

Veikko Vauhkonen – Jesse Heiskanen

Kyberturvallisuussäätely – tulkinta ja soveltaminen

© Edilex Lakitieto Oy ja tekijät

Kansi: Anu Korpijärvi

Taitto: Aste Helsinki Oy

Kannen kuva: KanawatTH / Shutterstock.com

Kustantaja: Edilex Lakitieto Oy

lakitieto.edilex.fi

ISBN 978-951-37-9398-2

Anna palautetta kirjasta: toimitus.edilex.kustannus@almamedia.fi

Painopaikka: Otavan kirjapaino Oy, Keuruu 2025



ALKUSANAT

Kyberturvallisuussäätely on uusi ja nykyisessä maailmanajassa erittäin ajankohtainen kokonaisuus. Se on moninainen palapeli uutta EU-lainsäädäntöä ja vanhempaa kansallista säätelyä. Viime vuosina on hyväksytty uutta horisontaalista kyberturvallisuussäätelyä. Kyberturvallisuuslaki tuli voimaan 8.4.2025 saattaen voimaan NIS 2 -direktiiviin perustuvia velvoitteita Suomessa. EU:n kyberkestävyyssäädöksen soveltaminen alkaa pääosin 11.12.2027. Uusia säädöksiä soveltava organisaatio voikin kokea olevansa vaikean paikan edessä – säädökset ovat pitkiä, verrattain monimutkaisia ja monilta osin riskiperusteisia. Riskiperusteisen säätelyn soveltaminen antaa organisaatioille klassisesti sekä vapautta että vastuuta: miten soveltaa kyberturvallisuussäätelyä oikein?

Allekirjoittaneilla on tarjota käytännön työn tueksi tämä teos, joka on tarkoitettu kattavaksi tietolähteeksi ja oppaaksi kaikille kyberturvallisuussäätelyä työssään soveltaville juristeille, kyberturvallisuudesta ja ICT:stä vastaaville asiantuntijoille sekä laitteiden ja ohjelmistojen kehittäjille. Teos soveltuu myös käytettäväksi oppikirjana korkeakouluissa.

Teoksen näkökulma kyberturvallisuuteen on oikeudellinen. Kirjoittajat ovat juristeja ja kirjailijaroolissaan ensikertalaisia. Olemme halunneet saattaa teoksen lukijoiden käytettäväksi mahdollisimman pian kyberturvallisuuslain voimaantulon sekä EU:n kyberkestävyyssäädöksen hyväksymisen jälkeen. Koska säätely on uutta, on teoksessa voitu huomioida vain rajallisesti sellaisia tulkintakysymyksiä, jotka ilmenevät ajan mittaan säätelyä sovellettaessa. Lisäksi eräiden tulkintakysymyksien osalta on saatavilla varsin niukasti oikeuslähteitä. Teoksen sisältämät mahdolliset virheet ovat luonnollisesti kirjoittajien omia ja otamme mielellämme vastaan parannusehdotuksia ja palautetta teoksesta.

Vauhkonen on työskennellyt liikenne- ja viestintäministeriössä kyberturvallisuuteen liittyvän lainsäädännön valmistelutehtävissä. Hän on toiminut NIS 2 -direktiiviä täytäntöönpanoa koskevan direktiivin lainsäädäntöhankkeen vastuuvalmistelijana ja kyberturvallisuuslain esittelijänä sekä osallistunut

kyberkestävyyssäädöstä koskevaan EU-valmisteluun ja sitä täydentävien kansallisten säännösten valmisteluun.

Heiskanen on työskennellyt useamman vuoden Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksessa ensin kansallisen turvallisuussääntelyn valvonnan parissa ja sittemmin CERT/CSIRT-juristina. Nykyisessä tehtävässään hän taiteilee juristina osana Suomen kansallisen kyberturvallisuuden etulinjaa, ainakin viranomaisnäkökulmasta. Päivätyönsä ohella Heiskanen valmistelee kyberturvallisuusaiheista väitöskirjaa Helsingin yliopistossa.

