lisää fyysisen turvallisuuden vaatimuksista 3.5.2 (”Kameravalvonta”) ja 3.5.3 (”Kulunvalvonta”).
[1232] Aarnio 1997: 40, 44.

> direktiivin toimeenpanevassa kansallisessa kyberturvallisuuslaissa käytetään käsitettä tekniset, operatiiviset ja organisatoriset toimenpiteet eli kyberturvallisuusriskien hallintatoimenpiteet[1233]. Osa käsitteistä painottaa selkeästi teknistä tietoturvallisuutta, kun taas osa painottaa toimenpiteitä henkilötietojen suojaamiseksi. Tiedonhallintalain käsite tietoturvallisuustoimenpiteet on näistä kolmesta kattavin hyvien tietoturvallisten käytänteiden kannalta, mutta se keskittyy näkökulmaltaan viranomaisen tietoaineistojen turvallisuuden takaamiseen. Jo lain valmisteluvaiheesta lähtien tulisi pyrkiä tuottamaan edellytykset tietoturvaa koskevan termistön selkiyttämiselle ja vakinaistamiselle[1234].

Onko sitten tutkimuskysymyksen mukaisesti nykyinen organisaatioiden tietoturvan sääntelyjärjestelmä hyvä? Positiivisena seikkana voidaan todeta, että teknologianeutraalisuuden periaate yhtenä tutkimuksen kriteerinä toteutuu hyvin nykyisessä tietoturvan sääntelyjärjestelmässä. Kuitenkin edellä nostettujen havaintojen perusteella tietoturvalainsäädännön hajaantuneisuus aiheuttaa monenlaisia ongelmia, jotka vaikuttavat negatiivisesti erityisesti tietoturvan sääntelyjärjestelmän yhtenäisyyteen ja johdonmukaisuuteen, tavoitettavuuteen, tehokkuuteen ja ymmärrettävyyteen. Toimiala- ja viranomaispainotteinen, säännöksiltään hajaantunut tietoturvan sääntelyjärjestelmä ei tule olemaan proaktiivisesti ja ketterästi mukana digitaalisen ympäristön muutoksissa. Se ei myöskään edistä riittävällä tasolla yksilöiden perusoikeuksien toteutumista, kuten yksilöiden oikeutta henkilötietojensa suojaan. Tällainen sääntelyjärjestelmä ei näyttäydy kohtuullisena ja oikeudenmukaisena, sillä se ei velvoita kaikkia toimijoita hyvän tietoturvatavan mukaisiin tietoturvatoimenpiteisiin. Eri säädöksiin hajaantunut tietoturvasääntely ei huomioi kattavasti organisaatioiden hyvien tietoturvakäytänteiden kokonaisuutta. Koska aikaisemmin mainitut kriteerit eivät täysin täyty, nykyinen tietoturvan sääntelyjärjestelmä ei ole normikeskeisesti tarkasteltuna hyvä.

Tietoturvasääntelyn hajaantumisen useaan eri säädökseen ei tulisi hankaloittaa käytännön tietoturvatyötä organisaatioissa. Lainsäädännössä määritellyt tietoturvavelvoitteet ovat suurimmaksi osaksi yleisluonteisia, jolloin riittävän tietoturvallisuuden tason määrittely ja käytännön toteutus on jätetty organisaatioiden vastuulle. Lainsäädäntö ei ole myöskään ainoa lähde, joka ohjaa organisaatioiden tietoturvavelvoitteita. Lainsäädännön lisäksi organisaatioiden tulee tunnistaa sopimuksiin perustuvat tietoturvavelvoitteet ja oikeudet. Organisaatioiden tietoturvatyö on käytännönläheistä ja toisinaan erittäin hektistä. Organisaatioilla ei välttämättä ole kaikissa tilanteissa aikaa taikka mahdollisuutta tulkita lain sisältöä ja

[1233] Ks. luku 3.4 (”Tietoturvan sääntelyjärjestelmän erilaiset tietoturvatoimenpiteet”).
[1234] Kinnunen 2015: 167.

tarkoitusta perusteellisesti.[1235] Lainsäädännön tulee olla yksinkertaista ja selkeää, jotta sitä on helppo hallita ja jotta se edistää digitalisaatiota[1236]. Oikeudellisen informaation keskeisiä tavoitteita ovat muun muassa tavoitettavuus, virheettömyys ja ymmärrettävyys. Ymmärrettävyyden pitäisi toteutua oikeudellisten tekstien sisäisessä ja ulkoisessa luotettavuudessa sekä oikeudellisten merkkien selkeydessä.[1237] Tässä tutkimuksessa tehdyllä tietoturvan sääntelyjärjestelmän kuvaamisella on pyritty osaltaan parantamaan sääntelyjärjestelmän tavoitettavuutta ja ymmärrettävyyttä. Lisäksi tutkimuksessa tehty eri säädöksien kokoamistyö on omiaan lisäämään myös säädösjärjestelmän yhtenäisyyttä ja johdonmukaisuutta. Tämä tutkimustyö ei kuitenkaan vähennä lainsäädännön yhtenäistämisen tarvetta. Näin ollen seuraavassa tutkimuskysymyksessä on arvioitu lainsäädännön yhtenäistämiseksi sekä hyvän tietoturvan sääntelyjärjestelmän parantamiseksi yleisen tietoturvalain säätämistarvetta eräänlaisena ratkaisuna edellä nostettuihin ongelmiin.

5.3 Onko Suomessa tarpeen kansallinen tietoturvalaki?

Suomessa ei ole yleistä tietoturvalakia, mutta sen sijaan tietoturvaa koskevia säännöksiä on lukuisia. Tietoturvavaatimuksia on asetettu kaikille organisaatioille erityisesti kattavan tietosuojalainsäädännön myötä. Lisäksi NIS 2 -direktiivin myötä toimeenpannaan kattava kyberturvallisuuslaki, joka ei tosin koske kaikkia organisaatioita. Tarvitaanko silti kansallista tietoturvan yleislakia? Tietoturvan yleislaki ideana ei ole uusi ja sitä on toivottu jo pitkään.

Ensinnäkin yleinen tietoturvalaki on perusteltavissa sillä, että se edistäisi ja turvaisi henkilöiden perusoikeuksien toteutumista. Tehokas tietoturva ei voi rajautua vain tiettyihin säännöksiin, vaan sen tulisi heijastua myös meta- ja oikeusperiaatteista. Metaperiaatteet heijastavat oikeusjärjestyksen ydinarvoja ja kertovat ihmis- ja perusoikeuksista. *Oikeus tietoturvaan* metaperiaatteena onkin oleellinen osa hyvää tietoturvan sääntelyjärjestelmää, sillä henkilöiden oikeuksia suojataan tietoturvatoimenpiteiden avulla ja lisäksi asianmukaisen tietoturvan myötä voidaan taata nykyisen verkkoyhteiskunnan informaatioinfrastruktuurin toimivuus[1238]. Näin ollen tietoturvan sääntelyjärjestelmässä tulisi korostaa myös yksilöiden oikeutta kyberturvaan perusoikeustason periaatteena tai

[1235] Laaksonen, Nevasalo & Tomula 2006, s. 18, 21, 27.
[1236] Korkea digitalisointiaste edellyttää myös tietoturvan korkeaa priorisointia. Ks. Valtiovarainministeriön julkaisuja 2023:8: 15, 17.
[1237] Korhonen 2003: 25.
[1238] Saarenpää 2016a: 123, 218; Saarenpää & Riekkinen 2023: 177.
Metaperiaatetasolla tietoturva nähdään ensisijaisesti yhteiskunnan toimivuuden ja yksilön oikeuksien toteutumisen takeena. Ks. Råman 2006a, s. 819.

jopa oikeusperiaatteena, sillä verkottuneessa ja järjestelmäriippuvaisessa yhteiskunnassamme kyberuhat muodostavat yhä vakavammat ja todennäköisemmät riskit yksilöiden kannalta.[1239] Perustuslaistamme on jo johdettavissa tiettyjä tietoturvaan liittyviä perusoikeuksia[1240], esimerkiksi oikeus turvallisuuteen (PL 7 §) ja omaisuuden suojaan (PL 15 §), oikeus yksityiselämän ja henkilötietojen suojaan sekä viestinnän luottamuksellisuuteen (PL 10 §), oikeus sananvapauteen ja oikeus saada tieto viranomaisen julkisesta asiakirjasta (PL 12 §)[1241]. Tietovarantojen kasvun ja digitalisaation kehittymisen ohella moni nykyisistä perusoikeuksista ei kuitenkaan toteudu ilman tietoturvatoimenpiteitä. Ihmisten tullessa yhä riippuvaisemmiksi sähköisistä palveluista, myös tietoturvapoikkeamat laajenevat koskemaan yhä useampaa organisaatiota ja samalla niiden vaikutukset luonnollisiin henkilöihin kasvavat suuriksi ja näkyvimmiksi. Tästä syystä tietoturvavaatimuksien huomioiminen on tärkeää lainsäädännön tasolla muidenkin organisaatioiden kuin viranomaisten taikka tiettyjen keskeisten tai tärkeiden toimijoiden osalta. Oikeuden uudistumista tarvitaan yksilön oikeuksien suojaamiseksi ja uudenlaisten ristiriitojen ratkaisemiseksi[1242]. Organisaatioita velvoittavien, hyvän tietoturvatavan mukaisten vähimmäisvaatimusten osalta on tärkeää, että ne muotoutuisivat tavanomaisen oikeuden sisällä olevista hyvistä, vakiintuneista tietoturvakäytänteistä[1243]. Huomioitava kuitenkin on se, että hyvän tavan mukaisuuden määrittely tulisi sitoa myös oikeusjärjestyksen sisälle, jolloin määrittelyn tulisi nojautua yhteiskunnan arvoja ilmentäviin perustuslain perusoikeuksiin[1244]. Näin ollen tietoturvan yleislain tarve sitoutuu hyvin paljon tarpeeseen tunnistaa *oikeus kyberturvaan* perusoikeutena. Hyvä tietoturvatapa tulisi myös tunnistaa lakisääteisenä hyvänä tapana osana tietoturvan sääntelyjärjestelmää, ja sen sisältöä voisi täydentää oikeuskäytännön, käytännesääntöjen, tietoturva-alan hyvien käytänteiden ja esimerkiksi tietosuojavaltuutetun päätösten ja linjausten ohella kaikkia organisaatioita velvoittavilla tietoturvan vähimmäisvaatimuksilla.

[1239] Ks. luvut 2.4.1 (”Oikeus tietoturvaan periaatteena”)
[1240] Tietoturvaan liittyviä perusoikeuksia on käsitelty yksityiskohtaisemmin luvussa 2.5 (”Tietoturva perusoikeutena osana tietoturvan sääntelyjärjestelmää”).
[1241] Ks. luku 2.5.6 (” Perusoikeuksien turvaaminen oikeusvaltiossa ja hyvä hallinto ”). Viranomaisia koskee erityisesti perustuslain 22 §, sillä kyseisen säännöksen mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen, eli viranomaisen on otettava toiminnassaan huomioon myös tietoturva-asiat. Perustuslain 21 §:n jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivästystä lain mukaan toimivaltaisessa viranomaisessa, jolloin vaatimus tietojärjestelmien laadukkaasta ja häiriöttömästä toiminnasta korostuu. Lisäksi perustuslain 2 §:n oikeusvaltioperiaatteen mukaan julkisen vallan tulee perustua lakiin, jolloin myös tietoturvan viranomaisvastuut tulee perustua lainsäädäntöön (ks. HE 1/1998 vp, s. 74).
[1242] Pöysti 1999: 297.
[1243] Ks. lisää hyvästä tavasta luku 1.5 (”Hyvä tapa tietoturvan sääntelyjärjestelmän elementtinä”).
[1244] Ks. myös Meri 2023: 67–68, 74.

Toinen peruste yleisen tietoturvalain tarpeelle liittyy voimassa olevan tietoturvan säädösjärjestelmän hajanaisuuteen ja heterogeenisuuteen. Lainsäädännön hajanaisuus, selkeän systematiikan puuttuminen sekä riittävän laajan ajattelun ja näkökulmien puute ovat jatkuvia ongelmia tietoturvalainsäädännössä[1245]. Oikeusvaltiomme yksi periaatteista on säädösten ymmärrettävyys, mikä tarkoittaa sitä, että lakitekstien tulisi olla helposti ymmärrettäviä jokaiselle[1246]. Vaikka voimassa olevat säädökset ovat helposti ja nopeasti saatavissa internetistä, säädösten hajanaisuus ja käsitteiden epäyhtenäisyys voivat aiheuttaa ristiriitoja lain tulkinnassa. Säädösten määrän lisääntyessä vaaditaan entistä enemmän suurta säännösmäärän tuntemusta, mikä vaikeuttaa entisestään säännösviidakosta selviytymistä[1247].

> Tietoturvallisuudesta huolehtiminen yksittäisin ohjeistuksin ja säännöksin sekä hyvän tietojenkäsittelytavan puitteissa ei ole riittävää nyky-yhteiskunnan uusien riskien takia. Näin ollen kattava, yleinen tietoturvalaki sekä tietoturvaperiaate ovat tarpeellisia. Yleinen tietoturvalaki edistäisi tietoturvaasioiden oikeudellista ymmärtämistä ja oikeudellisen tärkeyden osoittamista. Myös perustuslakia tulisi muuttaa niin, että tietoturvallisuuden merkitys perusoikeutena tulisi selkeämmin esiin.[1248]

> Tietoturvallisuuden jättäminen yksittäisten erillissäännösten varaan velvoittaa vain tietyn toimialan toimijoita. Myöskään rikosoikeudellisten sanktioiden varaan ei hyvää tietoturvaa voida jättää. Yleinen tietoturvalainsäädäntö tulisi ulottaa koskemaan kaikkia yhteiskunnan toimijoita, sen tulisi olla teknologianeutraali ja sen tulisi sisältää kaikki toimet tietojärjestelmien elinkaaren ajalta suunnittelusta sanktiosäännöksiin saakka. Lisäksi yleisen tietoturvalain tulisi sisältää yhteys ihmis- ja perusoikeuksiin. Tämä parantaisi luottamusta digitalisaation tarjontaan ja kysyntään, mikä myös edistäisi digitalisaatiota itsessään.[1249]

> Tietoturvan yleislaista voitaisiin poiketa sekä erityislailla että tietyissä tapauksissa sopimuksella. Sopimusvapautta ei rajoitettaisi, vaan sopijapuolet voisivat järjestää suhteensa muullakin kuin säännöksissä tarkoitetulla tavalla. Tällainen sääntely vähentäisi myös neuvottelu- ja sopimuskustannuksia, sillä kaikissa sopimussuhteissa ei ole tarpeen sopia yleisestä normeista poikkeavia järjestelyjä. Yleislaki konkretisoisi myös

[1245] Pöysti 2023: 44.
[1246] Korhonen 2016: 55. Tässä yhteydessä on myös huomioitava, että säädösten käyttäjien oikeudellinen lukutaito saattaa vaihdella suuresti (ks. Saarenpää 2016c: 38.)
[1247] Saarenpää 2016a: 84, 113, 240, 272; Saarenpää & Riekkinen 2023: 203, 287.
[1248] Ibid.
[1249] Lehtonen 2016: 272–273.

> erityislainsäädäntöä ja sen tietoturvallisuusvelvoitteiden oikeudellista sisältöä. Tällöin tietoturvallisuudella olisi yhteinen säädöspohja, josta poikkeaminen edellyttäisi erityisiä perusteita. Tietoturvallisuusnormien velvoittavuutta tehostettaisiin sanktioilla, jolloin seuraamuksena voisi koitua esimerkiksi vahingonkorvausvelvollisuus tai sopimustilanteissa oikeustoimen pätemättömyys.[1250]

Tietoturvallisuus sisältyy tavoitteena lukuisiin säädöksiin. Se mainittiin vuoden 2022 lopulla 116 säädöksessä. Laajassa merkityksessä tietoturvasäädöksinä voidaan pitää myös erityislainsäädännön salassapito- ja vaitiolosäännöksiä.[1251] Näillä säännöksillä pyritään nimenomaan turvaamaan salassa pidettävää tai muuta luottamuksellista tietoa, jotta sitä ei vuotaisi organisaation ulkopuolelle.

