IoT-laitteiden tietosuojahaasteet ja lainsäädännön toteutuminen

Turun yliopisto
Tietotekniikan laitos
LuK-tutkielma
Tietojenkäsittelytiede
Kesäkuu 2025
Rhea Nurmi

TURUN YLIOPISTO
Tietotekniikan laitos

Rhea Nurmi: IoT-laitteiden tietosuojahaasteet ja lainsäädännön toteutuminen

LuK-tutkielma, 23 s.
Tietojenkäsittelytiede
Kesäkuu 2025

IoT-teknologioiden nopea kehitys on haastanut niin yritysten innovaatiota kuin perinteisen tietosuojalainsäädännön sovellettavuutta. Tässä tutkielmassa tarkastellaan IoT-järjestelmien tietoturvaa ja tietosuojaa teknisestä ja oikeudellisesta näkökulmasta. Työn tavoitteena on selvittää, miten laitteiden arkkitehtuuri ja toiminnalliset piirteet vaikuttavat tiedon hallintaan ja suojaamiseen, sekä arvioida, miten nykyinen lainsäädäntö vastaa näihin haasteisiin. Tutkielma on toteutettu kirjallisuuskatsauksena. Tutkielma tuo esiin useita teknisiä riskitekijöitä, kuten IoT-järjestelmien hajautetun rakenteen, puutteellisen salauksen ja tiedonkeruun valtavan määrän, jotka yhdessä heikentävät IoT-laitteiden turvallisuutta ja altistavat käyttäjän tietovuodoille. Tiedonkeruun läpinäkymättömyys ja tiedon jakamisen epäselvät periaatteet vaikeuttavat käyttäjän oikeuksien toteutumista. Vaikka yleinen tietosuojaasetus asettaa vahvat vaatimukset yksityisyyden suojalle, monet IoT-sovellukset eivät teknisistä syistä kykene täyttämään näitä vaatimuksia. Oikeudellisen tarkastelun perusteella havaitaan, että nykyinen sääntely ei ratkaise keskeisiä ongelmia, jotka liittyvät vastuunjakoon, läpinäkyvyyteen ja tiedon omistajuuteen. Tutkielma esittää, että keskeisiä kehitystarpeita ovat sääntelyn selkeyttäminen, teknologian vastuullisuuden edistäminen sekä käyttäjien oikeuksien parempi turvaaminen osana kehittyviä IoT-ratkaisuja.

Asiasanat: IoT, tietoturva, tietosuoja, riskienhallinta, vastuu, lainsäädäntö

Sisällys

1 Johdanto

Esineiden internetiin kytkeytyvät laitteet eli IoT-laitteet (Internet of Things) ovat vakiinnuttaneet paikkansa osana modernia yhteiskuntaa ja tarjoavat monia arkea ja turvallisuutta parantavia ratkaisuja. Näitä älykkäitä laitteita käytetään jokapäiväisen elämän helpottamiseen. Esimerkiksi lääketieteelliset IoT-laitteet, kuten insuliinipumput ja uniapnealaitteet, auttavat käyttäjiä saamaan tärkeää tietoa hyvinvoinnistaan ja seuraamaan hoitotasapainoa. Tämänkaltaiset teknologiset innovaatiot tuovat mukanaan monia hyötyjä, mutta samalla herättävät kysymyksiä yksityisyydestä ja tietoturvasta. Yhä useammin esiin nousevat uutisoinnit tietovuodoista ja suositeltavista toimenpiteistä kertovat, ettei huoli ole perusteeton.

Tutkielman painopiste on tietoturvan haavoittuvuuksissa, joita tarkastellaan laitteiden kerrosarkkitehtuuria erittelemällä ja asiaankuuluvan lainsäädännön näkökulmasta. Tutkielmassa tarkastellaan seuraavia tutkimuskysymyksiä:

TK 1: Millaisia teknisiä ja tietoturvaan liittyviä haasteita liittyy IoT-laitteiden datan jakamiseen ja hallintaan?