Teoksen kirjoittamisvastuu on jakautunut siten, että Vauhkonen on vastannut kyberturvallisuuslakia ja kyberkestävyyssäädöstä käsittelevien 2–3 lukujen kirjoittamisesta. Heiskanen on vastannut itsenäisesti kyberturvallisuuden, yksityisyyden suojan ja tietosuojan välistä suhdetta käsittelevän 4 luvun kirjoittamisesta sekä kommentoinut ja osallistunut 2–3 lukujen kirjoittamiseen erityisesti haavoittuvuus- ja poikkeamaraportointivelvoitteita koskevan 3.5 jakson osalta. Lukujen 1 ja 5 osalta teos on kirjoitettu yhteisesti.

Kirjoitusprosessi kohtasi yllättävän käänteen, kun matkan varrella Alma Media osti kustantajana toimineen Edilex Lakitieto Oy:n. Haluamme joka tapauksessa osoittaa suuret kiitokset yhteistyöstä kustantajallemme sekä teoksen työstämiseen osallistuneille sen kaikissa vaiheissa. Erittäin lämpimät kiitokset ansaitsee kustannustoimittajamme Emma Matila, jonka ansiosta teos on saatettu painokelpoiseen muotoon. Yhteistyöstä Alma Median kanssa kiitämme erityisesti Heidi Antinkaria. Kirjan alkuvaiheen yhteistyön osalta kiitämme erityisesti Jonna Vihavaista ja Raisa Uljasta, joiden ansiota kirjoitusprosessin käynnistyminen on. Kiitämme alkuvaiheen kustannustoimitusyhteistyöstä Emilia Lindroosia.

Osoitamme luonnollisesti kiitollisuutta kaikille kirjan lukuja niiden eri vaiheissa kommentoineille kollegoillemme. Erityisen lämpimät kiitokset ansaitsevat ainakin Sara Aronen, Oskari Paasikivi, Marko Priiki, Outi Slant ja Eevi Vuorinen. Osoitamme kiitokset myös työnantajillemme kirjoitustyön kohtamasta suopeasta suhtautumisesta.

Haluamme osoittaa kiitokset myös kaikille teille, joiden kanssa olemme käyneet keskusteluja kirjan aihepiiristä ja tehneet yhteistyötä kyberturvallisuussääntelyyn liittyen. Lisäksi osoitamme erityiset kiitokset Kyberturvallisuuskeskuksen kollegoille asiantuntevista kommentteista, joita ilman tämän kirjan tekniset esimerkit eivät olisi osuneet maaliinsa samalla tarkkuudella. Tiedätte kyllä, keitä olette.

Haluamme luonnollisesti myös kiittää puolisoitamme, koska on tässä ollut teillekin jaksamista.

Helsingissä ja Vantaalla kauniin ja historiallisen lämpimän kirjoituskesän jälkeen, lokakuussa 2025.

Veikko Vaubkonen Jesse Heiskanen

SISÄLLYSLUETTELO

ALKUSANAT	V
LYHENTEET	XVII
1 JOHDANTO	1
2 KYBERTURVALLISUUSLAKI JA NIS 2 -DIREKTIIVI	13
2.1 NIS 2 -direktiivi	13
2.1.1 Mikä on NIS 2 -direktiivi?	13
2.1.2 NIS 2 -direktiivin taustasta	16
2.1.3 NIS 2 -direktiivin suhde eräisiin säädöksiin	17
2.1.4 NIS 2 -velvoitteet Suomessa	20
2.2 Kyberturvallisuuslain soveltamisala	21
2.2.1 Soveltamisen periaatteita	21
2.2.1.1 Soveltamisalasäännökset	21
2.2.1.2 Suhde muuhun lainsäädäntöön	21
2.2.1.3 Alueellinen soveltamisala	23
2.2.2 Toimijan määritelmä	25
2.2.2.1 Toimijan yleinen määritelmä	25
2.2.2.2 Poikkeukset kokokriteeristä	30
2.2.2.3 Eräitä huomioita toimijan käsitteestä	32
2.2.2.4 Keskeinen ja tärkeä toimija	33
2.2.3 Soveltamisen alkaminen ja päätyminen	38
2.2.4 Soveltamisalan rajaukset	39
2.2.5 Erimielisyys kyberturvallisuuslain soveltamisesta	42
2.2.6 Kyberturvallisuuslain soveltamisalan ulkopuoliset NIS 2 -toimialat	43
2.2.6.1 Julkishallinto ja tiedonhallintalaki	43
2.2.6.2 Pankkitoiminta ja finanssimarkkinoiden infrastruktuurit	45