Kehittyvä tietoturvasääntely kertoo siitä, että tietoturvallisuus on noussut entistä merkittävämmäksi asiaksi EU:ssa. Esimerkiksi kyberturvallisuusasetuksen ollessa suoraan sovellettavaa lainsäädäntöä on pohdittu, onko yleinen tietoturvallisuuslaki meillä sittenkään enää tarpeen. Yleistä tietoturvallisuuslain tarvetta voidaan kuitenkin edelleen perustella sillä, että kyberturvallisuusasetus tähtää ensisijaisesti infrastruktuureihin. Tietoturvallisuus on merkittävästi laajempi ilmiö.[1252]

Tiedonhallintalain toimiessa eräänlaisena julkisen sektorin tietoturvalakina ja ilmentäessä viranomaisen tietoturvan vähimmäisvaatimuksia, myös muut organisaatiot tarvitsevat kotimaista säädöskehystä. Omalta osaltaan EU:n yleisen tietosuoja-asetuksen tietoturvamääräykset edesauttavat kotimaista sääntelytilannetta. EU-sääntely ei ole myöskään nähty poistavan tarvetta täydentää perustuslakia tietoturvasäännöksellä.[1253] Tietosuojaa koskevan lainsäädännön osalta yleisesti sovellettavaa tietosuojalainsäädäntöä täydentävästä sääntelystä tulisi lähtökohtaisesti pidättäytyä ja myös erityislainsäädännön tarvetta tulisi arvioida riskiperusteisesti. Perustuslakivaliokunnan mukaan, mitä korkeampi riski henkilötietojen käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä hetkellä Suomessa on kuitenkin voimassa satoja erityislakeja, jotka sisältävät henkilötietojen käsittelyä koskevaa sääntelyä.[1254] Tämä korostaa sitä, kuinka hajanaista kansallinen tietoturva- ja tietosuojasääntely on.

[1250] Pöysti 1997: 526, 528, 579.
[1251] Saarenpää & Riekkinen 2023: 86. Ks. myös luku 2.5.5 (”Julkisuusperiaate sekä salassapitointressi”).
[1252] Saarenpää & Riekkinen 2023: 86, 204.
[1253] Saarenpää & Riekkinen 2023: 204.
[1254] Liikenne- ja viestintäministeriön julkaisuja 2021:1: 31; PeVL 14/2018 vp: 4–5.

NIS 2 -direktiivin implementoiva kyberturvallisuuslaki on kattava. Lisäksi se tulee yhtenäistämään etenkin toimialakohtaisia tietoturvavaatimuksia, sillä se kumoaa valtaosan NIS 1 -direktiivin myötä voimaan tulleista toimialakohtaista säännöksistä sekä laajentaa kriittisten toimialojen luetteloa.[1255] Joitain tietoturvavaatimuksia jää silti voimaan toimialakohtaisiin säädöksiin, jolloin tietoturvan sääntely on edelleen hajaantunutta ja epäyhtenäistä. Yleislakina toimiva kyberturvallisuuslaki ei aseta suoria vaatimuksia esimerkiksi pienyrityksille ja muille "vähemmän tärkeille" toimialoille. Se ei ulotu kaikkiin organisaatioihin samalla tavalla kuin henkilötietojen suojaamiseen liittyvä tietosuojalainsäädäntö. *Yleislakina* kyberturvallisuuslaki korostaa ainoastaan lakien etusijajärjestystä, mutta siihen se jää, eli se ei ole todellinen yleislaki. Vaikka NIS 2 -direktiivin (ja sitä myöten kyberturvallisuuslain) vaatimukset eivät suoraan kohdistu muihin kuin kriittisiin toimialoihin, sen vaatimukset todennäköisesti heijastuvat keskeisten ja tärkeiden toimijoiden sopimuskumppaneihin, jotta keskeiset ja tärkeät toimijat voisivat toteuttaa lain määrittämät velvollisuutensa. Käytännössä lain vaatimusten ja sopimusjärjestelyiden seurauksena keskeisten ja tärkeiden toimijoiden toimitusketjuista tulisi rajautua tietoturvatasoltaan epäkypsät organisaatiot pois, jotka saattavat olla pieniä tai tuoreita yrityksiä ja sijoittuvat myös näille ”vähemmän tärkeille” toimialoille. Tietoturvaa koskeva lainsäädäntö näyttäytyy tulevaisuudessakin sirpaloituneena ja epäjohdonmukaisena, sekä aavistuksen kohtuuttomana ja epäoikeudenmukaisena. Edellä mainitut seikat korostavat tietoturvallisuuden todellisen yleislain tarvetta, joka asettaisi tietoturvan vähimmäisvaatimuksia myös sellaisille toimialoille, joissa tietoturvan kypsyystaso todennäköisesti on matalampi[1256]. Näillä vähimmäisvaatimuksilla mitigoitaisiin myös nykyisen verkottuneen yhteiskunnan toimitusketjuriskejä.

[1255] HE 57/2024 vp, s. 1, 61. Ks. myös lisää luku 4.3.1 (”Keskeisten, tärkeiden ja kriittisten toimijoiden jaottelu , lainsäädännössä”). NIS 2 -direktiivin liitteissä I ja II korostetaan *kriittisiä toimialoja*, mutta itse direktiivin toimijat ovat keskeisiä ja tärkeitä. Sen sijaan kriittiset toimijat sijoittuvat CER-direktiiviin. Tällainen jaottelu tekee käsitteiden ja systematiikan osalta kyseisestä direktiivistä sekavan. NIS 2 -direktiivin **liitteessä I** määriteltyjä erittäin kriittisiä toimialoja ovat energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, tieto- ja viestintätekniikkapalveluiden (TVT-palvelujen) hallinta, julkishallinto ja avaruus. **Liitteessä II** määriteltyjä muita kriittisiä toimialoja ovat posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus, tuotanto ja jakelu, elintarvikkeiden tuotanto, jalostus ja jakelu, valmistus, digitaalisen palvelun tarjoajat ja tutkimustoiminta.

[1256] Eurooppa-neuvosto on kannanotossaan korostanut pienten ja keskisuurten yritysten (pk-yritykset) merkitystä kyberturvallisuusekosysteemissä (ks. Euroopan unionin neuvosto, Neuvoston päätelmät EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle 22.3.2021: 7). Lisäksi Eurooppa-neuvosto on varoittanut erityisesti kyberturvallisuussääntelyn hajanaisuudesta ja päällekkäisyyksistä Unionissa sektorikohtaisten tai erityissäädösten *lex specialis* takia. Kyberturvallisuus ei ole ainoastaan sektorikohtaista vaan horisontaalista. Ks. Euroopan unionin neuvosto, Council Conclusions on the Future of Cybersecurity: implement and protect together 21.5.2024: 7.

> Lainsäädännössä on oltava riittävät tietoturvaa ja tietosuojaa koskevat vaatimukset ja määräyksenantovaltuudet, joita voidaan täydentää velvoittavilla alemman tasoisilla määräyksillä. Lainsäädännön tasolla korostuu vähimmäisvaatimusten määritys.[1257]

Euroopan unionin ja Suomen kansallinen lainsäädäntö ovat muuttuneet, jolloin digitaalisen verkkoyhteiskunnan riskeihin puuttuminen on tullut lainsäädännössä selkeämmäksi. Kuitenkin hajanainen lainsäädäntö johtaa siihen, että yhtenäinen kokonaiskuva riskeistä voi kadota monien yksityiskohtien keskelle. Yksi oikeudellisen sääntelyn riski on yleisten kyber- ja tietoturvallisuusvaatimusten puuttuminen sekä EU:n hajanainen lähestyminen aiheeseen eri säädöksin. Kyber- ja tietoturvallisuus ovat osa infrastruktuurien laatua, mutta ne ovat myös keskeisiä yhteiskunnallisia tarpeita.[1258] EU:ssa on tunnistettu kyberturvallisuuden osalta ylisääntelyä, mutta samalla kehotettu varmistamaan johdonmukaisempi lähestymistapa tulevissa aloitteissa, jolloin voitaisiin vahvistaa tai täydentää nykyisiä rakenteita ja välttää tarpeetonta monimutkaisuutta sekä päällekkäisyyttä lainsäädännössä[1259]. Kansallinen tietoturvallisuuden yleislaki tavoittelisi nykyisen, kansallisen sääntelyjärjestelmän selkeyttämistä vähentämällä päällekkäistä ja hajanaista sääntelyä sekä ulottamalla vähimmäisvaatimukset kaikkiin toimijoihin. Tällainen sääntely ei estäisi yritysten markkinoille pääsyä tai innovointia, vaan päinvastoin. Yritysten markkinoille pääsy on helpompaa, kun turvallisuusasiat ovat kunnossa: tietoturva luo kilpailukykyä[1260] ja se on merkki laadukkaasta palvelusta. Sanomattakin on selvää, että lähtökohtaisesti innovointia ei voi tehdä yksilöiden oikeuksien ja verkkoyhteiskunnan toimivuuden kustannuksella.

Tietoturvan yleislailla olisi mahdollista asettaa tietoturvatoimenpiteille vähimmäistaso samaan tapaan kuin tietosuojalainsäädännössä suojataan henkilötietoja. Lainsäädäntöä täsmennettäisiin, jolloin keskiössä henkilötietojen suojaamisen ohella olisi myös organisaation muiden tietojen turvaaminen. Tällaiset tietoturvan vähimmäisvaatimukset ulottuisivat kaikkiin organisaatioihin hyvänä tietoturvatapana, jolloin tietoturvan vähimmäistaso yhtenäistyisi ja yksilöiden perusoikeuksia suojattaisiin tehokkaammin. Pienempien liiketoimintaa harjoittavien toimijoiden osalta tavoitteena tietoturvan osalta olisi erityisesti parempi asiakkaiden ja työntekijöiden henkilötietojen sekä liikesalaisuuksien suojaaminen. Kaikkia organisaatioita koskevien tietoturvavaatimusten koostaminen yhteen lakiin ei myöskään

---

[1257] Liikenne- ja viestintäministeriön julkaisuja 2021:1: 21–22, 24, 26, 50.
[1258] Pöysti 2023: 41–42, 45, 53. Ks. erityisesti s. 45–53, joissa on Pöystin listaus digitaalisen verkkoyhteiskunnan keskeisistä kyber- ja tietoturvallisuuden riskeistä.
[1259] Ks. esimerkiksi Euroopan unionin neuvosto, Council Conclusions on the Future of Cybersecurity: implement and protect together 21.5.2024, s. 7.
[1260] Vastaavaa on todettu myös esim. LiVM 10/2014 vp, s. 4, 18; Elinkeinoelämän keskusliitto 2018: 8; Suomen tietoturvallisuusstrategia 2016: 15–18.

estäisi sitä, että samassa laissa säädettäisiin korotettuja vaatimuksia keskeisille, tärkeille ja kriittisille toimijoille. Näiden osalta valvonta olisi myös tehostetumpaa, kuten NIS 2 -direktiivissä on määritelty.

Kolmas peruste tietoturvan yleislaille on se, että tietoturvaan ja tietosuojaan liittyvät haasteet nähdään usein kannustinongelmana. Tämän ongelman ratkaisemiseksi sääntelijän tehtävänä on luoda järjestelmä, jossa yksittäisellä toimijalla on riittävät kannustimet hankkia ja ylläpitää riittävää tietosuojan ja tietoturvan tasoa. Tällaisen kannustinjärjestelmän tulisi sisältää sekä ennaltaehkäiseviä että jälkikäteisiä toimia. Ennaltaehkäiseviä toimia olisi sääntely, jonka myötä tietoturva- ja tietosuojalainsäädännössä säädettäisiin vähimmäisvaatimuksista. Jälkikäteisiä toimia olisivat esimerkiksi valvonta ja sanktiot[1261] riittämättömästä tietoturvan ja tietosuojan tasosta. Myös konkreettinen tiedottaminen tietoturvavaatimuksista, niiden saavuttamiseksi tehtävistä toimista sekä sanktioista on mahdollisesti hyödyllinen ja kustannustehokas malli kannustamaan yksittäisiä toimijoita huolehtimaan tietoturvan ja tietosuojan tasostaan.[1262] Lainsäädännön tulisi olla tavoitettava sellaisille yrityksille, joissa tietoturvan maturiteettitaso on alhainen.

Organisaatioiden valitsemaan tietoturvatasoon vaikuttaa moni asia. Paremman tietoturvatason valitsemisen tekijöinä voivat olla esimerkiksi lakisääteiset velvoitteet sekä pelot mainehaitoista ja pääoman menetyksestä. Heikomman tietoturvatason valitsemisen syinä voivat olla esimerkiksi tietoturvatoimenpiteiden kustannukset, turvallisuustoimenpiteiden vaikutus toiminnan sujuvuuteen ja helppouteen sekä osaamisen puute. Tietoturvan yleislain kaikkia organisaatioita koskevien vähimmäisvaatimuksien velvoittavuutta tulisikin tehostaa sanktioilla, jolloin niistä voisi koitua esimerkiksi vahingonkorvausvelvollisuus tai sopimustilanteissa oikeustoimen pätemättömyys. Lisäksi sovellettavaksi voisivat tulla esimerkiksi rikoslain 38 luvun 9 §:n mukaisen tietosuojarikoksen rangaistussäännökset. Näillä sanktioilla vastuutettaisiin myös yksilöitä paremmin huolehtimaan organisaation tietoturvasta.

Nykyisessä verkottuneessa yhteiskunnassa monet organisaatiot ovat riippuvaisia toisistaan ja muiden organisaatioiden tuottamista palveluista ja toiminnoista. Tietoturvallisuuden toteutumisen pitäisi siksi perustua yhdenmukaisiin

[1261] Tietosuojapuutteiden osalta sanktiointi onkin varsin kattavaa. Kansallisen valvontaviranomaisen langettamat hallinnolliset sanktiot voivat olla hallinnollinen sakko, säännölliset tarkastukset tai kirjallinen varoitus, jonka myötä tietosuoja-asetus siirtää viranomaistoiminnan painopistettä ennakollisesta vaikuttamisesta jälkikäteistä sanktiointia kohden (Riekkinen 2016b, s. 423). Valvontaviranomainen voi määrätä Suomen tietosuojalain 22 §:n mukaisesti uhkasakon, joka on eri asia kuin tietosuoja-asetuksen hallinnollinen sakko (Nyyssölä 2018, s. 67).

[1262] Liikenne- ja viestintäministeriön julkaisuja 2021:1: 21–22, 24, 26, 50.

vaatimuksiin, jotka koskevat kaikkia organisaatioita – ei pelkästään julkista hallintoa taikka muita keskeisiä, tärkeitä ja kriittisiä toimijoita. Kansallista tietoturvalainsäädäntöä olisi mahdollista uudistaa ja yhtenäistää niin, ettei jokaiselle toimijalle tarvitsisi säätää omia tietoturvavelvoitteitaan EU-lakimuutosten yhteydessä ja toiminta- ja riskiympäristön muutosten myötä[1263].

[1263] On myös välttämätöntä huomioida EU:n lainvalmistelussa parhaillaan oleva tietosuoja-asetusta täydentävä sähköisen viestinnän tietosuoja-asetus (ePrivacy-asetus) erilaisten tietojen tietoturvaperusteista käsittelyä arvioitaessa. Kun asetus aikanaan hyväksytään, se harmonisoinee jäsenvaltioissa tapahtuvaa välitystietojen tietoturvaperusteista käsittelyä, jolloin myös sen voimaantulon yhteydessä olisi otollinen hetki Suomen kansallisen tietoturvalainsäädännön uudelleentarkastelulle. Ks. Heiskanen 2020, s. 131.

Lähdeluettelo

Aarnio, Aulis (1982). *Oikeussäännösten tulkinnasta – Tutkimus lainopillisen perustelun rationaalisuudesta ja hyväksyttävyydestä*. Helsinki: Juridica.

Aarnio, Aulis (1989). *Laintulkinnan teoria : yleisen oikeustieteen oppikirja*. Porvoo: WSOY.

Aarnio, Aulis (1997). *Oikeussäännösten systematisointi ja tulkinta*. Teoksessa Minun Metodini. Toimittanut: Juha Häyhä. Helsinki: WSOY, s. 35–56.