TK 2: Millä tavoin IoT-laitteiden tietosuojakäytännöt noudattavat nykyisiä lainsäädännöllisiä vaatimuksia yksityisyyden suojaamisessa?

TK 3: Mitkä ovat keskeiset puutteet ja kehitystarpeet IoT-laitteiden tietosuojakäytännöissä ja lainsäädännössä?

Tutkielma toteutetaan kirjallisuuskatsauksena. Lähteinä on käytetty ensisijaisesti tieteellisiä ja akateemisia artikkeleita, mutta mukana on myös lainsäädäntöön ja

sen tulkintaan liittyviä asiantuntijalähteitä. Näihin kuuluu esimerkiksi Euroopan komission verkkosivustoja ja lakialan asiantuntijoiden julkaisemia selventäviä tekstejä. Haussa hyödynnettiin IEEE Xplore, Volter ja Google Scholar -tietokantoja, mutta lisäksi osa lähteistä löytyi käytettyjen artikkeleiden lähdeluetteloja tutkimalla. Hakusanoja olivat muun muassa "IoT and data breach", "IoT vulnerabilities", "compliance", "accountability"ja "cyber security".

Johdantoluvun jälkeen tutkielma jakautuu neljään päälukuun. Toisessa luvussa tarkastellaan IoT-arkkitehtuurin rakennetta ja sen eri kerroksille sijoittuvia haavoittuvuuksia. Kolmannessa luvussa siirrytään tietosuojaa koskevan sääntelyn merkitykseen ja käsitellään kolme keskeisintä eurooppalaista tietosuojasäädöstä. Neljännessä luvussa yhdistetään aiemmin käsiteltyjä näkökulmia ja pohditaan, millaisia kehitystarpeita ja tulevaisuuden suuntauksia IoT-laitteiden tietosuojan parantamisessa on nähtävissä. Tutkielman lopuksi esitetään yhteenveto, jossa kerrataan tutkimuskysymykset sekä keskeiset havainnot, jotka on työssä tuotu esiin.

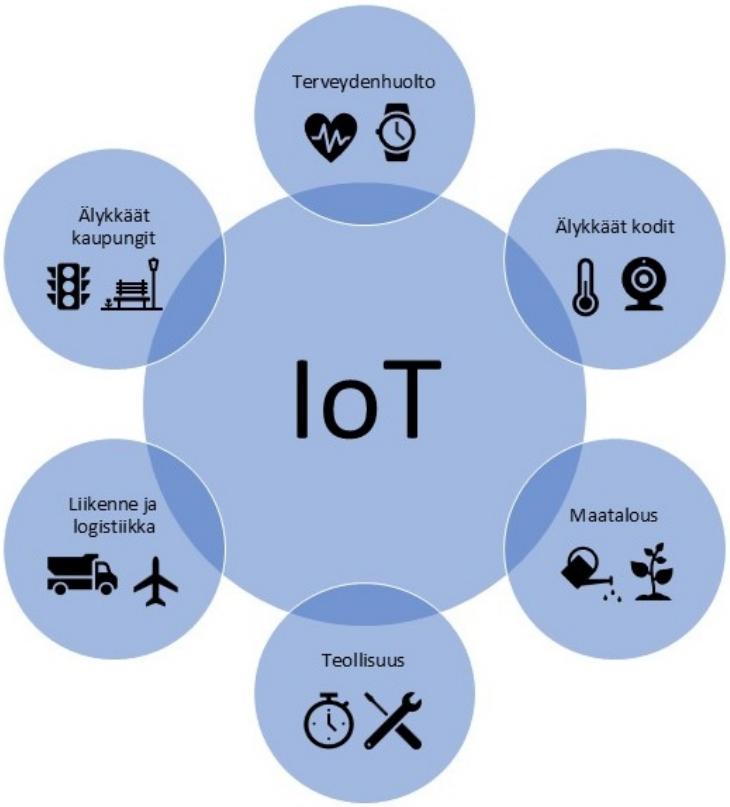
2 IoT-laitteiden tuottaman tiedon jakaminen ja tietoturvahaasteet