2.3	Toimijatyytit.....	46
2.3.1	Johdanto.....	46
2.3.2	Energia.....	48
2.3.2.1	Sähkö.....	48
2.3.2.2	Kaukolämmitys ja -jäähdytys.....	51
2.3.2.3	Kaasu.....	52
2.3.2.4	Öljy.....	53
2.3.2.5	Vety.....	54
2.3.3	Liikenne.....	54
2.3.3.1	Ilmailu.....	54
2.3.3.2	Raideliikenne.....	56
2.3.3.3	Vesiliikenne.....	58
2.3.3.4	Tieliikenne.....	60
2.3.4	Terveys.....	62
2.3.5	Juomavesi.....	66
2.3.6	Jätevesi.....	67
2.3.7	Digitaalinen infrastruktuuri.....	68
2.3.8	Yritysten välinen TVT-palvelujenhallinta.....	73
2.3.9	Avaruus.....	75
2.3.10	Posti- ja kuriiripalvelut.....	76
2.3.11	Jätehuolto.....	78
2.3.12	Kemikaalit.....	79
2.3.13	Elintarvikkeet.....	81
2.3.14	Valmistus.....	82
2.3.14.1	Teollisuus.....	82
2.3.14.2	Lääkinnälliset laitteet.....	86
2.3.15	Digitaalisen palvelun tarjoajat.....	87
2.3.16	Tutkimustoiminta.....	88
2.4	Toimijaluettelo.....	90
2.4.1	Tietojen ilmoittaminen valvovalle viranomaiselle.....	90
2.4.2	Toimijaluettelotietojen käsittelystä.....	95
2.5	Riskinhallintavelvoite.....	96
2.5.1	NIS 2 -direktiivin vaatimuksista riskienhallinnalle.....	96
2.5.2	Yleinen riskienhallintavelvoite.....	100
2.5.3	Kyberturvallisuutta koskeva riskienhallinnan toimintamalli.....	107
2.5.4	Riskienhallinnan toteuttaminen.....	111
2.5.4.1	Riskienhallinnan toimenpiteet.....	111
2.5.4.2	Riskienhallinnassa huomioitavat osa-alueet.....	112
2.5.4.3	Toimenpiteiden riskiperusteinen suhteuttaminen.....	128
2.5.4.4	Valvovan viranomaisen määräykset.....	129
2.5.4.5	Euroopan komission täytäntöönpanosäädökset.....	131

	2.5.4.6 Eurooppalaiset kyberturvallisuuden sertifointijärjestelmät	133
	2.5.5 Johdon vastuu kyberturvallisuuden riskienhallinnassa.....	134
2.6	Poikkeamaraportointi	136
	2.6.1 Ilmoitus- ja raportointivelvollisuudet tiivistetysti	136
	2.6.2 Merkittävä poikkeama.....	137
	2.6.3 Komission täytäntöönpanoasetuksen määritelmä	141
	2.6.4 Poikkeamaraportit viranomaiselle	149
	2.6.4.1 Ensi-ilmoitus.....	149
	2.6.4.2 Jatkoilmoitus.....	151
	2.6.4.3 Poikkeamaa koskeva loppuraportti	153
	2.6.4.4 Poikkeamaa koskeva väliraportti.....	154
	2.6.5 Merkittävästä poikkeamasta tai kyberuhkasta ilmoittaminen palvelujen vastaanottajille.....	155
	2.6.6 Vapaaehtoinen ilmoittaminen	158
	2.6.7 Poikkeamailmoitusten käsittely	160
2.7	Valvonta ja hallinnolliset seuraamukset	164
	2.7.1 Valvovat viranomaiset.....	164
	2.7.2 Valvonnan kohdistaminen.....	171
	2.7.3 Valvontatoimenpiteistä	175
	2.7.3.1 Tiedonsaantioikeus.....	175
	2.7.3.2 Tarkastusoikeus	183
	2.7.3.3 Turvallisuusauditointi	186
	2.7.3.4 Valvontapäätös ja varoitus	187
	2.7.3.5 Johdon toiminnan rajoittaminen.....	189
	2.7.3.6 Eräiden lupien peruuttaminen.....	191
	2.7.3.7 Ilmoitus tietosuojavaltuutetulle	192
	2.7.4 Hallinnollinen seuraamusmaksu.....	194
	2.7.4.1 Tausta	194
	2.7.4.2 Seuraamusmaksun perusteet	196
	2.7.4.3 Seuraamusmaksun määrä.....	198
	2.7.4.4 Seuraamusmaksun määräämättä jättäminen.....	200
	2.7.4.5 Seuraamusmaksulautakunta.....	202
	2.7.5 Muutoksenhaku.....	204
	2.7.6 Valvovien viranomaisten yhteistyö eräissä tilanteissa.....	205
2.8	CSIRT-yksikkö	207
	2.8.1 CSIRT-yksikkö ja sen tehtävät.....	207
	2.8.2 Haavoittuvuuskoordinaatio.....	209
2.9	Eräät varautumista koskevat säännökset.....	213