Aarnio, Aulis (2006). *Tulkinnan taito – Ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta*. Helsinki: WSOY. 428 s. ISBN 951-0-32116-8.

Aarnio, Aulis (2010). *Hyvän asianajajatavan eettinen perustelu – Kunniakoodista kultaiseen sääntöön*. Defensor Legis N:o 5/2010, s. 541–547.

Aarnio Aulis (2011). *Luentoja lainopillisen tutkimuksen teoriasta*. Helsinki: Helsingin yliopiston oikeustieteelliset julkaisut.

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. https://doi.org/10.1016/j.diin.2018.01.012

Alapuranen, Leena (2020). *Työelämän henkilötietojen käsittelyedellytykset*. Teoksessa: Henkilötietojen käsittely työelämässä. 3. uudistettu painos Keuruu: Edita Publishing Oy, s. 5–168.

Alasoini, Tuomo (2015). *Digitalisaatio muuttaa työtä – millaista työelämää uudistavaa innovaatiopolitiikkaa tarvitaan?* Työpoliittinen aikakauskirja 2/2015. Työ- ja elinkeinomisteriö. http://urn.fi/URN:NBN:fi-fe2016100724889

Alavesa, Eija (2016). *Tietoturvallisuuden sääntely, tausta, tekijät ja tulevaisuus – Missä mennään nyt?* Teoksessa: Society Trapped in the Network – Does it have a future? Rovaniemi: Lapin yliopisto, s. 214–267. https://urn.fi/URN:ISBN:978–952–484–917–3

Alepis, E.; Michota, A.; Patsakis, C.; Pocs, M. & Politou, E. (2018). *Backups and the right to be forgotten in the GDPR: An uneasy relationship*. Computer Law & Security Review, Vol. 34, Issue 6, December 2018, s. 1247–1257. Elsevier Ltd. 2018. https://doi.org/10.1016/j.clsr.2018.08.006

Andersson, Helena & Nordén, Anna (2018). *Säker informationshantering i digitala miljöer*. Teoksessa: Rättsinformatik - Juridiken I det digitala informationssamhället. 3. painos. Lund: Studentlitteratur AB, s. 55–144.

Andersson, Jenna (2018). *Organisaation tietoturva- ja tietosuojariskienhallinta sekä lainsäädännön vaatimukset*. Edilex-sarja 2018/4. Julkaistu 21.2.2018. Saatavissa: https://www.edilex.fi/artikkelit/18528

Andreasson A. & Koivisto J. (2013). *Tietoturvaa toteuttamassa*. Helsinki ja Tallinna: Tietosanoma Oy: Helsinki ja Tallinna.

Andreasson A.; Koivisto J. & Ylipartanen A. (2013). *Tietosuojavastaavan käsikirja*. Helsinki: Tietosanoma Oy.

Andreasson A.; Koivisto J. & Ylipartanen A. (2016). *Tietosuojakäsikirja johdolle*. Helsinki: Tietosanoma Oy.

ATK-sanakirja 1 (2008). *Tietotekniikan monikielinen hakuteos – Termit, määritelmät ja vastineet eri kielillä*. Tietotekniikan liitto ry. 14. uudistettu painos. Helsinki: Talentum.

Ayanso, A. & Herath, T. (2012). *Law and Technology at Crossroads in Cyberspace: Where Do We Go from Here?* Teoksessa: Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices. Toimittanut: Dudley, A; Braman, J & Vincenti, G. Towson University, USA: IGI Global 2012, s.57–77.

Blume, Peter (2001). *Denmark*. Teoksessa: Nordic Data Protection Law. Helsinki: Kauppakaari Oyj, Kööpenhamina: DJØF Publishing Copenhagen, s: 11–37.

Bruun, Lars (1984). *Informationens lagar och normer*. Helsinki: Suomen Lakimiesliiton kustannus.

Cate, F.H; Kuner, C.; Lynskey, O.; Millard, C. & Svantesson S. (2017). *The rise of cybersecurity and its impact on data protection*. International Data Privacy Law, 2017, Vol. 7, No. 2. Oxford University Press 2017.
https://doi.org/10.1093/idpl/ipx009

Christofi, A.; Dewitte, P.; Ducuing, C. & Valcke, P. (2020). *Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment Up to (GDPR) Standard?* Teoksessa: Personal Data Protection and Legal Developments in the European Union. Toimittanut: Tzanou Maria. Keele University, UK: IGI Global 2020, Christofi et al. s.140–167.

CNIL (2018). *Privacy Impact Assessment (PIA)*. Knowledge bases. February 2018 edition. [Viitattu 15.1.2024]. Saatavissa: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

CNIL (2019). *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*. 21.1.2019. [Viitattu 27.3.2019]. Saatavissa: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Digitaleurope (2016). *EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi) saattaminen osaksi kansallista lainsäädäntöä*. Bryssel 5.7.2016. [Viitattu 27.8.2024]. Saatavissa : https://www.digitaleurope.org/resources/eun-verkko-ja-tietoturvadirektiivin-nis-direktiivi-saattaminen-osaksi-kansallista-lainsaadantoa/

DMARC (2021). *DMARC FAQ*. Päivitetty 19.2.2021.[Viitattu 16.4.2024]. Saatavissa: https://dmarc.org/wiki/FAQ#IP_Addresses_are_in_various_reports.2C_is_that_a_privacy_issue.3F

Eduskunta (2015). *Tietoverkkorikosdirektiivin täytäntöönpano*. Lakihankkeiden tietopaketit - LATI. [Viitattu 21.8.2018]. Saatavissa: https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/tietoverkkorikosdirektiivin-taytantoonpano.aspx

Eduskunta (2018a). *EU:n yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano – Uusi tietosuojalaki*. Lakihankkeiden tietopaketit - LATI. [Viitattu 21.8.2018]. Saatavissa: https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx

Eduskunta (2018b). *Tiedotteet: Perustuslain 10 §:n muutos julistettiin kiireelliseksi ja hyväksyttiin täysistunnossa*. Julkaistu 3.10.2018. [Viitattu 20.1.2019]. Saatavissa: https://www.eduskunta.fi/FI/tiedotteet/Sivut/Perustuslain-10n-muutos-julistettiin-kiireelliseksi-ja-hyv%C3%A4ksyttiin-t%C3%A4ysistunnossa.aspx

Eduskunta (2019). *Eduskunta hyväksyi siviili- ja sotilastiedustelua koskevan lainsäädännön*. Julkaistu 11.3.2019. [Viitattu3.1.2022]. Saatavissa: https://www.eduskunta.fi/FI/tiedotteet/Sivut/tiedustelulait-hyvaksytty.aspx

Elinkeinoelämän keskusliitto (2018). *Turvallisuudesta kilpailuetua – Yritysten näkemyksiä ja viestejä turvallisuudesta*. [Viitattu 6.9.2018]. Saatavissa: https://ek.fi/wp-content/uploads/Turvallisuudesta-kilpailuetua_taitto_net.pdf

Euroopan digitaalistrategia (2023). Euroopan parlamentti. Kirjoittajat: Christina Ratcliff, Barbara Martinello & Vasileios Litos. 07/2022. [Viitattu 25.1.2023]. Saatavissa: https://www.europarl.europa.eu/ftu/pdf/fi/FTU_2.4.3.pdf

Euroopan komissio (2023). *EU:n kybersolidaarisuutta koskeva säädös*. Euroopan unionin virallinen verkkosivusto, Shaping Europe's digital future. Päivitetty: 18.4.2023. [Viitattu 4.6.2023]. Saatavissa: https://digital-strategy.ec.europa.eu/fi/policies/cyber-solidarity

Euroopan parlamentti (2019). *Parlamentti hyväksyi EU:n kyberturvallisuuslain ja puuttuu Kiinan teknologiauhkaan*. Lehdistötiedote 12.3.2019. [Viitattu 27.3.2019]. Saatavissa: https://www.europarl.europa.eu/news/fi/press-room/20190307IPR30694/ep-hyvaksyi-eu-n-kyberturvallisuuslain-ja-puuttuu-kiinan-teknologiauhkaan

Euroopan parlamentti (2023). *EU-parlamentti hyväksyi kantansa: tekoälyn käytön oltava turvallista ja avointa*. Lehdistötiedote 14.6.2023. [Viitattu 28.11.2023]. Saatavissa: https://www.europarl.europa.eu/news/fi/press-room/20230609IPR96212/eu-parlamentti-tekoalyn-kayton-oltava-turvallista-ja-avointa

Euroopan parlamentti (2024a). *Parlamentti hyväksyi maailman ensimmäiset tekoälysäännöt*. Lehdistötiedote 13.3.2024. [Viitattu 27.3.2024]. Saatavissa: https://www.europarl.europa.eu/news/fi/press-room/20240308IPR19015/parlamentti-hyvaksyi-maailman-ensimmaiset-tekoalysaannot

Euroopan parlamentti (2024b). *Henkilötietojen suoja*. [Viitattu 29.7.2024]. Saatavissa: https://www.europarl.europa.eu/factsheets/fi/sheet/157/henkilotietojen-suoja

Euroopan tietosuojaneuvosto (2024). *European Data Protection Board*. [Viitattu 16.6.2024]. Saatavissa: https://www.edpb.europa.eu/edpb_fi

Euroopan tietosuojaneuvoston (EDPB) ohje 3/2019. *Ohjeet 3/2019 henkilötietojen käsittelystä videolaitteilla*. Versio 2.0, 29.1.2020.

Euroopan tietosuojaneuvoston (EDPB) ohje 4/2019. *Ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta*. Versio 2.0, 29.10.2020.

Euroopan tietosuojaneuvoston (EDPB) ohje 1/2021. *Ohjeet 1/2021 henkilötietojen tietoturvaloukkauksesta ilmoittamisista koskevista esimerkeistä*. Versio 2.0, 14.12.2021.

Euroopan tietosuojaneuvoston (EDPB) ohje 1/2022. *Ohjeet 1/2022 rekisteröityjen oikeuksista – oikeus tutustua tietoihin*. Versio 2.1, 28.3.2023.

Euroopan tietosuojaneuvoston (EDPB) ohje 9/2022. *Guidelines 9/2022 on personal data breach notification under GDPR*. Versio 2.0, 28.3.2023.

Euroopan unionin kyberturvallisuusstrategia (2013). Avoin, turvallinen ja vakaa verkkoympäristö. Yhteinen tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Euroopan komissio, Bryssel 7.2.2013. [Viitattu 25.8.2018]. Saatavissa: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=fi

Euroopan unionin kyberturvallisuusstrategia (2020). The EU's Cybersecurity Strategy for the Digital Decade. Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle. Euroopan komissio, Brysseli 16.12.2020. [Viitattu 30.5.2024]. Saatavissa: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Euroopan WP29-tietosuojatyöryhmä WP136: *Lausunto 4/2007 henkilötietojen käsitteestä*. 20.6.2007.

Euroopan WP29-tietosuojatyöryhmä WP168: *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*. 1.12.2009.

Euroopan WP29-tietosuojatyöryhmä WP169: *Opinion 1/2010 on the concepts of "controller" and "processor"*. 16.2.2010.

Euroopan WP29-tietosuojatyöryhmä WP216: *Lausunto 5/2014 anonymisointitekniikoista*. 10.4.2014.

Euroopan WP29-tietosuojatyöryhmä WP217: *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. 9.4.2014.

Euroopan WP29-tietosuojatyöryhmä WP218: *Statement on the role of a risk-based approach in data protection legal frameworks*. 30.5.2014.

Euroopan WP29-tietosuojatyöryhmä WP248: *Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää "liittyykö käsittelyyn todennäköisesti" asetuksessa (EU) 2016/679 tarkoitettu "korkea riski"*. Julkaistu 4.10.2017.

Euroopan WP29-tietosuojatyöryhmä WP250: *Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta*. Viimeksi tarkistettu ja hyväksytty 6.2.2018.

Eurooppa-neuvosto (2018). *Kyberturvallisuuden uudistus Euroopassa*. Päivitetty 19.10.2018. [Viitattu 8.11.2018]. Saatavissa: https://www.consilium.europa.eu/fi/policies/cyber-security/

Eurooppa-neuvosto (2020). *Euroopan kyberturvallisuus: tiukemmat säännöt ja parempaa suojaa*. Päivitetty 6.3.2020. [Viitattu 2.4.2020]. Saatavissa: https://www.consilium.europa.eu/fi/policies/cybersecurity/

Eurooppa-neuvosto (2022). *EU:n häiriönsietokyky: neuvostolta direktiivi kriittisten toimijoiden häiriönsietokyvyn vahvistamisesta*. Lehdistötiedote. Päivitetty 8.12.2022. [Siteerattu 14.2.2023]. Saatavissa: https://www.consilium.europa.eu/fi/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/

Eurooppa-neuvosto (2023). *Datasäädös: neuvosto hyväksyi uuden lain datan oikeudenmukaisesta saatavuudesta ja käytöstä*. Lehdistötiedote. Päivitetty 27.11.2023. [Viitattu 28.12.2023]. Saatavissa: https://www.consilium.europa.eu/fi/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/

Eurooppa-neuvosto (2024a). *Tekoäly*. Päivitetty 11.1.2024. [Viitattu 23.3.2024]. Saatavissa: https://www.consilium.europa.eu/fi/policies/artificial-intelligence/

Eurooppa-neuvosto (2024b). *Eurooppalainen terveysdata-avaruus: neuvosto ja parlamentti sopuun*. Lehdistötiedote. Päivitetty 23.3.2024. [Viitattu 27.3.2024]. Saatavissa: https://www.consilium.europa.eu/fi/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

Finanssivalvonta (2014). *Operatiivisen riskin hallinta rahoitussektorin valvottavissa*. Määräykset ja ohjeet 8/2014. Annettu 4.11.2014, voimassa toistaiseksi 1.2.2015 lähtien. Dnro: FIVA 8/01.00/2014. [Viitattu 29.8.2018]. Saatavissa: http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/2014_08/08_2014.M3.pdf

Finanssivalvonta (2020). *Varautumissuunnitelmat toimitettava Finanssivalvonnalle 31.12.2020 mennessä*. Valvottavatiedote 7.7.2020 – 44/2020. [Viitattu 22.6.2022]. Saatavissa: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2020/varautumissuunnitelmat-toimitettava-finanssivalvonnalle-31.12.2020-mennessa/

Finnish Accreditation Service (2018). *FINAS*. [Viitattu 6.9.2018]. Saatavissa: https://www.finas.fi/Tietoa/Sivut/Tietoa-FINASista.aspx

Finto.fi - Suomalainen asiasanasto- ja ontologiapalvelu 2024. *Data (alimman jalostusasteen tieto)*. [Viitattu 23.3.2024]. Saatavissa: http://urn.fi/URN:NBN:fi:au:tt:t108

Fredman, Markku (2021). *Rikosasianajajan käsikirja*. 2. uudistettu painos. Helsinki: Alma Talent Oy, Verkkokirjahylly.

Frände, D.; Korkka-Knuts, H. & Wahlberg, M. (2023). *Kameravalvonnan rikosoikeudellinen sääntely*. Teoksessa: Keskeiset rikokset. Viides uudistettu painos. Toimittanut Frände, Hyttinen, Kallio, Korkka-Knuts, Matikkala, Tapani, Tolvanen, Viljanen & Wahlberg. Helsinki: Edita, s. 430–442.

Gullans, M.; Pellonpää, M.; Pölönen, P. & Tapanila, A. (2018). *Euroopan ihmisoikeussopimus*. 6. uudistettu painos. Helsinki: Alma Talent ja Lakimiesliiton kustannus.

Hakala, M.; Vainio, M. & Vuorinen, O. (2006). *Tietoturvallisuuden käsikirja*. Jyväskylä: Docendo Finland Oy.

Hallberg, Pekka (2011). *Perusoikeusjärjestelmä*. Teoksessa: Perusoikeudet – Oikeuden perusteokset. Toinen uudistettu painos. Helsinki: WSOYpro, s. 29–59.

Haukilehto, Tero (2024). *Cybersecurity management in healthcare : Policies, awareness and incident reporting*. Vaasan yliopisto: Acta Wasaensia, 532. Väitöskirja.

Heikkilä, S. & Hirvelä, P. (2017). *Ihmisoikeudet – Käsikirja EIT:n oikeuskäytäntöön*. Toinen uudistettu painos. Helsinki: Alma Talent Oy.