Eri käyttökohteet, kuten älykaupungit, älyteollisuus ja älykodit, asettavat IoT- laitteiden tietojen hallinnalle ja jakamiselle vaihtelevia teknisiä ja tietoturvallisia haasteita. Yhteisiä teemoja ovat datan reaaliaikaisuuden vaatimukset, sensorien luotettavuus ja tiedon eheys, mutta jokaisella sovellusalueella on myös ainutlaatuisia haasteita. Nämä on huomioitava ratkaisuja suunniteltaessa, jotta mahdolliset haavoittuvuudet saadaan minimoitua ja tietovuodot estettyä. [1]

IoT-laitteiden sovellusalueet vaihtelevat laajasti käyttökohteen mukaan, ja teknologian rooli muovautuu tarpeiden ja ympäristön mukaan. Esimerkiksi terveydenhuollossa IoT mahdollistaa etäluettavan terveyden seurannan älykellojen ja muiden sensorien avulla, mikä tukee ennakoivaa hoitoa ja potilasturvallisuutta. Älykkäissä kodeissa IoT-järjestelmät mahdollistavat lämpötilan automaattisen säädön sekä kodin turvallisuuden parantamisen valvontakameroilla ja vauvamonitoreilla. Maataloudessa sovellukset ulottuvat esimerkiksi automaattisiin kastelujärjestelmiin ja kasvuolosuhteiden seurantaan, mikä tehostaa veden käyttöä ja parantaa tuottavuutta. [1]

Teollisuudessa IoT auttaa ajankäytön hallinnassa ja koneiden huoltotarpeiden ennakoivassa tunnistamisessa, kun taas liikenteessä ja logistiikassa sen avulla voidaan optimoida reittisuunnittelua ja seurata kuljetuksia reaaliajassa. Älykkäissä

kaupungeissa puolestaan liikenne- ja katuvaloja ohjataan todellisen tarpeen mukaan, mikä lisää energiatehokkuutta ja parantaa liikenteen sujuvuutta. Kuvassa 2.1 on esitetty kuusi keskeistä IoT:n käyttökohdetta, joiden jaottelulla pyritään selventämään, miten erilaiset tarpeet ohjaavat IoT-teknologian kehitystä. [1]



Kuva 2.1: IoT-laitteiden jaottelu

IoT-laitteilla on niille ominaisia teknisiä rajoitteita, mutta nämä eivät ole yksin syy tietomurtoihin johtavien haavoittuvuuksien löytymiseen [2]. Yrityksiin kohdistuu painetta tuoda markkinoille uusia innovatiivisia tuotteita nopeasti. Tämä paine, yhdessä voittojen maksimoinnin ja asiaan liittyvän lainsäädännön puutteiden kanssa, on paikoin johtanut siihen, että valmistajat eivät ole täyttäneet vastuitaan laitteiden tietoturvan takaamiseksi [2]. Tunnettu esimerkki tästä on Mirai-haittaohjelma, joka hyödynsi suojaamattomia IoT-laitteita yhden kaikkien aikojen suurimman hajaute-

tun palvelunestohyökkäyksen toteuttamiseen. Kaapatut laitteet muodostivat laajan bottiverkon, joka ruuhkatti internetin DNS-nimipalvelimia suurella määrällä yhtäaikaisia palvelupyyntöjä, estäen näin käyttäjien pääsyn moniin verkkopalveluihin [3].

Yksi tunnetuimmista ongelmista on, että moniin IoT-laitteisiin pääsee käsiksi oletuskäyttäjätunnuksilla, joita ei ole suojattu tai vaihdettu riittävästi. Juuri tätä heikkoutta hyödynsi myös edellä mainittu Mirai-haittaohjelma. Tällaiset haavoittuvuudet ovat jääneet huomiotta suunnitteluvaiheessa, ja vastuu tietoturvasta on usein siirtynyt loppukäyttäjälle. Lisäksi käyttäjiltä edellytetään usein esimerkiksi ohjelmistopäivitysten suorittamista manuaalisesti, mikä ei aina toteudu käytännössä. Tässä yhteydessä korostuu käyttäjien tietoturvatietoisuuden ja päivityskäytäntöjen merkitys. [2]