3	KYBERKESTÄVYYSSÄÄDÖS (CRA)	215
3.1	Kyberkestävyysääädös – mitä ja miksi?	215
3.2	Soveltamisala	219
3.2.1	Soveltamisen kolme kriteeriä	219
3.2.1.1	Digitaalisen elementin sisältävä tuote	220
3.2.1.2	Asettaminen saataville markkinoilla	223
3.2.1.3	Käyttötarkoitus tai kohtuudella ennakoitavissa oleva käyttö	226
3.2.2	Soveltamisalan rajaukset	228
3.2.2.1	Lääkinnälliset laitteet, ajoneuvot ja ilma-alukset	228
3.2.2.2	Poissulkemismenetelmä	231
3.2.2.3	Laivavarusteet	232
3.2.2.4	Varaosat	233
3.2.2.5	Kansallinen turvallisuus, yleinen turvallisuus ja puolustus	233
3.2.3	Soveltamisen alkaminen	234
3.2.3.1	Olennaisten kyberturvallisuusvaatimusten soveltaminen	234
3.2.3.2	Haavoittuvuuksista ja poikkeamista ilmoittaminen	235
3.2.3.3	Merkittävä muutos	235
3.3	Valmistajan velvollisuudet	240
3.3.1	Valmistaja	240
3.3.2	Tuotteen ominaisuudet	241
3.3.2.1	Tuotteen ominaisuuksia koskevat olennaiset kyberturvallisuusvaatimukset	241
3.3.2.2	Kyberturvallisuusriskien arviointi	245
3.3.2.3	Tekniset asiakirjat	247
3.3.2.4	Huolellisuus komponenttien integroinnissa	250
3.3.3	Haavoittuvuuksien käsittelyä koskevat vaatimukset	252
3.3.3.1	Haavoittuvuuksien käsittelyä koskevat olennaiset kyberturvallisuusvaatimukset	252
3.3.3.2	Tietoturvapäivitysten tarjoaminen	255
3.3.3.3	Tukiaika	257
3.3.3.4	Tukiajan päättymisen	261
3.3.4	Vaatimustenmukaisuus	262
3.3.4.1	Vaatimustenmukaisuuden arviointi	262
3.3.4.2	EU-vaatimustenmukaisuusvakuutus ja CE-merkintä	268
3.3.5	Muita valmistajan velvollisuuksia	271
3.3.5.1	Käyttäjälle annettavat tiedot ja ohjeet	271
3.3.5.2	Tuotteen yksilöinti ja valmistajan yhteystiedot	272