Heiskanen, Jesse (2020). *Passive DNS-tietojen hyödyntäminen tietoturvaperusteella*. Referee artikkeli. Teoksessa: Sanan vapauksia ja rajoja – Viestintäoikeuden vuosikirja 2020. Toimittanut: Päivi Korpisaari. FORUM IURIS, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Helsinki: Unigrafia Oy, s. 88–131.

Helopuro, S.; Perttula, J. & Ristola, J. (2009). *Sähköisen viestinnän tietosuoja*. Helsinki: Talentum Media Oy.

Hert, P.; Markopoulou, D. & Papakonstantinou, V. (2019). *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*. Computer Law & Security Review, Volume 35, Issue 6, 11/2019, 105336. Elsevier Ltd. 2019. [Viitattu 2.9.2020]. Saatavissa: https://doi.org/10.1016/j.clsr.2019.06.007

Hildebrandt, Mireille & Tielemans, Laura (2013). *Data Protection by design and technology neutral law*. Computer Law & Security Review, Vol. 29, Issue 5, October 2013, s. 509–521. Elsevier Ltd. 2013. [Viitattu 4.9.2020]. Saatavissa: https://doi.org/10.1016/j.clsr.2013.07.004

Hildén, Jockum (2019). *The politics of datafication: The influence of lobbyist on the EU's data protection reform and its consequences for the legitimacy of the*

general data protection regulation. Helsinki: Unigrafia. Helsingin yliopiston väitöskirja.

Hirvonen, Ari (2011). *Mitkä metodit? Opas oikeustieteen metodologiaan*. Helsinki: Yleisen oikeustieteen julkaisuja 17. [Viitattu 3.1.2019]. Saatavissa: https://helda.helsinki.fi/server/api/core/bitstreams/20149471-38b2-4cc8-94b7-2f6b3feed81d/content

Hoikka, M.; Neuvonen, R. & Rautiainen, P. (2016). *Viestintämarkkinaoikeus. Viestintämarkkinalainsäädännön ajantasainen kommentaari*. Helsinki: Helsingin Kamari Oy.

Huhtamäki, Ari (1992). *Hyvää pankkitapa*. Teoksessa: Hyvä Tapa. Toimittanut: Seija Huhtamäki. Turku: Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. Kokoomateosten sarja C:16, s. 17–44.

Husa, J. & Jyränki, A. (2012). *Valtiosääntöoikeus*. Hämeenlinna: Helsingin Kamari Oy / Helsingin seudun kauppakamari.

Hyvönen, Tommi (2017). *Talous on taitolaji. 45 vuotta suomalaista talouden asiantuntijuutta*. Helsinki: Oy Tuokko Ltd. Kiriprintti Oy.

Häyhä, Juha (1997). *Johdanto – Minun metodini*. Toimittanut: Juha Häyhä. Porvoo: WSOY, s. 15–34.

Innanen A. & Saarimäki J. (2012). *Internetoikeus*. 2. uudistettu painos. Helsinki: Edita Publishing Oy.

International Organization for Standardization (2018a). *About ISO*. Viitattu 6.9.2018]. Saatavissa: https://www.iso.org/about-us.html

International Organization for Standardization (2018b). *Reducing the risks of information security breaches with ISO/IEC 27005*. [Viitattu 7.9.2018]. Saatavissa: https://www.iso.org/news/ref2309.html

ISO/IEC 27001:2013

ISO/IEC 27001:2020

It-viikko.fi (2007). *Asiantuntija: kyberrikoslaki voi poikia näyttövaikeuksia*. Julkaistu 29.8.2007, Tuomas Linnake. [Viitattu 17.1.2016]. Saatavissa: http://www.itviikko.fi/tie toturva/2007/08/29/asiantuntija-kyberrikoslaki-voi-poikia-nayttovaikeuksia/200720974/23

Ivanova, Yordanka (2020). *Data Controller, Processor, or Joint Controller: Towards Reaching GDPR Compliance in a Data- and Technology-Driven World*. Teoksessa: Personal Data Protection and Legal Developments in the European Union. Toimittanut: Tzanou Maria. Keele University, UK: IGI Global 2020, s. 61–84.

Johnssén, Gustaf (2018). *Vidareutnyttjande av offentlig information*. Teoksessa: Rättsinformatik - Juridiken I det digitala informationssamhället. 3. painos. Lund: Studentlitteratur AB, s. 371–392.

Jokela, Antti (2018). *Rikosprosessioikeus*. 5. uudistettu painos. Helsinki: Alma Talent Oy, Verkkokirjahylly.

Jyränki, Antero (1997). *Toiset työt, toiset metodit*. Teoksessa Minun Metodini. Toimittanut: Juha Häyhä. Porvoo: WSOY, s. 74–89.

Järvinen P. & Rousku K. (2017). *Työpaikan tietoturvaopas - tunnista uhat, hallitse riskit*. Helsinki: Alma Talent.

Järvinen, Petteri (2022a). *Digiajan tietosuoja – Turvaa henkilötietosi, torju identiteettivarkaudet, suojaudu urkinnalta*. Helsinki: Tammi.

Järvinen, Petteri (2022b). *Yrityksen tietoturvaopas*. Helsingin seudun kauppakamari / Helsingin Kamari Oy. Viro: Meedia Zone OÜ.

Kaasalainen, Minna (2008). *Informaation suojaaminen liikeneuvotteluissa*. Vaasan yliopisto: Talousoikeuden lisensiaatintutkimus. [Viitattu 18.12.2020]. Saatavissa: https://osuva.uwasa.fi/handle/10024/404

Kallio, Heikki & Rikander, Henri (2021). *Voimakeinojen käyttö – rikosoikeuden systematiikka ja tekijän tahallisuus*. Defensor Legis N:o 2/2021, s. 338–352. Referee-artikkeli.

Kangas, Urpo (1997). *Minun Metodini*. Teos: Minun Metodini. Toimittanut: Juha Häyhä. Porvoo: WSOY, s. 90–109.

Kanta (2024). *Sertifioinnin osapuolet ja vastuut*. Sivua päivitetty 26.2.2024. [Viitattu 27.3.2024]. Saatavissa: https://www.kanta.fi/jarjestelmakehittajat/sertifioinnin-osapuolet-ja-vastuut

Katakri 2015. *Tietoturvallisuuden auditointityökalu viranomaisille – 2015*. Puolustusministeriö. [Viitattu 15.9.2018]. Saatavissa: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Katakri 2020. *Tietoturvallisuuden auditointityökalu viranomaisille – 2020*. Kansallinen turvallisuusviranomainen. Traficomin julkaisusarja 232/2020. [Viitattu 18.12.2020]. Saatavissa: https://um.fi/documents/35732/0/Katakri-2020_201218.pdf/e19df3b3-b690-bc45-6c3b-de992ac7a21e?t=1608290804847

Keller and Heckman LLP (2018). *German Court Issues First GDPR Ruling*. 9.7.2018. [Viitattu 23.10.2018]. Saatavissa: https://www.khlaw.com/German-Court-Issues-First-GDPR-Ruling

Kemppinen, Jukka (2011). *Informaatio-oikeuden alkeet*. Tallinna: Tietosanoma Oy.

Kinnunen, Niina (2015). *Tietoturvaohjeistusten noudattamisen motivaatio ja sen muuttuminen*. Vaasan yliopisto: Acta Wasaensia, 331. Väitöskirja.

Kiviniemi, Pekka (2000). O*ikeutetusta puuttumisesta luottamukselliseen viestiin: Sähköpostiviesti ja muut viestit*. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja, Rikos- ja prosessioikeuden julkaisusarja B. Turku: Turun yliopisto.

Kiviniemi, Johanna (2002). *Hyvä tiedonhallintatapa viranomaisen toimintaa ohjaavana periaatteena – Selvitystyö Lapin Lääninhallituksessa*. Teoksessa Pohjois-Suomen tuomarikoulun julkaisuja 2/2002: Tietoturvallisuus ja laki – Ajankohtaista asiaa tietoturvasta. Rovaniemi: Lapin yliopisto, s. 15–32.

Kolehmainen Antti (2016). *Tutkimusongelma ja metodi lainopillisessa työssä*. Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Toimittanut: Tarmo Miettinen. Kokoomateos 16.2.2016, Edilex Publishing Oy, s. 106–134.

Koponen, Pekka (2017). *Ylimääräinen muutoksenhaku*. Helsinki: Alma Talent Oy, Verkkokirjahylly.

Korhonen, Rauno (2003). *Perusrekisterit ja tietosuoja*. Helsinki: Edita Publishing Oy.

Korhonen, Rauno (2016). *The New information Society Code of Finland*. Teoksessa: Lawyers in the Media Society – The Legal Challenges of the Media Society. Toimittanut Ahti Saarenpää & Karolina Sztobryn. Rovaniemi: Lapin yliopisto, s. 52–58.

Korja, Juhani (2016a). *The Privacy Risks of Biometric Identification*. Teoksessa: Society Trapped in the Network – Does it have a future? Rovaniemi: Lapin yliopisto, s. 196–213. https://urn.fi/URN:ISBN:978–952–484–917–3

Korja, Juhani (2016b). *Biometrinen tunnistaminen ja henkilötietojen suoja – tutkimus biometristen tietojen lainsäädännöllisestä asemasta*. Rovaniemi: Lapin yliopisto. Akateeminen väitöskirja.

Korkea-aho, Emilia (2005). *Pehmeä sääntely sääntelytutkimuksen ja oikeusjärjestyksen haasteena*. Teoksessa: Lainsäädäntöä vai muuta oikeudellista ohjailua? Julkaisusarja: Oikeuspoliittisen tutkimuslaitoksen tutkimustiedonantoja; 67. Toimittanut: Heidi Lindfors. Helsinki: Oikeuspoliittinen tutkimuslaitos, s. 69–83.

Korpisaari, P.; Pitkänen, O. & Warma-Lehtinen, E. (2018). *Uusi tietosuojalainsäädäntö*. Helsinki: Alma Talent Oy.

Korpisaari, P.; Pitkänen, O. & Warma-Lehtinen, E. (2022). *Tietosuoja*. 2. uudistettu painos. Helsinki: Alma Talent Oy.

Korpisaari, P. & Toikkanen, I. (2020). *Ajoneuvon sijaintitieto älyliikenteessä – Henkilötietojen suoja, osapuolten roolit ja tietosuojaperiaatteiden toteuttaminen*. Lakimies 3-4 / 2020. Julkaistu 12.6.2020, referee-artikkeli, s. 458–479.

Koskinen, Seppo (2020). *Työhönotto ja henkilötietojen kerääminen*. Teoksessa: Henkilötietojen käsittely työelämässä. 3. uudistettu painos. Keuruu: Edita Publishing Oy, s. 169–238.

Koskinen, S. & Kulla, H. (2019). *Virkamiesoikeuden perusteet*. Helsinki: Alma Talent.

Koskinen, S. & Ullakonoja, V. (2020). *Oikeudet ja velvollisuudet työsuhteessa*. 5. uudistettu painos. Helsinki: Edita Publishing Oy.

Kosola, Leo (2016) *Mitä sinun pitäisi tietää big datasta, datanlouhinnasta ja datafuusiosta?* Julkaistu 28.06.2016. Yle-artikkeli. [Viitattu 23.3.2024]. Saatavissa: https://yle.fi/aihe/artikkeli/2016/06/28/mita-sinun-pitaisi-tietaa-big-datasta-datanlouhinnasta-ja-datafuusiosta

Koulu, Riikka (2012). *Jokakodin laajakaista – Pääsy internettiin perusoikeutena*. Lakimies 2/2012, s. 280–302.

Kulla, Heikki (2018). *Hallintomenettelyn perusteet*. 10. uudistettu painos. Helsinki: Alma Talent Oy.

Kulla, H. & Salminen, J. (2021). *Hallintomenettelyn perusteet*. 11. uudistettu painos. Juridica-kirjasarjan 1. teos. Helsinki: Alma Talent Oy.

Kurvinen, Evgeniya (2019). *Kameravalvonnan toteuttaminen työpaikalla Suomessa ja Venäjällä*. Defensor Legis N:o 2/2019, s. 194–209. Referee-artikkeli.

Laaksonen M.; Nevasalo T. & Tomula K. (2006). *Yrityksen tietoturvakäsikirja: Ohjeistus, toteutus ja lainsäädäntö*. Helsinki: Edita Publishing Oy.

Laurikkala, Jenna (2020). *Virkasalaisuusrikokset - Tutkimus rikoslain 40 luvun 5 §:n virkasalaisuusrikostunnusmerkistöjen sisällöstä ja muutostarpeista*. Akateeminen väitöskirja: Lapin yliopisto, oikeustieteiden tiedekunta. Helsinki: Alma Talent Oy.

Lavapuro, J. & Tuori, K. (2011). *Perusoikeuksien ja ihmisoikeuksien turvaamisvelvollisuus (PL 22 §)*. Teoksessa: Perusoikeudet – Oikeuden perusteokset. Toinen uudistettu painos. Helsinki: WSOYpro, s. 809–820.

Lehtonen, Asko (2001). *Sähköpostin suojasta*. Teoksessa: Oikeustieteen rajoja etsimässä. Juhlajulkaisu Juha Tolonen 15.4.2001. Toimittajat: Vesa Annola ja Brita Herler. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. Kokoomateosten sarja, Juhlajulkaisu A:9. Turku: Kirjapaino Grafia, s. 113–133.

Lehtonen, Asko (2005). *Sähköpostin rikosoikeudellisen suojan kehitys muutosten paineissa*. Teoksessa: Rikos, rangaistus ja prosessi. Juhlajulkaisu Eero Backman 1945 – 14/5 - 2005. Toimittajat: Ari-Matti Nuuttila ja Elina Pirjatanniemi. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. A. Juhlajulkaisut N:o 15. Jyväskylä: Gummerus Kirjapaino Oy, s. 153–172.

Lehtonen, Asko (2008). *Työnantajan oikeudesta tutkia työntekijän sähköpostiviestintää*. Defensor Legis N:o 4/2008, s. 550–567.

Lehtonen, Asko (2016). *Digitalisaation edistäminen tietoturvalainsäädännön avulla*. Teoksessa: Society Trapped in the Network – Does it have a future? Rovaniemi: Lapin yliopisto, s. 268–276. https://urn.fi/URN:ISBN:978–952–484–917–3

Lehtonen, Asko (2021). *KKO 2019:86 – Vastuu sähköpostin perille saapumisesta tuomioistuinmenettelyssä*. Lakimies 2/2021, s. 272–281.

Lehtonen, Lasse (2001). *Potilaan yksityisyyden suoja*. Suomalaisen Lakimiesyhdistyksen julkaisuja, A-Sarja N:o 230. Yliopistollinen väitöskirja. Helsinki: Suomen Lakimiesyhdistys.

Lentzis, Dimosthenis (2020). *Revisiting the Basics of EU Data Protection Law: On the Material and Territorial Scope of the GDPR*. Teoksessa: Personal Data Protection and Legal Developments in the European Union. Toimittanut: Tzanou Maria. Keele University, UK: IGI Global 2020, s.19–33.

Leskinen, Minni (2022). *De lege ferenda -tutkimuksesta metodina ja tieteenä*. Lakimies 7–8/2022, s. 1158–1185.

Liikenne- ja viestintäministeriö (2023). *NIS2 direktiivin kansallinen toimeenpano, sidosryhmätilaisuus 31032023, LVM ja KTK*. [Viitattu 13.5.2023]. Saatavissa: https://api.hankeikkuna.fi/asiakirjat/34beb41e-515a-4fcd-a824-5136fd497329/630e7cea-2d6a-4e7f-adc3-c0ae044d0ffd/ESITYS_20230331073019.PDF

Liikenne- ja viestintäministeriön julkaisuja 9/2017. *Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti*. Julkaistu 20.4.2017. [Viitattu 21.2.2018]. Saatavissa: http://urn.fi/URN:ISBN:978-952-243-505-7

Liikenne- ja viestintäministeriön julkaisuja 2021:1. *Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla - Työryhmän loppuraportti*. Julkaistu 1.2.2021. [Viitattu 28.3.2022]. Saatavissa: http://urn.fi/URN:ISBN:978-952-243-614-6

Liikenne ja viestintäministeriön ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta (2022). Traficom/376384/03.04.05.01/2022. Antopäivä 25.10.2022. Voimaantulopäivä 27.10.2022. Voimassa toistaiseksi. [Viitattu 15.2.2023]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Liikenne-%20ja%20viestint%C3%A4viraston%20ohje%20v%C3%A4litystietojen%20k%C3%A4sittely%C3%A4%20koskevien%20tietojen%20tallentamisesta.pdf

Limnéll, J. & Lonka, H. (2015). *Strategiasta käytäntöön: Suomi kyberlainsäädäntöä kehittämässä*. Julkaisupäivä: 4.8.2015. Julkaisussa: Oikeus 2/2015. s. 202–213.