Canonical Ltd:n suorittaman kyselyn [4] mukaan 48 % kuluttajista ei ollut tietoisia siitä, että kotoa löytyvät älylaitteet voivat olla mahdollisia kyberhyökkäysten kohteita ja 40 % ei päivitä laitteitaan tietoisesti. On kuitenkin huomattava, että kyselyn tulokset heijastavat tilannetta vuodelta 2017. Älyteknologian kehitys on nopeaa ja valistuneisuus lisääntyy, joten tänä päivänä osuus saattaa erota edellä mainituista luvuista. Kehityksen taustalla olevien teknisten ratkaisujen ymmärtäminen edellyttää perehtymistä IoT-järjestelmien arkkitehtuuriin ja siihen, minkälaisen kokonaisuuden arkkitehtuurin eri tasot muodostavat.

2.1 IoT-arkkitehtuuri

IoT-arkkitehtuurin jaottelu vaihtelee lähteestä riippuen kolme-, neljä- tai viisikerroksiseen järjestelmään perustuen kerrosten ominaisuuksiin ja suunnitteluvaatimuksiin [5]. Yleisesti käytössä on kuvassa 2.2 esitetty nelikerroksinen malli, johon kuuluu sovelluskerros (Application Layer), väliohjelmistokerros (Middleware Layer), verkkokerros (Networking Layer) ja havaintokerros (Perception Layer) [6].

Kuva 2.2: Nelikerroksinen IoT-arkkitehtuuri

Arkkitehtuurimalli helpottaa tietoturvakysymysten erottelua ja analyysiä, koska kerrosten toiminta, tiedonkäsittely ja sitä myötä haasteet ovat erilaiset. Ennen tietoturvaa koskevien haasteiden tarkempaa luokittelua selvennetään, mitä eri kerroksilla tapahtuu ja millaisia edellytyksiä niiden toiminnalla on.

Alimmalla tasolla IoT-laitteen perustana toimii havaintokerros, joka yhdistää fyysisen ja digitaalisen ympäristön. Tämä kerros vastaa fyysisten objektien tunnistettavuudesta, havaittavuudesta ja hallittavuudesta. Anturit keräävät aktiivisesti tietoa ympäristöstä, ja toimilaitteet eli aktuaattorit mahdollistavat ympäristöön vaikuttamisen ohjatuilla liikkeillä, kuten venttiilin avaamisella tai valojen sytyttämisellä. Fyysisten esineiden yksilöinnissä voidaan käyttää mm. RFID-tunnisteita (Radio Frequency Identification) eli radiotaajuiseen etätunnistukseen perustuvia merkintöjä. [7]

Yhdyskäytävä (Gateway) tai reunapalvelin (Edge Server) toimii havaintokerroksen ja verkkokerroksen välissä, ja sen kautta kulkee kaikki laitteiden keräämä data

ennen välitystä edelleen verkkoon tai pilvipalveluihin. Yhdyskäytävä voidaan sijoittaa käyttäjän hallitsemaan ns. henkilökohtaiseen vaikutuspiiriin, jolloin se tarjoaa mahdollisuuden toteuttaa tietosuojaa tukevia toimenpiteitä, kuten datan minimointia, salausta tai anonymisointia. [6]

Verkkokerros toimii keskeisenä yhdistävänä tekijänä havainto- ja väliohjelmistokerrosten välillä, koska se mahdollistaa kerätyn datan ja ohjauskäskyjen saumattoman siirron. Toisin kuin perinteisessä internetin arkkitehtuurissa, IoT-verkkokerros koostuu lukuisista keskenään erilaisista ja virtarajoitteisista laitteista sekä sovelluskohtaisista vaatimuksista [5]. Koska IoT-verkkokerros sisältää laitteita, joilla on rajalliset resurssit ja vaihtelevat sovellusvaatimukset, sen viestintätekniikoiden on tuettava matalaa energiankulutusta, vähäistä viivettä, korkeaa kapasiteettia ja suurta tiedonsiirtonopeutta. Yleisiä IoT-verkoissa käytettyjä tiedonsiirtoteknologioita ovat esimerkiksi Bluetooth, WLAN eli langaton lähiverkko, Ethernet ja 5G-mobiiliverkot [6].