3.3.5.3	Valmistajan keskitetty yhteyspiste.....	273
3.3.5.4	Tuotteen kyberturvallisuuteen liittyvien seikkojen dokumentointi.....	274
3.3.5.5	Sarjatuotanto.....	274
3.3.5.6	Toiminnan lopettamisesta ilmoittaminen.....	274
3.4	Muiden talouden toimijoiden velvollisuudet.....	275
3.4.1	Maahantuojien ja jakelijoiden velvollisuudet.....	275
3.4.1.1	Maahantuojat	275
3.4.1.2	Jakelijat.....	278
3.4.2	Valmistajan velvollisuuksien soveltaminen muissa tilanteissa	280
3.4.2.1	Valtuutettu edustaja.....	280
3.4.2.2	Tuotetta muuttava taho	282
3.4.3	Avoimen lähdekoodin ohjelmistovastaavien velvollisuudet.....	283
3.5	Haavoittuvuuksista ja poikkeamista ilmoittaminen.....	290
3.5.1	Haavoittuvuusraportointivelvoitteiden taustasta	290
3.5.2	Valmistajien raportointivelvoitteet.....	294
3.5.2.1	Yleisesti raportointivelvoitteiden sisällöstä	294
3.5.2.2	Aktiivisesti hyödynnetyt haavoittuvuudet.....	295
3.5.2.3	Tuotteen tietoturvaan vaikuttavat vakavat poikkeamat.....	304
3.5.2.4	Raportoitavien poikkeamien ja haavoittuvuuksien välinen suhde.....	309
3.5.2.5	Ilmoituksen vastaanottaja.....	311
3.5.2.6	Käyttäjille tiedottaminen	315
3.5.3	Vapaaehtoinen raportointi	318
3.5.3.1	Vapaaehtoinen raportointi käytännössä.....	318
3.5.3.2	Haavoittuvuustutkijoiden suoja.....	321
3.5.4	Ilmoitusten käsittely	325
3.5.4.1	Ilmoitusten välittäminen jäsenvaltioiden välillä ja ilmoitusten käsittely Suomessa	325
3.5.4.2	Tietojen välittäminen markkinavalvonta- viranomaisille.....	329
3.5.4.3	Ilmoitettujen tietojen käsitteleminen ENISA:ssa....	330
3.5.4.4	Ilmoitusten käsittelyn suhde NIS 2 -direktiivin ja kyberturvallisuuslain mukaiseen haavoittuvuuskoordinaatioon	330
3.5.5	Maahantuojien ja jakelijoiden ilmoitusvelvoitteet	331
3.5.6	Avoimen lähdekoodin ohjelmistovastaavien raportointivelvoitteet	333
3.6	Suhde eräisiin säädöksiin.....	334
3.6.1	Yleinen tuoteturvallisuusasetus	334

3.6.2	Tekoälyasetus ja suuririskisiä tekoälyjärjestelmiä koskevat erityissäännökset	336
3.6.3	Koneasetus	338
3.7	Eräitä muita säännöksiä	339
3.7.1	Markkinavalvonta	339
3.7.2	Ilmoitetut laitokset	341
3.7.3	Hallinnollinen seuraamusmaksu	342
3.7.4	Tuotevastuu	344
3.7.5	Edustajakanteet	345
3.7.6	Kyberkestävyyden sääntelyn testiympäristö	346
4	KYBERTURVALLISUUDEN SUHDE YKSITYISYYDEN SUOJAAN JA TIETOSUOJAAN	347
4.1	Lähtökohdat	347
4.2	Kyberturvallisuus tietosuoja-asetuksen näkökulmasta	355
4.2.1	Tietosuoja-asetuksen lähtökohdat	355
4.2.2	Tietosuoja-asetuksen keskeiset määritelmät kyberturvallisuuden näkökulmasta	357
4.2.2.1	Henkilötiedon käsite	357
4.2.2.2	Henkilötietojen käsittely – kaikki on henkilötietojen käsittelyä	369
4.2.2.3	Rekisterinpitäjä ja henkilötietojen käsittelijä – kuka määrittää kyberturvallisuudessa henkilötietojen käsittelyn tarkoitukset ja keinot?	370
4.2.3	Henkilötietojen tietoturvaperusteinen käsittely	376
4.2.3.1	Kyberturvallisuuden riskienhallinta-toimenpiteiden sisällöstä	376
4.2.3.2	Tietosuojaperiaatteet	378
4.2.3.3	Henkilötietojen käsittelyn oikeusperusteet	385
4.2.3.4	Henkilötietojen käsittelyn turvallisuutta koskevat velvoitteet	394
4.2.3.5	Tietosuojaa koskeva vaikutustenarviointi	403
4.2.4	Henkilötietojen tietoturvaloukkaukset	407
4.2.5	Tietosuojavastaavan rooli	417
4.2.6	Tietosuoja-asetuksen valvonta	420
4.3	Kyberturvallisuus ja viestinnän luottamuksellisuus	422
4.3.1	Kansalliset säännökset sähköisen viestinnän käsittelystä	422
4.3.2	SVPL:n keskeiset määritelmät kyberturvallisuuden kannalta	425
4.3.2.1	Roolipohjaisuus	425