Lindfors, Heidi (2011). *KKO 2011:63 Sähköpostitse lähetetyn valituskirjelmän saapumisajankohta*. Teoksessa: KKO:n ratkaisut kommentein 2011:II. Toimittanut: Pekka Timonen. Helsinki: Alma Talent Oy, Verkkokirjahylly.

Lindqvist, Jenna (2018). *Personal Data Protection on the Internet of Things, an EU perspective*. Helsingin yliopiston oikeustieteellinen tiedekunta. Väitöskirja. Helsinki: Unigrafia Oy.

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

Lohse, Mikael (2005). *Rikostiedustelu terrorismin torjunnassa*. Defensor Legis N:o 6/2005, s. 1187–1200.

Lohse, Mikael (2012). *Terrorismirikoksen valmistelu ja edistäminen*. Suomalaisen lakimiesyhdistyksen julkaisuja, A-sarja N:o 312. Väitöskirja, Helsingin yliopisto.

Lohse, Mikael (2015). *Kybervakoilu*. Defensor Legis N:o 4/2014, s.762–771.

Lohse, Mikael & Viitanen, Marko (2019). *Johdatus tiedusteluun*. Helsinki: Alma Talent.

Lohse, M.; Honkanen, K. & Meriniemi, M. (2019). *Tiedustelumenetelmät*. Helsinki: Alma Talent.

Luoto, Lauri (2022). *KKO 2022:32 Viestintäsalaisuuden loukkaus ja välillinen tekeminen*. Teoksessa: KKO:n ratkaisut kommentein 2022:1. Toimittanut: Pekka Timonen. Helsinki: Alma Talent Oy, Verkkokirjahylly.

Länsineva, Pekka (2011). *Omaisuudensuoja (PL 15§)*. Teoksessa: Perusoikeudet – Oikeuden perusteokset. Toinen uudistettu painos. Helsinki: WSOYpro, s. 549–604.

Magnusson Sjöberg, Cecilia (1992). *Rättsautomation: Särskilt om statsförvaltningens datorisering*. Tukhoma: Nordtedt.

Magnusson Sjöberg, Cecilia (2018). *Om rättsinformatik*. Teoksessa: Rättsinformatik - Juridiken I det digitala informationssamhället. 3. painos. Lund: Studentlitteratur AB, s. 19–26.

Manninen, Sami (2011). *Sananvapaus ja julkisuus (PL 12 §)*. Teoksessa: Perusoikeudet – Oikeuden perusteokset. Toinen uudistettu painos. Helsinki: WSOYpro, s. 459–491.

Melander, Sakari (2019). *Rikos, julkisuus ja yksityisyyden suoja*. Lakimies 7–8/2019, s.953–982.

Melander, Sakari & Rautio, Ilkka (2022). *RL 38: Tieto- ja viestintärikokset*. Teoksessa: Rikosoikeus – Oikeuden perusteokset. Viides uudistettu painos. Toimittanut: Lappi-Seppälä, Hakamies, Helenius, Melander, Nuotio, Ojala & Rautio. Helsinki: Alma Talent Oy, s. 1283–1320.

Meri, Otto (2023). *Lain ja hyvän tavan vastaiset sopimukset: Sopimusoikeudellinen tutkimus kiellonvastaisista oikeustoimista ja niiden oikeusvaikutuksista*. Väitöskirja, Helsingin yliopiston oikeustieteellinen tiedekunta 21.1.2023. Helsinki: Alma Talent Oy.

Mäenpää, Olli (2016). *Julkisuusperiaate*. Helsinki: Talentum Pro.

Mäenpää, Olli (2017). *Yleinen hallinto-oikeus*. Helsinki: Alma Talent Oy.

Mäenpää, Olli (2019). *Oikeudenkäynti hallintoasioissa - Hallintoprosessioikeuden perusteet*. Helsinki: Alma Talent Oy.

Neuvonen, Riku (2014). *Yksityisyyden suoja Suomessa*. Helsinki: Lakimiesliiton kustannus.

Neuvonen, Riku (2019). *Viestintä- ja informaatio-oikeuden perusteet*. Helsinki: Kauppakamari.

Nieminen, Liisa (2020). *Ristiriitainen soft law – liian paljon vai liian vähän soft law'ta?* Lakimies 7–8/2020, s. 1081–1103.

NIST Special Publication 800-12 (1995). *An Introduction to Computer Security: The NIST Handbook*. [Viitattu 20.4.2016]. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

NIST Special Publication 800-100 (2006). *Information Security Handbook: A Guide for Managers*. [Viitattu 20.4.2016]. Saatavissa: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

NordVPN blogi (2021). *Mitä toinen henkilö voi tehdä IP-osoitteellani?* Blogi – Verkkouhat. Julkaistu 16.8.2021. [Viitattu 21.4.2024]. Saatavissa: https://nordvpn.com/fi/blog/mita-toinen-henkilo-voi-tehda-ip-osoitteellani/

Nyblin, Klaus (2003). *Yrityssalaisuuden suoja ja entiset työntekijät*. Defensor Legis N:o 2/2003, s. 230–253.

Nyblin, Klaus (2008). *Yrityssalaisuuksien suojaaminen ja oma henkilöstö*. Defensor Legis N:o 4/2008, s. 535–549.

Nyblin, Klaus (2009). *Työelämän sähköposti*. 3. uudistettu painos. Helsinki: Talentum Media Oy.

Nyblin, Klaus (2016). *Yrityssalaisuusrikokset – Korkeimman oikeuden ratkaisut 2013–2015, Osa II*. Defensor Legis N:o 2/2016, s. 205–224.

Nyyssölä, Mikko (2018). *Yksityisyyden suoja työsuhteessa*. Helsinki: Alma Talent Oy.

OECD 2012, The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy. OECD Digital Economy Papers no. 209. OECD Publishing, Paris. Julkaistu 16.11.2012. [Viitattu 20.2.2019]. Saatavissa: https://doi.org/10.1787/5k8zq930xr5j-en

OECD 2015, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, OECD/LEGAL/0415. Julkaistu 17.9.2015. [Viitattu 11.11.2020]. Saatavissa: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415

OECD 2022, OECD Policy Framework on Digital Security. OECD Publishing, Paris. Julkaistu 14.12.2022. [Viitattu 7.7.2024]. Saatavissa: https://doi.org/10.1787/a69df866-en

OECD 2022, Recommendation of the Council on Digital Security Risk Management, OECD/LEGAL/0479. OECD Legal Instruments. Julkaistu 26.9.2022.

[Viitattu 7.7.2024]. Saatavissa: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479

OECD 2022, Recommendation of the Council on National Digital Security Strategies, OECD/LEGAL/0480. OECD Legal Instruments. Julkaistu 26.9.2022. [Viitattu: 7.7.2024]. Saatavissa: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480

OECD 2022, Recommendation of the Council on the Digital Security of Products and Services, OECD/LEGAL/0481. OECD Legal Instruments. Julkaistu 26.9.2022. [Viitattu 7.7.2024]. Saatavissa: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481

OECD 2022, Recommendation of the Council on the Treatment of Digital Security Vulnerabilities, OECD/LEGAL/0482. OECD Legal Instruments. Julkaistu 26.9.2022. [Viitattu 7.7.2024]. Saatavissa: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482

Oikeusministeriön julkaisu 11/2012. *Lainlaatijan EU-opas. Kansallisten säädösten valmistelua koskevat ohjeet*. Selvityksiä ja ohjeita. OM 8/469/2012. http://urn.fi/URN:ISBN:978-952-259-170-8

Oikeusministeriön julkaisu 8/2018. *EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) loppumietintö*. Mietintöjä ja lausuntoja. OM 21/41/2016 & OM005:00/2017. http://urn.fi/URN:ISBN:978-952-259-683-3

Oikeusministeriön julkaisuja 2023:32. *Julkisuuslain ajantasaistaminen*. Työryhmän mietintö. Julkaistu 12.12.2023. Helsinki: Oikeusministeriö. http://urn.fi/URN:ISBN:978-952-400-005-5

Ojala, Timo (2022). *RL 12: Maanpetosrikokset*. Teoksessa: Rikosoikeus – Oikeuden perusteokset. Viides uudistettu painos. Toimittanut: Lappi-Seppälä, Hakamies, Helenius, Melander, Nuotio, Ojala & Rautio. Helsinki: Alma Talent Oy, s. 325–346.

Ojanen, Tuomas (2015). *Perusoikeusjuridiikka*. Helsinki: Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja.

Olson, D.L. & Wu, D.D. (2017). *Enterprise risk management models*. Saksa: Springer Texts in Business and Economics.

Paasonen, J. & Luomala, M. (2021). *Kameravalvonta tutkimus- ja sääntelykohteena*. Edilex-artikkeli. Julkaistu 7.10.2021. [Viitattu 25.4.2022]. Saatavissa: www.edilex.fi/artikkelit/24627

Paasonen, J.; Lindfors, H. & Vainio, J. (2022). *Turvallisuusselvitys vai turha selvitys?* Defensor Legis 4/2022, s. 962–980.

Pellonpää, Matti (2011). *Henkilökohtainen koskemattomuus (PL 7§)*. Teoksessa: Perusoikeudet – Oikeuden perusteokset. Toinen uudistettu painos. Helsinki: WSOYpro, s. 281–301.

Perusoikeuskomitea (1992). *Perusoikeuskomitean mietintö 1992:3*. Helsinki: Oikeusministeriö, Valtion painatuskeskus.

Pesonen, Pirkko (2013). *Sosiaalisen median lait*. Helsinki: Lakimiesliiton kustannus.

Pesonen, Pirkko (2017). *Viestinnän lait*. Keuruu: Edita Publishing Oy.

Pihlajamäki, Antti (2004). *Tietojenkäsittelyrauhan rikosoikeudellinen suoja: Datarikoksia koskeva sääntely Suomen rikoslaissa*. Helsinki: Suomalainen lakimiesyhdistys. Väitöskirja, Helsingin yliopisto.

Pitkänen, O.; Tiilikka, P. & Warma, E. (2013). *Henkilötietojen suoja*. Helsinki: Alma Talent Oy.

Pohjonen, Marja (1993). *Hyvä tapa ja oikeuskäytäntö eräillä immateriaalioikeuden aloilla*. Teoksessa: Hyvän tavan vastaisuudesta. Toimittanut: Ari Saarnilehto. Turku: Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. B, muut kokoomateokset N:o 2, s. 137–172.

Porvari, Paavo (2012). *Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa*. Aalto University publication series: Doctoral Dissertations 131/2012. Helsinki: Unigrafia Oy.

Pöysti, Tuomas (1997). *Tietoturvallisuus ja laki: Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä*. Tutkimusraportti. Toimittanut: Ahti Saarenpää & Tuomas Pöysti. Helsinki: Valtiovarainministeriö & Lapin yliopisto, Luvut 1-2, 4.10-4.11, 9, osittain 12, 13–14.

Pöysti, Tuomas (1999). *Tehokkuus, informaatio ja eurooppalainen oikeusalue*. FORUM IURIS, Helsinki: Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut. Yliopistollinen väitöskirja.

Pöysti, Tuomas (2000). *Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin turvallisuutta*. Oikeus 1/2000, s. 91–112.

Pöysti, Tuomas (2010). *Information Government in Practise: Functional Gains and Legal Perils*. Julkaisu: Scandinavian studies in law, volume 56, s. 91–124.

Pöysti, Tuomas (2023). *Governance of Societal Cyber and Information Security Risks: How Legal Informatics Can Help Future-Looking Law*. Julkaisu: Legal Informatics as Science of Legal Methods : Proceedings of the 26th International Legal Informatics Symposium IRIS 2023. Julkaistu: 24.2.2023. Editoijat: Erich Schweighofer; Jakob Zanol; Stefan Eder. Weblaw: Bern 2023, s. 39–55.

Rautio, Ilkka (2022). *Yrityssalaisuusrikokset*. Teoksessa: Rikosoikeus – Oikeuden perusteokset. Viides uudistettu painos. Toimittanut: Lappi-Seppälä, Hakamies, Helenius, Melander, Nuotio, Ojala & Rautio. Helsinki: Alma Talent Oy, s. 1024–1033.

Rautio, Jaakko & Frände, Dan (2020). *Todistelu. Oikeudenkäymiskaaren 17 luvun kommentaari*. 2. uudistettu painos. Helsinki: Edita Publishing Oy.

Riekkinen, Juhana (2016a). *Criminal Evidence in the Network Society: New Problems, New Solutions?* Teoksessa: Lawyers in the Media Society – The Legal Challenges of the Media Society. Toimittanut Ahti Saarenpää & Karolina Sztobryn. Rovaniemi: Lapin yliopisto, s. 74–87.

Riekkinen, Juhana (2016b). *Suomen tietosuojaviranomaiset – Katsaus tietosuojavaltuutetun ja tietosuojalautakunnan historiaan, nykytilaan ja tulevaisuuteen*. Teoksessa: Society Trapped in the Network – Does it have a future? Rovaniemi: Lapin yliopisto, s. 315–424. https://urn.fi/URN:ISBN:978–952–484–917–3

Riekkinen, Juhana (2019). *Sähköiset todisteet rikosprosessissa – Tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaareen*. Yliopistollinen väitöskirja. Helsinki: Alma Talent Oy.

Råman, Jari (2006a). *Tietoturvallisuus on myös perusoikeus*. Julkaisupäivä: 15.10.2006. Julkaisussa: Lakimies 5/2006. s. 818–824.

Råman, Jari (2006b). *Regulating Secure Software Development: Analysing the potential regulatory solutions for the lack of security in software*. Acta Electronica Universitatis Lapponiensis. Lapin yliopisto, oikeustieteellinen tiedekunta, väitöskirja.

Saarenpää, Ahti (2002). *Tietoturva ja tietosuoja, identiteetin näkökulma*. Teoksessa Pohjois-Suomen tuomarikoulun julkaisuja 2/2002: Tietoturvallisuus ja laki – Ajankohtaista asiaa tietoturvasta. Rovaniemi: Lapin yliopisto, s. 33–77.

Saarenpää, Ahti (2005). *Tietojenkäsittelystä läsnä-älyyn – Katkelmia oikeusinformatiikan kehityksestä*. Teoksessa Talousoikeuden taitekohtia: Juhlajulkaisu professori Asko Lehtoselle. Toimittanut Annola Vesa, Herler Brita & Tolonen Juha. Vaasa: Vaasan yliopiston julkaisuja, tutkimuksia 266, s. 91–122.

Saarenpää, Ahti (2015). *Henkilö- ja persoonallisuusoikeus*. Teoksessa: Oikeus tänään - Osa II. Kolmas uudistettu painos. Toimittanut Marja-Leena Niemi. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja C 63, s. 203–430.

Saarenpää, Ahti (2016a). *Oikeusinformatiikka*. Teoksessa: Oikeus tänään - Osa I. Neljäs uudistettu painos. Toimittanut Marja-Leena Niemi. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja C 64, s. 67–273.

Saarenpää, Ahti (2016b). *Does Legal Informatics Have a Method in the New Network Society?* Teoksessa: Society Trapped in the Network – Does it have a future? Rovaniemi: Lapin yliopisto, s. 51–75. https://urn.fi/URN:ISBN:978–952–484–917–3

Saarenpää, Ahti (2016c). *Law: Linear Texts or Visual Experiences? Challenges for Teaching Law in the Network Society*. Teoksessa: Lawyers in the Media Society – The Legal Challenges of the Media Society. Toimittanut Ahti Saarenpää & Karolina Sztobryn. Rovaniemi: Lapin yliopisto, s. 34–42.