Palvelin sijoittuu arkkitehtuurissa verkkokerroksen ja väliohjelmistokerroksen rajalle komponenttina, joka vastaanottaa verkon kautta siirrettyä dataa ja välittää sen edelleen käsiteltäväksi väliohjelmistokerrokseen. Palvelin voi toimia alustana erilaisille väliohjelmistotoiminnoille, kuten datan koostamiselle, tallennukselle ja autentikoinnille. [6]

Väliohjelmistokerros toimii kuvainnollisesti laitteen aivoina, sillä se käsittelee, järjestää ja yhdistää alempien kerrosten vastaanottaman tiedon monimutkaisemmiksi kokonaisuuksiksi. Väliohjelmisto mahdollistaa eri laitteiden ominaisuuksien yhtenäisen kuvaamisen ja nimeämisen esimerkiksi esimerkiksi Extensible Markup Language (XML) -pohjaisten kuvauskielten avulla. Tämä parantaa laitteiden ja järjestelmien välistä yhteentoimivuutta. Lisäksi kerros vastaa tiedon tallentamisesta pilvipalveluihin tai tietokantoihin sekä sen jatkokäsittelystä. [6]

IoT-arkkitehtuurin ylimmällä tasolla oleva sovelluskerros sisältää kaikki IoT-

sovellukset, jotka hyödyntävät järjestelmän keräämää dataa ja toiminnallisuuksia. Sovellukset voivat olla hyvin erilaisia käyttökohteestaan riippuen, ja esimerkiksi yksityisyyden suoja voi muodostua suureksi haasteeksi, jos sovellus käsittelee käyttäjien henkilökohtaisia tietoja. [6]

2.2 Tietoturvariskien sijainti IoT-arkkitehtuurissa

IoT-järjestelmän ja käyttäjän välisestä vuorovaikutuksesta on tunnistettavissa tiedonkäsittelyn vaiheita, jotka kattavat koko tiedonsiirron elinkaaren alkaen vuorovaikutuksesta ja tiedon keräämisestä jatkaen prosessointiin, jakamiseen ja toteutukseen. Jokaisessa näistä vaiheista data altistuu erilaisille tietoturvauhille, erityisesti kun kyse on yksityisyyden suojasta ja henkilötietojen tunnistettavuudesta. IoT-teknologian monimutkaisuus ja valtava datan määrä tekevät yksityisyyden hallinnasta haastavaa, koska erot henkilötietojen ja ei-henkilötietojen välillä hämärtyvät. [8]

IoT-arkkitehtuurin kerroksia ja datan elinkaaren vaiheita voidaan tarkastella tietoturvan näkökulmasta kerroskohtaisesti. Tiedon elinkaaren eri vaiheisiin liittyvien riskien näkökulmasta erityisesti sovelluskerros on merkittävä, sillä se kokoaa yhteen käyttäjän näkymän järjestelmään ja käsittelee usein henkilökohtaista tietoa. Monet uhat liittyvät todennukseen, ohjelmointikäytäntöihin ja tietoliikenteen suojaamiseen. Väliohjelmistokerroksessa korostuvat järjestelmän hallintaan ja päivityksiin liittyvät haasteet, kun taas verkkokerroksessa esiintyy puutteita viestinnän turvallisuudessa ja pääsynhallinnassa. Havaintokerroksessa, joka käsittää erilaisia laitteita ja antureita, painottuvat fyysiseen turvallisuuteen ja toimintakykyyn liittyvät riskit. Taulukko 2.1 kokoaa yleisimpiä tunnettuja haavoittuvuuksia ja auttaa hahmottamaan niiden sijoittumista arkkitehtuurin eri tasoille.