4.3.2.2	Roolit viestinnän käsittelyssä.....	426
4.3.2.3	Viestintänä suojattavat tiedot.....	435
4.3.3	Sähköisen viestinnän käsittelyperusteet.....	439
4.3.3.1	Yleistä käsittelyperusteista.....	439
4.3.3.2	Viestinnän käsittely tietoturvasta huolehtimiseksi.....	444
4.3.3.3	Pahamaineinen Lex Nokia.....	464
4.3.4	Sähköisen viestinnän tietosuojaa koskevan sääntelyn valvonta.....	469
4.3.5	Viestinnän luottamuksellisuuden loukkaamisen rangaistavuus.....	470
4.4	Kyberturvallisuus ja työelämän tietosuojasääntely.....	471
4.4.1	Työelämän tietosuojalain lähtökohdat.....	471
4.4.2	Työelämän tietosuojalain vaatimukset.....	473
4.4.2.1	Tarpeellisuusvaatimus.....	473
4.4.2.2	Työntekijän henkilötietojen keräämisen yleiset edellytykset.....	474
4.4.2.3	Työntekijöiden tekninen valvonta.....	477
4.4.3	Työelämän tietosuojalain valvonta.....	480
4.5	Kyberturvallisuuden riskienhallinnan edellyttämä henkilötietojen käsittely.....	481
4.5.1	Sääntelyn kokonaiskuvan hahmottamisesta.....	481
4.5.2	Kyberturvallisuuden riskienhallinnan sovittaminen tietosuojalainsäädäntöön.....	483
5	KYBERRIKOKSISTA.....	491
5.1	Yleistä kyberrikoksista.....	491
5.1.1	Kyberrikokset.....	491
5.1.2	Kyberrikoksista ilmoittamisesta poliisille.....	497
5.2	Keskeiset kyberrikokset.....	503
5.2.1	Tietomurto.....	503
5.2.1.1	Tietomurron kriminalisoinnin taustasta.....	503
5.2.1.2	Perusmuotoinen tietomurto.....	503
5.2.1.3	Törkeä tietomurto.....	510
5.2.1.4	Tietomurron yritys.....	511
5.2.2	Datavahingonteko.....	515
5.2.2.1	Perusmuotoinen datavahingonteko.....	515
5.2.2.2	Törkeä datavahingonteko.....	516
5.2.2.3	Lievä datavahingonteko.....	518
5.2.3	Viestintäsalaisuuden loukkaus.....	518
5.2.3.1	Perusmuotoinen viestintäsalaisuuden loukkaus...	518
5.2.3.2	Törkeä viestintäsalaisuuden loukkaus.....	522

5.2.4	Tietoliikenteen häirintä	524
5.2.4.1	Perusmuotoinen tietoliikenteen häirintä.....	524
5.2.4.2	Törkeä tietoliikenteen häirintä.....	525
5.2.4.3	Lievä tietoliikenteen häirintä.....	528
5.2.5	Tietojärjestelmän häirintä.....	528
5.2.5.1	Perusmuotoinen tietojärjestelmän häirintä	528
5.2.5.2	Törkeä tietojärjestelmän häirintä	530
5.2.6	Luvaton käyttö kyberrikoksena.....	533
5.2.7	Vaaran aiheuttaminen tietojenkäsittelylle.....	537
5.2.8	Tietoverkkorikosvälineen hallussapito	543
5.3	Kyberrikokset ja kyberturvallisuuslaki	544
 LÄHTEET		547
 ASIAHAKEMISTO		563