Saarenpää, Ahti (2018). *Legal Informatics: a Modern Social Science and a Crucial One*. Teoksessa: 50 Years of Law and IT – the Swedish Law and Informatics Research Institute, 1968-2018. Scandinavian Studies in Law, volume 65. Editoija:

Peter Wahlgren. Stockholm Institute for Scandinavian Law: Stockholm University 2018, s. 15–38.

Saarenpää, Ahti & Riekkinen, Juhana (2023). *Oikeusinformatiikan perusteet*. Rovaniemi: Lapin yliopisto.

Saarnilehto, Ari (1992). *Hyvää tapaa koskevista säännöksistä*. Teoksessa: Hyvä Tapa. Toimittanut: Seija Huhtamäki. Turku: Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. Kokoomateosten sarja C:16, s. 5–16.

Saarnilehto, Ari (1993). *Huoneenvuokrasuhteen purkamisesta vuokralaisen hyvän tavan vastaisen käyttäytymisen johdosta*. Teoksessa: Hyvän tavan vastaisuudesta. Toimittanut: Ari Saarnilehto. Turku: Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. B, muut kokoomateokset N:o 2, s. 173–205.

Sallinen, Pekka (2010). *Kameravalvontaopas*. Turva-alan yrittäjät ry.

Salminen, Mirva (2022). *”Et nää on näitä meiän kyberhyökkäyksiä nämä” – The government of one and all in everyday digital security in Finnish Lapland*. Acta electronica Universitatis Lapponiensis 339. Väitöskirja. Rovaniemi: Lapin yliopisto.

Salo, Marika (2015). *Hyvä liiketoimintapäätös ja johdon vastuu*. Vaasan yliopisto, väitöskirja. Helsinki: Talentum.

Sanastokeskus TSK (2004). *Tiivis tietoturvasanasto*. Helsinki: Taloustieto. [Viitattu 6.2.2016]. Saatavissa: http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf

Saraviita, Ilkka (2011). *Perustuslaki*. Toinen uudistettu painos. Hämeenlinna: Talentum Media Oy.

Sarja, Mikko (2011). *Hyvä edunvalvontatapa holhoustoimessa*. Defensor Legis N:o 2/2011, s. 133–162.

Seipel, Peter (2001). *Sweden*. Teoksessa: Nordic Data Protection Law. Helsinki: Kauppakaari Oyj, Kööpenhamina: DJØF Publishing Copenhagen, s. 115–151.

Seipel, Peter (2004). *Juridik och IT: Introduktion till rättsinformatiken*. Tukholma: Norstedts Juridik AB.

Shelly, Marita (2020). *Digital Death: What happens to Digital Property Upon an Individual’s Death?* Teoksessa: Legal Regulations, Implications, and Issues Surrounding Digital Data. Toimittanut: Jackson, M. & Shelly, M. RMIT University, Australia: IGI Global, s. 23–40.

Siltala, Raimo (2001). *Johdatus oikeusteoriaan*. Helsinki: FORUM IURIS.

Siltala, Raimo (2003). *Oikeustieteen tieteenteoria*. Helsinki: Suomalaisen lakimiesyhdistyksen julkaisuja, A-sarja N:o 234.

Sitra työpaperi (2022). *EU-sääntely rakentaa reilumpaa datataloutta – Euroopan viiden datalainsäädäntöehdotuksen tarjoamat mahdollisuudet yrityksille, yksilöille ja julkiselle sektorille*. 7.6.2022. Helsinki: Sitra.

Streng, Alfred (2007). *Ideella rättigheter i digital miljö*. Vaasan yliopisto. Vaasa: Acta Wasaensia, nr 172.

Ståhlberg, Pauli & Karhu, Juha (2020). *Suomen vahingonkorvausoikeus*. 7. uudistettu painos. Lakimiesliiton kustannus. Helsinki: Alma Talent.

Suomen Standardisoimisliitto SFS ry (2018a). *Standardisoimisliiton tehtävät*. [Viitattu 6.9.2018]. Saatavissa: https://www.sfs.fi/sfs_ry/sfs_n_tehtavat

Suomen Standardisoimisliitto SFS ry (2018b). *Riskit hallintaan – SFS-ISO 31000*. [Viitattu 7.9.2018]. Saatavissa: https://www.sfs.fi/files/8535/31000_riskienhallinta_esite_A4_web.pdf.pdf

Suomen kyberturvallisuusstrategia (2013). Valtioneuvoston periaatepäätös. 24.1.2013. Turvallisuuskomitean sihteeristö: Forssa Print.

Suomen kyberturvallisuusstrategia (2019). Valtioneuvoston periaatepäätös 3.10.2019. Helsinki: Turvallisuuskomitean sihteeristö-

Suomen tietoturvallisuusstrategia (2016). *Maailman luotetuinta digitaalista liiketoimintaa*. Liikenne- ja viestintäministeriön julkaisuja 7/2016. Julkaistu 19.4.2016. http://urn.fi/URN:ISBN:978-952-243-475-3

Suomidigi 2023. *Ohjeet ja tuki: VAHTI-ohjeet*. Päivitetty 8.8.2023. [Viitattu 8.10.2023]. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet

Svantesson, Dan (2018). *Rättens internationalisering genom digitalisering*. Teoksessa: Rättsinformatik - Juridiken I det digitala informationssamhället. 3. painos. Lund: Studentlitteratur AB, s. 27–53.

Talus, Anu (2019). *From simply sharing the cage to living together: reconciling the right of public access to documents with the protection of personal data in the European legal framework*. Helsingin yliopisto, väitöskirja. Helsinki: Unigrafia.

The Guardian (2017). *Uber concealed massive hack that exposed data of 57m users and drivers*. Kirjoittaja Julia Carrie Wong, julkaistu 22.11.2017. [Viitattu 3.9.2018]. Saatavissa: https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

Tieteen termipankki (2016). *Oikeustiede: Oikeustieteellinen tutkimus*. Kirjoittaja: Raimo Siltala. Päivitetty 12.5.2016. [Viitattu 1.6.2023]. Saatavissa: https://tieteentermipankki.fi/wiki/Oikeustiede:oikeustieteellinen_tutkimus/laajempi_kuvaus

Tieteen termipankki (2018). *Oikeustiede: Eurooppaoikeuden etusijaperiaate*. Kirjoittaja: Tomi Tuominen. Päivitetty 25.6.2018. [Viitattu 1.6.2023]. Saatavissa: https://tieteentermipankki.fi/wiki/Oikeustiede:eurooppaoikeuden etusijaperiaate

Tietosuojavaltuutetun toimisto (2018). *Tietosuojavaltuutetun päätös luetteloksi käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi*. Päivitetty

21.12.2018. [Viitattu 20.3.2019]. Saatavissa: https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista

Tietosuojavaltuutetun toimisto (2019a). *Tietosuojavaltuutetun toimisto*. [Viitattu 25.3.2019]. Saatavissa: https://tietosuoja.fi/tietosuojavaltuutetun-toimisto

Tietosuojavaltuutetun toimisto (2019b). *Pseudonymisoidut ja anonymisoidut tiedot*. [Viitattu 19.3.2019]. Saatavissa: https://tietosuoja.fi/pseudonymisointi-anonymisointi

Tietosuojavaltuutetun toimisto (2019c). *Tietosuojavastaavan nimittäminen*. [Viitattu 19.3.2019]. Saatavissa: https://tietosuoja.fi/tietosuojavastaavan-nimittaminen

Tietosuojavaltuutetun toimisto (2019d). *Tietoturvaloukkaukset*. [Viitattu 20.3.2019]. Saatavissa: https://tietosuoja.fi/tietoturvaloukkaukset

Tietosuojavaltuutetun toimisto (2021a). *Tietoturvaloukkausten dokumentointivelvollisuuden piiriin kuuluvat myös tapahtuma-ajan lokitiedot*. Tietosuojavaltuutetun toimiston tiedote 15.11.2021. [Viitattu 16.10.2022]. Saatavissa: https://tietosuoja.fi/-/tietoturvaloukkausten-dokumentointivelvollisuuden-piiriin-kuuluvat-myos-tapahtuma-ajan-lokitiedot

Tietosuojavaltuutetun toimisto (2021b). *Tietosuojan vaikutustenarvioinnin ohje*. Julkaistu 12/2021. [Viitattu 15.1.2024]. Saatavissa: https://tietosuoja.fi/documents/6927448/66036250/TVA+ohje.pdf/ff0b6e1b-5b89-e85e-a2e5-6c4bd4c0ccfc/TVA+ohje.pdf?t=1639729535787

Tietosuojavaltuutetun toimisto (2023). *Vaikutustenarviointi*. [Viitattu 27.4.2023]. Saatavissa: https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto (2024). *Euroopan tietosuojaneuvoston ohjeet*. [Viitattu 16.6.2024]. Saatavissa: https://tietosuoja.fi/euroopan-tietosuojaneuvoston-ohjeet

Tornberg, Johanna (2016). *Oikeudellinen laatu edunvalvontapalveluissa*. Teoksessa: Society Trapped in the Network – Does it have a future? Rovaniemi: Lapin yliopisto, s. 277–305. https://urn.fi/URN:ISBN:978–952–484–917–3

Traficom, kyberturvallisuuskeskus (2023a). *Hyväksytyt tietoturvallisuuden arviointilaitokset*. Päivitetty 28.6.2022. [Viitattu 11.10.2023]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset

Traficom, kyberturvallisuuskeskus (2023b). *Arviointi, hyväksyntä ja neuvonta*. Päivitetty 20.3.2023. [Viitattu 11.10.2023]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta?toggle=Liikenne-%20ja%20viestint%C3%A4virasto%20Traficomin%20ohje%20tietoj%C3%A4rjestelmien%20arviointi-%20ja%20hyv%C3%A4ksynt%C3%A4prosesseista&toggle=Arviointilaitokseksi%20hyv%C3%A4ksymist%C3%A4%20koskeva%20hakemus

Traficom, kyberturvallisuuskeskus (2023c). *Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi.* Päivitetty: 6.3.2023. [Viitattu 19.5.2023]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi?toggle=Tekstiviestitse%20tapahtuva%20todennus&toggle=Todennuslaite%20tai%20suojausavain&toggle=Todennussovellus

Traficom, kyberturvallisuuskeskus (2024a). *M365-tietomurroissa hyödynnetään yhä useammin AiTM-tietojenkalastelutekniikkaa*. Ohjeet ja oppaat tietoturva-ammattilaisille. Päivitetty 8.4.2024. [Viitattu 22.4.2024]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/m365-tietomurroissa-hyodynnetaan-yha-useammin-aitm?toggle=AiTM-kalastelun%20kulku&toggle=K%C3%A4ytt%C3%A4j%C3%A4tilimurron%20tyypillinen%20kulku

Traficom, kyberturvallisuuskeskus (2024b). *Kybermittari*. Tilannekuva- ja verkostojohtaminen. Päivitetty 12.6.2024. [Viitattu 4.7.2024]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

Traficomin julkaisuja 2/2020. *Kyberturvallisuus ja yrityksen hallituksen vastuu*. Julkaisija: Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus. [Viitattu 24.2.2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Traficomin julkaisuja 13/2020. *Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)*. Julkaisija: Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus. Versio 1.1 – Maaliskuu 2020. [Viitattu 8.10.2023]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Traficomin julkaisuja 21/2022. *Toimintaohje – Toimitusketjuhyökkäys*. Julkaisija: Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus. [Viitattu 20.12.2023]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toimitusketjuhy%C3%B6kk%C3%A4ysToimintaohje.pdf

Traficomin julkaisuja 30/2022. *Tekoälyn mahdollistamat kyberhyökkäykset*. Julkaisija: Liikenne- ja viestintävirasto Traficom. Julkaistu: 13.12.2022. [Viitattu 18.3.2023]. Saatavissa: https://traficom.fi/sites/default/files/media/publication/TRAFICOM_Teko%C3%A4lyn_mahdollistamat_kyberhy%C3%B6kk%C3%A4ykset%202022-12-12_web.pdf

Tuori, Kaarlo (1999a). *Yleinen järjestys ja turvallisuus -perusoikeusko?* Lakimies 6–7/1999, 10.artikkeli, s. 920–931. Helsinki: Suomalainen lakimiesyhdistys. [Viitattu 27.8.2024]. Saatavissa: https://www.edilex.fi/lakimies/19010020

Tuori, Kaarlo (1999b). *Perusoikeuksien ja ihmisoikeuksien turvaamisvelvollisuus*. Teoksessa: Perusoikeudet. Toimittaja: Pekka Hallberg. Helsinki: WSLT, s. 667–674.

Turunen, Santtu (2005). *KKO 2005:3 Tyytymättömyyden ilmoittaminen sähköpostilla*. Teoksessa: KKO:n ratkaisut kommentein 2005:I. Toimittanut: Pekka Timonen. Helsinki: Alma Talent Oy, Verkkokirjahylly.

Turvallisuuskomitea (2017). *Suomen kyberturvallisuusstrategian toimeenpanoohjelma 2017–2020*. [Viitattu 6.9.2018]. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

Turvallisuuskomitea (2018). *Kyberturvallisuuden sanasto*. Helsinki: Sanastokeskus TSK ry. [Viitattu 6.9.2018]. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Työ- ja elinkeinoministeriö (2023). *Digimarkkinasäädös*. [Viitattu 26.1.2023]. Saatavissa: https://tem.fi/digimarkkinasaados

Työturvallisuuskeskus (2019). *Työturvallisuus ja työsuojelu*. 1. painos. Helsinki: Työturvallisuuskeskus.

Vaasan yliopiston opinto-opas 2023–2024: Informaatio- ja tietotekniikkaoikeus.

VAHTI 7/2003. *Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa*. Valtionvarainministeriö, Valtionhallinnon tietoturvallisuuden johtoryhmä 7/2003. Helsinki: Edita Prima Oy.

VAHTI 5/2004. *Valtionhallinnon keskeisten tietojärjestelmien turvaaminen*. Valtionvarainministeriö, Valtionhallinnon tietoturvallisuuden johtoryhmä 5/2004. Helsinki: Edita Prima Oy.

VAHTI 3/2007. *Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan*. Valtionvarainministeriö, Valtionhallinnon tietoturvallisuuden johtoryhmä 3/2007. Helsinki: Edita Prima Oy.

VAHTI 2/2010. *Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta*. Valtionvarainministeriö, Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2010.

VAHTI 4/2013. *Henkilöstön tietoturvaohje*. Valtiovarainministeriö, Valtiohallinnon tietoturvallisuuden johtoryhmä 4/2013. Juvenes Print - Suomen Yliopistopaino Oy.

VAHTI 1/2016. *EU-tietosuojan kokonaisuudistus*. Valtiovarainministeriö, Valtiohallinnon tietoturvallisuuden johtoryhmä 1/2016.

VAHTI 2/2016. *Toiminnan jatkuvuudenhallinta*. Valtiovarainministeriö, Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmä 2/2016.