Taulukko 2.1: Tunnetut IoT-laitteiden haavoittuvuudet kerroksittain

Haavoittuvuus	**Kerroksen taso**	**Kuvaus**
Puutteellinen todennus	Sovelluskerros	Heikot tai puuttuvat autentikointimekanismit mahdollistavat tunkeutumisen ja datan manipuloinnin.
Virheellinen salaus	Sovellus- ja verkkokerros	Heikot salausalgoritmit tai tiedonsiirron salaamattomuus voivat vaarantaa datan ja verkkoliikenteen luottamuksellisuuden.
Heikot ohjelmointikäytännöt	Sovellus-, väliohjelmisto- ja havaintokerros	Takaportit, suojaamattomat käyttöliittymät ja virheellinen koodaus voivat altistaa hyökkäyksille ja virhetoiminnalle.
Riittämättömät auditointimekanismit	Sovellus- ja verkkokerros	Puutteellinen lokitus ja auditointi vaikeuttavat hyökkäysten jäljittämistä ja analysointia.
Puutteellinen päivitysten hallinta	Väliohjelmistokerros	Päivitysprosessien puutteellisuus altistaa laitteet tunnetuille haavoittuvuuksille.
Riittämätön pääsynhallinta	Väliohjelmisto- ja verkkokerros	Pääsynhallinnan puutteet mahdollistavat laitteiden väärinkäytön tai luvattoman etäohjauksen.
Tarpeettomat palveluportit	Verkkokerros	Avoimet portit tarjoavat hyökkäyspisteitä tunkeutumisille ja tietomurroille.
Puutteellinen fyysinen suojaus	Havaintokerros	Fyysisen suojauksen puute mahdollistaa laitteiden sabotaasin tai luvattoman käsittelyn.
Riittämätön tehonhallinta	Havaintokerros	Energiankulutuksen hallinnan puutteet voivat johtaa palvelunestohyökkäyksiin (DoS).

3 Tietosuojakäytännöt ja lainsäädäntö

3.1 Tietosuojan toteutus IoT-laitteissa

Esineiden internet on käynnistänyt uuden aikakauden, jossa laitteet tuottavat valtavia määriä dataa. Yksinkertaisista sensoreista kehittyneisiin henkilökohtaisiin terveysmittareihin ulottuva IoT-ekosysteemi kasvaa nopeasti, ja suurten datamäärien käsittelyllä voi olla mullistava vaikutus monilla aloilla. Samalla laitteiden nopea yleistyminen tuo mukanaan haasteita yksityisyyden suojan, tietoturvan ja sääntelyn näkökulmasta [9]. Näihin haasteisiin on pyritty vastaamaan kansainvälisin ohjeistuksin, kuten esimerkiksi EU:n GDPR-asetuksella, NIS2-direktiivillä sekä tulevalla CRA-säädöksellä, joita käsitellään tarkemmin luvussa 3.2.

Koska IoT-laitteiden käyttöympäristöt ovat hyvin monimuotoisia, yhdenmukaisen ja johdonmukaisen sääntelyn soveltaminen on haastavaa. IoT-laitteet kommunikoivat pääasiassa kahdella tavalla: joko suoraan internetin kautta tai rajattujen langattomien yhteyksien, kuten Bluetoothin, avulla. Kun laitteella on suora internetyhteys, se tallentaa ja lähettää dataa pilvipohjaiseen sovellukseen. Tämä parantaa tiedon saavutettavuutta, mutta lisää samalla laitteen alttiutta hyökkäyksille. Sen sijaan laitteet, jotka toimivat vain toistensa läheisyydessä, eivät ole suoraan yhteydessä internetiin, jolloin tietomurto edellyttää joko pääsyä yhdyskäytävään tai hyök-

kääjän fyysistä läsnäoloa. Yksi keskeinen IoT-laitteisiin liittyvä haaste on tiedonhallinnan ja vastuunjaon epäselvyys. Data kulkee usein monivaiheisen polun kautta pilveen ja mahdollisesti edelleen kolmansille osapuolille, jolloin käyttäjän mahdollisuudet vaikuttaa yksityisyydensuojan säilymiseen ovat hyvin rajalliset. Käyttäjätasolla keskeistä on riskien ja uhkien tiedostaminen. Tietoisuuden lisääminen auttaa vähentämään tarpeettoman tiedon jakamista, ylläpitämään riittävää suojaustasoa sekä edistää ohjelmistopäivitysten säännöllistä asennusta. Kun vastuu tietoturvasta jakautuu useiden toimijoiden kesken ja tekniset keinot eivät yksin riitä, sääntely muodostuu keskeiseksi työkaluksi yksityisyyden turvaamisessa. [10]

3.2 Lainsäädäntö ja tietosuojavaatimukset

EU-alueella IoT-järjestelmiä koskee kolme keskeistä säädöstä: Euroopan unionin yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR), NIS2-direktiivi (Network and Information Security Directive 2) ja Kyberresilienssisäädös (Cyber Resilience Act, CRA). Nämä säädökset muodostavan lainsäädännöllisen perustan, jonka tavoitteena on suojata sekä käyttäjien tietosuojaa että järjestelmien turvallisuutta. Taulukko 3.1 havainnollistaa, kuinka GDPR, NIS2 ja CRA täydentävät toisiaan tietoturvan ja tietosuojan sääntelyssä.

Taulukko 3.1: GDPR:n, NIS2:n ja CRA:n vertailu

	GDPR	**NIS2**	**CRA**
Tavoite	Henkilötietojen ja yksityisyyden suojaus EU:n alueella	Kyberturvallisuuden parantaminen kriittisillä ja keskeisillä toimialoilla	Kyberturvallisuus digituotteille ja -palveluille
Kohdeorganisaatiot	Kaikki henkilötietoja käsittelevät EU:n sisällä toimivat organisaatiot	Keskeiset ja tärkeät toimijat, esim. energia, pankki, kuljetus	Digitaalisten tuotteiden valmistajat, jakelijat ja maahantuojat
Rikkeiden seuraamukset	Vakavuuden mukaan 2–4% edellisen tilivuoden liikevaihdosta tai 10–20 miljoonaa euroa	Toimijasta riippuen 2% / 10 miljoonaa euroa tai 1,4% / 7 miljoonaa euroa	Jopa 2,5% edellisen tilivuoden liikevaihdosta tai 15 miljoonaa euroa
Raportointivelvoite	72h sisällä tietoturvaloukkauksesta	Esiraportti 24h sisällä, laaja raportti 72h	Ilmoitus ENISA:lle 24h sisällä haavoittuvuuden havaitsemisesta
Valvontaviranomainen	Tietosuojaviranomaiset EU:ssa	Kansalliset viranomaiset, koordinointi ENISA:n kautta	Komissio ja jäsenvaltioiden markkinavalvontaviranomaiset
Voimaantulo	2018	Loppuvuodesta 2024 alkaen	Joulukuu 2027 alkaen

3.2.1 Yleinen tietosuoja-asetus

GDPR on koko EU-alueella sovellettava säädös, jonka tavoitteena on vahvistaa yksilöiden oikeuksia henkilötietojen käsittelyssä ja yhtenäistää tietoturvasääntelyä eri jäsenvaltioiden välillä [11]. GDPR:n piiriin kuuluvan tiedon ei tarvitse olla suoraan tunnistettavaa, vaan siihen lukeutuu myös epäsuora tunnistaminen tai uudelleenidentifiointimahdollisuus [12]. IoT-laitteet voivat kerätä esimerkiksi lämpötila-, käyttöaika-, ympäristööääni- tai aktiivisuustietoja, joita voidaan yhdistää keskenään tai liittää muihin datalähteisiin, kuten verkko-osoitteisiin, sijaintitietoihin tai lait-

teen yksilöllisiin tunnisteisiin. Tällaisista yhdistelmistä voi muodostua kokonaisuus, joka paljastaa yksilön käyttäytymistä ja mahdollistaa hänen suoran tai epäsuoran tunnistamisensa [10].