Valtiovarainministeriö (2017a). *Tieto- ja kyberturvallisuus*. [Viitattu 23.3.2017]. Saatavissa: http://vm.fi/tieto-ja-kyberturvallisuus

Valtiovarainministeriö (2017b). *Ohjaus*. [Viitattu 23.3.2017]. Saatavissa: http://vm.fi/ohjaus

Valtiovarainministeriö (2018). *Tietoturvallisuuden standardisointiverkosto - Kokous 1/2018 – VAHTI 100*. 13.2.2018. [Viitattu 10.9.2018]. Saatavissa: https://www.viestintavirasto.fi/attachments/esitykset/Tiesta_kokous_01_2018_liite_3_VAHTI_100.pdf

Valtiovarainministeriö (2022). *Käsikirja digilainsäädännön soveltamisesta*. [Viitattu 24.1.2023]. Saatavissa: https://www.suomidigi.fi/sites/default/files/2022-12/VM_kasikirja_digilainsaadannon_soveltamisesta_1.pdf

Valtiovarainministeriö (2023). *EU:n digisäädökset: EU:n digisäädöksillä luodaan pelisääntöjä digitaalisen ajan toimintaympäristöön*. [Viitattu 26.1.2023]. Saatavissa: https://vm.fi/eu-n-digisaadokset

Valtiovarainministeriön julkaisu 28/2016. *Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi – OECD:n suositus ja liiteasiakirja*. Julkaistu 09/2016. https://urn.fi/URN:ISBN:978-952-251-790-6

Valtiovarainministeriön julkaisu 10/2017. *Pilkahduksia tulevaisuuteen – digitalisaation ja robotisaation mahdollisuudet*. Julkaistu 15.2.2017. https://urn.fi/URN:ISBN:978-952-251-836-1

Valtiovarainministeriön julkaisuja 22/2017a. *Ohje riskienhallintaan*. Julkaistu 5.6.2017. https://urn.fi/URN:ISBN:978-952-251-862-0

Valtiovarainministeriön julkaisuja 22/2017b. *Ohje riskienhallintaan- LIITTEET 1–6*. Julkaistu 5.6.2017. https://urn.fi/URN:ISBN:978-952-251-862-0

Valtiovarainministeriön julkaisuja 2021:65. *Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta*. Julkaistu 8.11.2021. Lautakunnat. Helsinki: Valtiovarainministeriö. https://urn.fi/URN:ISBN:978-952-367-897-2

Valtiovarainministeriön julkaisuja 2023:8. *Digitalisaation säädöstilanne ja ehdotukset sen edistämiseksi*. Julkaistu 13.2.2023. Helsinki: Valtiovarainministeriö. https://urn.fi/URN:ISBN:978-952-367-257-4

Valtiovarainministeriön julkaisuja 2023:41. *Selvitys digitalisaation ja uusien teknologioiden vaikutuksista tiedonhallintalakiin pohjautuvaan tietoturvallisuussääntelyyn ja suosituksiin*. Julkisen hallinnon ICT. Esiselvitys. Tiedonhallintalautakunta. Helsinki: Valtiovarainministeriö. https://urn.fi/URN:ISBN:978-952-367-437-0

Valtiovarainministeriön julkaisuja 2023:46. *Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) – Suositus ja kriteeristö*. Kuvailulehti 12.6.2023. Tiedonhallintalautakunta. Helsinki: Valtiovarainministeriö. https://urn.fi/URN:ISBN:978-952-367-458-5

Valtiovarainministeriön julkaisuja 2023:57. *Suositus tietoturvallisuudesta hankinnoissa*. Kuvailulehti 4.8.2023. Tiedonhallintalautakunta. Helsinki: Valtiovarainministeriö. https://urn.fi/URN:ISBN:978-952-367-645-9

Valtiovarainministeriön julkaisuja 2024:19. *Suositus tietoturvallisuuden vähimmäisvaatimuksista*. Kuvailulehti 11.3.2024. Tiedonhallintalautakunta. Helsinki: Valtiovarainministeriö. https://urn.fi/URN:ISBN:978-952-367-679-4

Viitanen, Marko (2022). *KKO 2022:23 Datatakavarikko vai telepakkokeino*. Teoksessa: KKO:n ratkaisut kommentein 2022:1. Toimittanut: Pekka Timonen. Helsinki: Alma Talent Oy, Verkkokirjahylly.

Viljanen, Veli-Pekka (2011). *Yksityiselämän suoja (PL 10 §)*. Teoksessa: Perusoikeudet – Oikeuden perusteokset. Toinen uudistettu painos. Helsinki: WSOYpro, s. 389–411.

Viljanen, Pekka (2014). *KKO 2014:86 Potilastietojen luvaton katselu virkarikoksena*. Teoksessa: KKO:n ratkaisut kommentein 2014:II. Toimittanut: Pekka Timonen. Helsinki: Alma Talent Oy, Verkkokirjahylly.

Viljanen, Pekka (2023a). *Yrityssalaisuusrikokset*. Teoksessa: Keskeiset rikokset. Viides uudistettu painos. Toimittanut: Frände, Hyttinen, Kallio, Korkka-Knuts, Matikkala, Tapani, Tolvanen, Viljanen & Wahlberg. Helsinki: Edita, s. 714–770.

Viljanen, Pekka (2023b). *Virkarikokset*. Teoksessa: Keskeiset rikokset. Viides uudistettu painos. Toimittanut: Frände, Hyttinen, Kallio, Korkka-Knuts, Matikkala, Tapani, Tolvanen, Viljanen & Wahlberg. Helsinki: Edita, s. 890–1003.

Voutilainen, Tomi (2006a). *Hyvä sähköinen hallinto*. Helsinki: Edita Publishing Oy.

Voutilainen, Tomi (2006b). *Hyvä tietohallinto ja sen sääntely viranomaistoiminnassa*. Referee-artikkeli, versio 1.0. Julkaistu Edilexissä 15.9.2006. [Viitattu 1.4.2020]. Saatavissa: https://www.ulapland.fi/loader.aspx?id=404ab602-8b00-44a1-875d-2fda14fe709a

Voutilainen, Tomi (2009). *ICT-oikeus sähköisessä hallinnossa – ICT oikeudelliset periaatteet ja sähköinen hallintomenettely*. Joensuun yliopisto, väitöskirja. Helskinki: Edita Publishing Oy.

Voutilainen, Tomi (2012). *Oikeus tietoon – informaatio-oikeuden perusteet*. Helsinki: Edita Publishing Oy.

Voutilainen, Tomi (2019). *Oikeus tietoon – informaatio-oikeuden perusteet*. 2. uudistettu painos. Helsinki: Edita Publishing Oy.

Voutilainen, Tomi (2020). *Digitaalisten palvelujen sääntely*. Helsinki: Alma Talent.

Voutilainen, Tomi (2022). *KHO 2021:110 – Digitaalisen palvelun toiminnallisuudet ja sähköisen asiakirjan lähettäminen määräajassa*. Lakimies 1/2022, s. 222–234.

Voutilainen, Tomi (2023). *Digitaalisten palvelujen sääntely*. 2. uudistettu painos. Helsinki: Alma Talent.

Wahlgren, Peter (2018). *From Lex Scripta to Law 4.0 On Legislation of the Future*. Teoksessa: 50 Years of Law and IT – the Swedish Law and Informatics Research Institute, 1968-2018. Scandinavian Studies in Law, volume 65. Editoija: Peter Wahlgren. Stockholm Institute for Scandinavian Law: Stockholm University 2018, s. 159–174.

Wallin, Anna-Riitta & Nurmi, Pekka (1991). *Tietosuojalainsäädäntö: Henkilörekisterilaki ja siihen liittyvät säädökset*. 2. uudistettu painos. Helsinki: Lakimiesliiton kustannus.

Wiatrowski, Aleksander (2016). *Less Privacy, More Security? Network Society in the Times of Prism*. Teoksessa: Society Trapped in the Network – Does it have a future? Rovaniemi: Lapin yliopisto, s. 95–118. https://urn.fi/URN:ISBN:978–952–484–917–3

Widlund, Joonas (2020). *Kansallinen turvallisuus: Vapauden ehto vai rajoitus?* Julkaistu 24.6.2020. Oikeus 2/ 2020, Referee-artikkeli, s. 134–153. [Viitattu 11.10.2020]. Saatavissa: <https://www.edilex.fi/oikeus/21106>.

Ämmälä, Tuula (1993). *Oikeustoimen hyvän tavan vastaisuudesta*. Teoksessa: Hyvän tavan vastaisuudesta. Toimittanut: Ari Saarnilehto. Turku: Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja, B, muut kokoomateokset N:o 2, s. 5–47.

Säädösluettelo

1.1.1734/4	Oikeudenkäymiskaari
19.12.1889/39	Rikoslaki
31.5.1974/412	Vahingonkorvauslaki
22.12.1978/1061	Laki sopimattomasta menettelystä elinkeinotoiminnassa
30.4.1987/471	Henkilörekisterilaki
22.4.1999/523	Henkilötietolaki - kumottu lailla 1050/2018
22.4.1999/565	Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta - kumottu lailla 516/2004
21.5.1999/621	Julkisuuslaki (laki viranomaisen toiminnan julkisuudesta)
11.6.1999/731	Suomen perustuslaki
12.11.1999/1030	Julkisuusasetus (asetus viranomaiset toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta) - kumottu pääosin 1.1.2020
26.1.2001/55	Työsopimuslaki
9.2.2001/119	Vesihuoltolaki
23.8.2002/738	Työturvallisuuslaki
24.1.2003/13	Asiointilaki (laki sähköisestä asioinnista viranomaistoiminnassa)
6.6.2003/434	Hallintolaki
11.6.2004/485	Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta
16.6.2004/516	Sähköisen viestinnän tietosuojalaki - kumottu lailla 917/2014
24.6.2004/588	Laki kansainvälisistä tietoturvallisuusvelvoitteista
13.8.2004/759	Työelämän tietosuojalaki (laki yksityisyyden suojasta työelämässä)
23.6.2005/503	Laki liikennejärjestelmästä ja maanteistä
5.8.2005/623	Alusliikennepalvelulaki
27.8.2021/784	Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä – kumottu lailla 703/2023

30.3.2007/334 1333/2021	YT-laki (laki yhteistoiminnasta yrityksissä) - kumottu lailla
18.7.2008/521	Vakuutusyhtiölaki
19.12.2008/878	Laki Finanssivalvonnasta
7.8.2009/617	Tunnistus- ja luottamuspalvelulaki (laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista)
24.6.2010/629	Laki eräistä EU-direktiiveissä säädetyistä lääkinnällisistä laitteista
1.7.2010/681	Tietoturvallisuusasetus (valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa) - kumottu 1.1.2020
8.4.2011/304	Rautatielaki - kumottu lailla 1302/2018
22.7.2011/806	Pakkokeinolaki
22.7.2011/872	Poliisilaki
22.12.2011/1405	Arviointilaitoslaki (laki tietoturvallisuuden arviointilaitoksista)
22.12.2011/1406	Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista
29.12.2011/1552	Valmiuslaki
9.8.2013/588	Sähkömarkkinalaki
30.12.2013/1226	Laki valtion yhteisten tieto- ja viestintäteknisten palveluiden järjestämisestä
8.8.2014/610	Laki luottolaitostoiminnasta
19.9.2014/726	Turvallisuusselvityslaki
7.11.2014/864	Ilmailulaki
7.11.2014/917	Laki sähköisen viestinnän palveluista (entinen tietoyhteiskuntakaari)
13.1.2015/10	Turvallisuusverkkolaki (laki julkisen hallinnon turvallisuusverkkotoiminnasta)
4.12.2015/1412	Laki kaupunkiraideliikenteestä - kumottu lailla 1302/2018
29.6.2016/571	Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (tukipalvelulaki)
24.5.2017/320	Liikennekaari (laki liikenteen palveluista)

25.8.2017/587	Maakaasumarkkinalaki
28.12.2017/1070	Laki kaupankäynnistä rahoitusvälineillä
10.8.2018/595	Liikesalaisuuslaki
5.12.2018/1050	Tietosuojalaki
5.12.2018/1054	Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (rikosasioiden tietosuojalaki)
28.12.2018/1302	Raideliikennelaki
15.3.2019/306	Digipalvelulaki (laki digitaalisten palvelujen tarjoamisesta)
9.8.2019/906	Tiedonhallintalaki (laki julkisen hallinnon tiedonhallinnasta)
30.12.2021/1333	Yhteistoimintalaki
14.4.2023/703	Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (asiakastietolaki)
16.1.2024/18	Laki verkon välityspalvelujen valvonnasta

EU-asetukset, direktiivit ja päätökset

1995/46/EY	Euroopan parlamentin ja neuvoston direktiivi 1995/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta käsittelystä (”henkilötietodirektiivi”)
2002/58/EY	Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (”sähköisen viestinnän tietosuojadirektiivi”)
2002/584/YOS	Neuvoston puitepäätös 2002/584/YOS eurooppalaisesta pidätysmääräyksestä ja jäsenvaltioiden välisistä luovuttamismenettelyistä
2003/361/EY	Komission suositus mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä
2005/222/YOS	Neuvoston puitepäätös 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä
2008/977/YOS	Neuvoston puitepäätös 2008/977/YOS, rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta (”EU:n tietosuojapuitepäätös”)
2013/40/EU	Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta (”tietoverkkorikosdirektiivi”)
2013/488/EU	Neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä
2016/679/EU	Euroopan parlamentin ja neuvoston asetus 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (”yleinen tietosuoja-asetus, GDPR”)
2016/680/EU	Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta (”direktiivi lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta eli tietosuojadirektiivi”)

2016/798/EU	Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/798 rautateiden turvallisuudesta
2016/1148/EU	Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (”verkko- ja tietoturvadirektiivi eli NIS-direktiivi”)
2016/2102/EU	Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/2102 julkisen sektorin elinten verkkosivujen ja mobiilisovellusten saavutettavuudesta (”saavutettavuusdirektiivi”)
2018/1972/EU	Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972 eurooppalaisesta sähköisen viestinnän säännöstöstä (”teledirektiivi”)
2019/881/EU	Euroopan unionin kyberturvallisuusvirasto ENISA:sta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (”kyberturvallisuusasetus”)
2022/868/EU	Euroopan parlamentin ja neuvoston asetus (EU) 2022/868 eurooppalaisen datan hallinnoinnista ja asetuksen (EU) 2018/1724 muuttamisesta (”datanhallinta-asetus, Data Governance Act”)
2022/1925/EU	Euroopan parlamentin ja neuvoston asetus (EU) 2022/1925 kilpailullisista ja oikeudenmukaista markkinoista digitaalialalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta (”digimarkkinasäädös, Digital Markets Act”)
2022/2065/EU	Euroopan parlamentin ja neuvoston asetus (EU) 2022/2065 digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta (”digipalvelusäädös, Digital Services Act)
2022/2554/EU	Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554 finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta (”DORA-säädös”)
2022/2555/EU	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 (”NIS 2 -direktiivi, kyberturvallisuusdirektiivi”)

2022/2557/EU	Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557 kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta (”resilienssidirektiivi eli CER-direktiivi, Critical Entities Resilience Directive”)
2023/436/EU	Neuvoston päätös (EU) 2023/436 jäsenvaltioiden valtuuttamisesta ratifioimaan Euroopan unionin edun mukaisesti tietoverkkorikollisuutta koskevan yleissopimuksen toinen lisäpöytäkirja tiiviimmästä yhteistyöstä ja sähköisen todistusaineiston luovuttamista
2023/2854/EU	Euroopan parlamentin ja neuvoston asetus (EU) 2023/2854 datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä ja asetuksen (EU) 2017/2394 ja direktiivin (EU) 2020/1828 muuttamisesta (”datasäädös”)
2024/1689/EU	Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689 tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (”tekoälysäädös”)

Hallituksen esitykset

HE 58/1988 vp. *Hallituksen esitys Eduskunnalle virkarikoslainsäädännön uudistamisesta.*

HE 66/1988 vp. *Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen ensimmäisen vaiheen käsittäväksi rikoslain ja eräiden muiden lakien muutoksiksi.*

HE 94/1993 vp. *Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi.*

HE 309/1993 vp. *Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.*

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

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

HE 96/1998 vp. *Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.*

HE 184/1999 vp. *Hallituksen esitys Eduskunnalle yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi.*

HE 75/2000 vp. *Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi.*

HE 17/2002 vp. *Hallituksen esitys Eduskunnalle laiksi sähköisestä asioinnista viranomaistoiminnassa.*

HE 125/2003 vp. *Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi.*

HE 162/2003 vp. *Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta.*

HE 153/2006 vp. *Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain, pakkokeinolain 4 luvun, esitutkintalain 27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioista annetun lain 15 ja 23 §:n muuttamisesta.*

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

HE 222/2010 vp. *Hallituksen esitys Eduskunnalle esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi.*

HE 57/2013 vp. *Hallituksen esitys eduskunnalle turvallisuusselvityslaiksi sekä siihen liittyviksi laeiksi*

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

HE 46/2014 vp. *Hallituksen esitys eduskunnalle oikeudenkäymiskaaren 17 luvun ja siihen liittyvän todistelua yleisissä tuomioistuimissa koskevan lainsäädännön uudistamiseksi.*

HE 232/2014 vp. *Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.*

HE 151/2017 vp. *Hallituksen esitys eduskunnalle laeiksi sijoituspalvelulain muuttamisesta ja kaupankäynnistä rahoitusvälineillä sekä eräiksi niihin liittyviksi laeiksi.*

HE 192/2017 vp. *Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta.*

HE 198/2017 vp. *Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.*

HE 202/2017 vp. *Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi.*

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

HE 31/2018 vp. *Hallituksen esitys eduskunnalle laiksi henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä sekä eräiksi siihen liittyviksi laeiksi.*

HE 49/2018 vp. *Hallituksen esitys eduskunnalle liikesalaisuuslaiksi ja eräiksi siihen liittyviksi laeiksi.*

HE 60/2018 vp. *Hallituksen esitys eduskunnalle laeiksi digitaalisten palvelujen tarjoamisesta sekä sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta.*

HE 97/2018 vp. *Hallituksen esitys eduskunnalle laeiksi yksityisyyden suojasta työelämässä annetun lain ja lasten kanssa työskentelevien rikostaustan selvittämisestä annetun lain 10 §:n muuttamisesta.*

HE 105/2018 vp. *Hallituksen esitys eduskunnalle raideliikennelaiksi ja laiksi liikenteen palveluista annetun lain muuttamisesta.*

HE 144/2018 vp. *Hallituksen esitys eduskunnalle laiksi sähkömarkkinalain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.*

HE 226/2018 vp. *Hallituksen esitys eduskunnalle laeiksi sähköisen viestinnän palveluista annetun lain ja julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain muuttamisesta.*

HE 264/2018 vp. *Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta ja väliaikaisesta muuttamisesta.*

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

HE 98/2020 vp. *Hallituksen esitys eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.*

HE 237/2020 vp. *Hallituksen esitys eduskunnalle laeiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta sekä vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta ja väliaikaisesta muuttamisesta annetun lain voimaantulosäännöksen muuttamisesta.*

HE 63/2022 vp. *Hallituksen esitys eduskunnalle laeiksi valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta.*

HE 217/2022 vp. *Hallituksen esitys eduskunnalle laeiksi pakkokeinolain ja esitutkintalain muuttamisesta sekä niihin liittyviksi laeiksi.*

HE 50/2023 vp. *Hallituksen esitys eduskunnalle laeiksi sähköisen viestinnän palveluista annetun lain ja sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta.*

HE 70/2023 vp. *Hallituksen esitys eduskunnalle laiksi verkon välityspalvelujen valvonnasta ja eräiksi muiksi laeiksi.*

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

HE 67/2024 vp. *Hallituksen esitys eduskunnalle laiksi Finanssivalvonnasta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.*

Luonnos: *Hallituksen esitys laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi.*

Muut virallislähteet

COM (2017) 10 final: *Ehdotus Euroopan parlamentin ja neuvoston asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta ("sähköisen viestinnän tietosuoja-asetus, ePrivacy-asetus")*. Euroopan komissio: Brysseli 10.1.2017.

COM (2021) 206 final: *Ehdotus Euroopan parlamentin ja neuvoston asetus tekoälyä koskevista yhdenmukaistetuista säännöistä ja tiettyjen unionin säädösten muuttamisesta ("Tekoälysäädös, Artificial Intelligence Act")*. Euroopan komissio: Brysseli 21.4.2021.

COM (2022) 68 final: *Ehdotus Euroopan parlamentin ja neuvoston asetus datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä ("Datasäädös, Data Act")*. Euroopan komissio: Brysseli 23.2.2022.

COM (2022) 197 final: *Ehdotus Euroopan parlamentin ja neuvoston asetukseksi eurooppalaisesta terveysdata-avaruudesta*.

COM (2022) 454 final: *Ehdotus Euroopan parlamentin ja neuvoston asetus digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvavaatimuksista ja asetuksen (EU) 2019/1020 muuttamisesta* ("Kyberkestävyyssäädös, CRA – Cyber Resilience Act"). Euroopan komissio: Brysseli 15.9.2022.

COM (2023) 209 final: *Proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents* ("Kybersolidaarisuussäädös"). Euroopan komissio: Strasbourg 18.4.2023.

Euroopan datastrategia (C 494/37): *Euroopan parlamentin päätöslauselma 25. maaliskuuta 2021 Euroopan datastrategiasta (2020/2217(INI). 2021/C 494/04. P9_TA(2021)0098*.

Euroopan neuvoston yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi (Euroopan ihmisoikeussopimus, EIS), 4.11.1950

Euroopan neuvoston tietosuojasopimus, yleissopimus nro 108.

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus eli tietoverkkorikossopimus (ETS nro 185), 23.11.2001.

Euroopan neuvosto: *Lisäpöytäkirja atk-järjestelmien avulla tehtyjen rasismiin tai muukalaisvihaan perustuvien tekojen kriminalisoimisesta* (ETS nro 189), 28.1.2003.

Euroopan neuvosto: *Tietoverkkorikollisuutta koskevan yleissopimuksen toinen lisäpöytäkirja tiiviimmästä yhteistyöstä ja sähköisen todistusaineiston luovuttamisesta* (EUVL L 63), 28.2.2023.

Euroopan parlamentin päätöslauselma RC-B8-0154/2019: *Kiinalaisen teknologian lisääntymiseen EU:ssa liittyvät turvallisuusuhkat ja mahdolliset EU:n toimet niiden vähentämiseksi*. 12.3.2019.

Euroopan unionin neuvosto, Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime 6.6.2019. Neuvoston pääsihteeristö, 10083/19.

Euroopan unionin neuvosto, Euroopan digitaalisen tulevaisuuden rakentaminen - Neuvoston päätelmät 9.6.2020. Neuvoston pääsihteeristö, 8711/20.

Euroopan unionin neuvosto, Neuvoston päätelmät internetiin yhdistettyjen laitteiden kyberturvallisuudesta 2.12.2020. Neuvoston pääsihteeristö, 13629/20.

Euroopan unionin neuvosto, Neuvoston päätelmät EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle 22.3.2021. Neuvoston pääsihteeristö, 7290/21.

Euroopan unionin neuvosto, Neuvoston päätelmät tieto- ja viestintäteknisen toimitusketjun turvallisuudesta 17.10.2022. Neuvoston pääsihteeristö, 13664/22.

Euroopan unionin neuvosto, Council conclusions on digital empowerment to protect and enforce fundamental rights in the digital age 20.10.2023. Neuvoston pääsihteeristö, 14309/23.

Euroopan unionin neuvosto, EU:n digitaalipolitiikan tulevaisuus – Neuvoston päätelmät 21.5.2024. Neuvoston pääsihteeristö, 9957/24.

Euroopan unionin neuvosto, Council Conclusions on the Future of Cybersecurity: implement and protect together 21.5.2024. Neuvoston pääsihteeristö, 10133/24

Euroopan unionin perusoikeuskirja, juhlallinen julistus 18.12.2000 (2000/C 364/01).

EV 187/2017 vp. *Eduskunnan vastaus: Hallituksen esitys eduskunnalle laeiksi sijoituspalvelulain muuttamisesta ja kaupankäynnistä rahoitusvälineillä sekä eräiksi niihin liittyviksi laeiksi*.

EV 77/2018 vp. *Eduskunnan vastaus: Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta*.

EV 113/2018 vp. *Eduskunnan vastaus: Hallituksen esitys eduskunnalle laiksi henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä sekä eräiksi siihen liittyviksi laeiksi*.

EV 236/2018 vp. *Eduskunnan vastaus: Hallituksen esitys eduskunnalle laeiksi yksityisyyden suojasta työelämässä annetun lain ja lasten kanssa työskentelevien rikostaustan selvittämisestä annetun lain 10 §:n muuttamisesta*.

HaVM 38/2018 vp. *Hallintovaliokunnan mietintö: Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi*.

KOM (2007) 267 lopullinen. *Komission tiedonanto neuvostolle, Euroopan parlamentille ja alueiden komitealle: Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi*. Euroopan yhteisöjen komissio: Bryssel 22.5.2007.

LaVM 29/2014 vp. *Lakivaliokunnan mietintö 29/2014 vp: Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.*

LiVM 10/2014 vp. *Liikenne- ja viestintävaliokunnan mietintö 10/2014 vp: Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.*

LVM037:00/2016. *Säädöshankepäätös: Euroopan parlamentin ja neuvoston verkko- ja tietoturvadirektiivin kansallinen täytäntöönpano.* Asiakirja 213394, Liikenne- ja viestintäministeriö.

LVM044:00/2022. *Säädösvalmistelu: Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallinen täytäntöönpano.*

OM005:00/2017 (2018). *EU:n tietosuojadirektiivin täytäntöönpano*. Säädösvalmistelu. Oikeusministeriön hankkeet.

P9_TA(2023)0236. *Tekoälysäädös. Euroopan parlamentin tarkistukset 14. kesäkuuta 2023 ehdotukseen Euroopan parlamentin ja neuvoston asetukseksi tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös) ja tiettyjen unionin säädösten muuttamisesta (COM(2021)0206 – C9-0146/2021–2021/0106(COD). Tavallinen lainsäätämisjärjestys: ensimmäinen käsittely. (https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_FI.pdf)*

PeVL 71/2002 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys hautaustoimilaiksi.*

PeVL 9/2004 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi.*

PeVL 10/2004 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta.*

PeVL 19/2008 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys laiksi Jokelan koulukeskuksessa sattuneiden kuolemaan johtaneiden tapahtumien tutkinnasta.*

PeVL 6/2009 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys valmiuslaiksi ja eräiksi siihen liittyviksi laeiksi.*

PeVL 18/2014 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.*

PeVL 31/2017 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys eduskunnalle laiksi valtakunnallisista opinto- ja tutkintarekistereistä Sivistysvaliokunnalle.*

PeVL 14/2018 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.*

PeVL 73/2018 vp. *Perustuslakivaliokunnan lausunto: Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.*

PeVM 25/1994 vp. *Perustuslakivaliokunnan mietintö: N:o 25 hallituksen esityksestä perustuslakien perusoikeussäännösten muuttamisesta.*

PeVM 4/2018 vp. *Perustuslakivaliokunnan mietintö: Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.*

StVL 2/2024 vp. *Sosiaali- ja terveysvaliokunnan lausunto: Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi eurooppalaisesta terveysdata-avaruudesta.*

TyVM 8/2004 vp. *Työelämä- ja tasa-arvovaliokunnan mietintö: Hallituksen esitys laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta.*

TyVL 14/2008 vp. *Työelämä- ja tasa-arvovaliokunnan lausunto: Hallituksen esitys sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta.*

U 61/2022 vp. *Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi eurooppalaisesta terveysdata-avaruudesta.*

YK:n taloudellisia, sosiaalisia ja sivistyksellisiä oikeuksia koskeva kansainvälinen yleissopimus (TSS-sopimus), New York 16.12.1966.

YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (KP-sopimus), New York 16.12.1966.

Tietosuojavaltuutetun toimiston kannanotot

TSV 4.9.2015, dnro. 1661/41/2014. *Tietosuojavaltuutetun lausunto 4.9.2015: Yrityksen kulunvalvontajärjestelmän henkilörekisterin käytöstä.*

TSV 28.2.2017, dnro. 2450/41/2016 & 2856/41/2012. *Tietosuojavaltuutetun vastaus 28.2.2017: Millä edellytyksillä pilvipalveluita voidaan käyttää opetuksen järjestämisessä.*

TSV 12.7.2017, dnro. 1081/41/2017. *Tietosuojavaltuutetun toimiston vastaus 12.7.2017: Seloste käsittelytoimista.*

TSV 9.10.2019, dnro. 1689/41/17. *Apulaistietosuojavaltuutetun päätös 9.10.2019: Vankien henkilötietojen käsittely.*

TSV 3.1.2020, dnro. 60/171/2020. *Apulaistietosuojavaltuutetun päätös 3.1.2020: Huomautus tietoturvaloukkauksesta ilmoittamisesta, kun rekisteröityjen yhteystiedot eivät ole rekisterinpitäjän tiedossa.*

TSV 4.6.2021, dnro 4900/182/18. *Apulaistietosuojavaltuutetun päätös sisäänrakennettua ja oletusarvoista tietosuojaa, rekisteröityjen informointia, tietojen minimointia, säilytyksen rajoittamista ja henkilötietojen käsittelyn läpinäkyvyyttä koskevassa asiassa.*

TSV 5.7.2021, dnro 3843/163/20. *Apulaistietosuojavaltuutetun ja seuraamuskollegion päätökset: Työntekijän sijaintiin liittyvien henkilötietojen käsittely työajanseurannassa.*

TSV 7.12.2021, dnro 1150/161/2021. *Apulaistietosuojavaltuutetun päätös 7.12.2021: Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen.*

TSV 31.5.2022, dnro 6813/171/21. *Apulaistietosuojavaltuutetun päätös rekisteröityjen sijaintitietojen käsittelyä koskevassa asiassa.*

TSV 31.5.2022, dnro 1141/161/22. *Apulaistietosuojavaltuutetun päätös rekisteröityjen sijaintitietojen käsittelyä koskevassa asiassa.*

TSV 31.5.2022, dnro 2464/161/22. *Apulaistietosuojavaltuutetun päätös rekisteröityjen sijaintitietojen käsittelyä koskevassa asiassa.*

TSV 15.11.2022, dnro 4022/171/22. *Apulaistietosuojavaltuutetun päätös henkilötietojen käsittelyn turvallisuutta koskevassa asiassa.*

Tuomioistuinten ja viranomaisten ratkaisut

Euroopan ihmisoikeustuomioistuin

EIT 3.7.2007 asianro. 62617/00, Copland v. Yhdistynyt kuningaskunta

EIT 17.7.2008 asianro. 40412/98, I. V. Finland

EIT 5.9.2017 asianro. 61496/08, Bărbulescu v. Romania

Euroopan unionin tuomioistuin

EUT 24.11.2011 asianro. C-70/10, Scarlet Extended SA v. SABAM (ECLI:EU:C:2011:771)

EUT 17.10.2013 asianro. C-291/12, Schwarz v. Stadt Bochum (ECLI:EU:C:2013:670)

EUT 19.10.2016 asianro. C-582/14, Breyer v. Saksan liittotasavalta (ECLI:EU:C:2016:779)

EUT 20.12.2017 asianro. C-434/16, Nowak (ECLI:EU:C:2017:994)

EUT 5.6.2018 asianro C-210/16 Wirtschaftsakademie Schleswig-Holstein (ECLI:EU:C:2018:388)

EUT 10.7.2018 asianro. C25-17, Tietosuojavaltuutettu v. Jehovan todistajat (ECLI:EU:C:2018:551)

EUT 16.7.2020 asianro. C-311/18, Schrems II (ECLI:EU:C:2020:559)

EUT 17.6.2021 asianro. C-597/19, M.I.C.M (ECLI:EU:C:2021:492)

EUT 22.6.2023 asianro. C-579/21, Pankki S (ECLI:EU:C:2023:501)

EUT 4.5.2023 asianro. C-487/21, Österreichische Datenschutzbehörde ja CRIF (ECLI:EU:C:2023:369)

EUT 14.12.2023 asianro. C-340/21, VB v. Natsionalna agentsia za prihodite (ECLI:EU:C:2023:986)

EUT 25.1.2024 asianro C-687/21, MediaMarktSaturn (ECLI:EU:C:2024:72)

Korkein oikeus

KKO 1999:83 taltio 1850

KKO 2005:3 taltio 7

KKO 2010:39 taltio 1296

KKO 2011:63 taltio 1866

KKO 2013:20 taltio 788

KKO 2014:86 taltio 2393

KKO 2015:42 taltio 1169

KKO 2019:86 taltio 1741

KKO 2022:23 taltio 630

KKO 2022:32 taltio 809

Korkein hallinto-oikeus

KHO 2007:83 taltio 3078

KHO 27.9.2013 taltio 3084

KHO 12.10.2017 taltio 5055

KHO 2018:112 taltio 3774

KHO 2018:171 taltio 5927

Hallinto-oikeus

Kuopion HAO 11.11.2011 11/0424/2

Helsingin HAO 8.12.2016 16/1028/5

Itä-Suomen HAO 22.12.2023 2891/2023

Käräjäoikeus

Länsi-Uudenmaan käräjäoikeus 30.4.2024 R 23/3965

Työtuomioistuin

TT 2020:4, 10.1.2020, Dnro R 55/18

Bonnin oikeusistuin (Saksa)

10 O 171/18

Eduskunnan oikeusasiamiehen kanslia

EOAK 1777/2009, Dnro 1777/4/08

EOAK 537/2010, Dnro 537/4/10

EOAK 1140/2011, Dnro 1140/4/11

EOAK 2455/2016

EOAK 4542/2021