Ennen yleisen tietosuoja-asetuksen voimaantuloa EU:n henkilötietojen suojaa ohjasi direktiivi 95/46/EY [13]. Sen tarkoituksena oli luoda tasapaino korkeatasoisen yksityisyydensuojan ja jäsenvaltioiden välisen henkilötietojen vapaan liikkuvuuden välillä, sillä tietokoneet ja sähköinen tiedonkäsittely yleistyivät nopeasti ja EU:n sisämarkkinat olivat kehittymässä. Koska direktiivi on säädösmuodoltaan velvoittava, mutta ei sellaisenaan suoraan sovellettava, jokainen EU-maa noudatti omaa harkintaansa ottaessaan sen osaksi lainsäädäntöään. Tämä johti eroihin sekä sääntelyn sisällössä että siinä, millaisia seuraamuksia rikkomuksista määrättiin. Tulkinnanvaraisuus ja johdonmukaisuuden puute aiheuttivat ongelmia erityisesti monikansallisille organisaatioille [14]. Vuoden 1995 tietosuojadirektiiviä täydennettiin ja tuettiin muilla säädöksillä, mutta merkittäviä muutoksia ei tehty ennen kuin yleinen tietosuoja-asetus korvasi sen kokonaan.

Yleinen tietosuoja-asetus astui voimaan vuonna 2018, mutta vielä vuonna 2020 International Association of Privacy Professionals toi ilmi vuotuisessa tietosuojanhallinnan raportissaan, että vain 47 % eurooppalaisista yhtiöistä täyttää asetuksen mukaiset vaatimukset hyvällä tasolla [15]. IoT-laitteet toimivat usein jatkuvan tiedonkeruun periaatteella, mikä voi johtaa yksityiskohtaisten henkilötietojen tallentumiseen. Tietojen kerääminen tapahtuu usein ilman, että käyttäjä on täysin tietoinen siitä, mitä tietoja kerätään, mihin tarkoitukseen niitä käytetään tai kenelle niitä mahdollisesti luovutetaan, mikä rikkoo läpinäkyvyyden ja tiedottamisvelvoitteen periaatteita [12].

Käyttäjän voi olla vaikeaa tarkastella, muokata tai poistaa omia tietojaan, sillä IoT-ympäristöissä data on tyypillisesti hajautettu useisiin eri paikkoihin: laitteen lokaali tiedonkeräys, välityssiltana toimivat sovellukset, pilvipalvelimet ja kolman-

net osapuolet. Tietoturvan kannalta riskejä lisää myös laitteiden koosta johtuvat rajoitukset sekä päivitysten vähäisyys. Yleinen tietosuoja-asetus määrittelee periaatteen *privacy by design*, jonka mukaan tietosuoja tulee huomioida jo järjestelmien suunnitteluvaiheessa. Tämä ei kuitenkaan IoT-laitteiden kohdalla aina toteudu, sillä suunnittelussa painottuvat usein käytettävyys ja teknologiset ratkaisut tietosuojan kustannuksella. [12]

3.2.2 NIS2-direktiivi

Joulukuussa 2022 hyväksytty NIS2-direktiivi on osa Euroopan unionin pyrkimystä vahvistaa verkko- ja tietojärjestelmien turvallisuutta. Direktiivi astui virallisesti voimaan tammikuussa 2023. NIS2 korvasi vuoden 2016 NIS-direktiivin ja laajensi sen soveltamisalaa merkittävästi vastauksena EU:n yhä monimuotoistuvampaan kyberuhkaympäristöön. [16]

Toimijat jaetaan kahteen ryhmään riskiperusteisesti ja yhteiskunnallisten vaikutusten mukaan. Keskeiset toimijat ovat julkisia tai yksityisiä tahoja, joiden häiriöt voisivat vakavasti vaarantaa yhteiskunnan toiminnan, kuten pankit, kuljetus-, energia- ja vesihuoltoalat. Merkittävät toimijat puolestaan tarjoavat merkityksellisiä palveluita, jotka eivät ole yhtä kriittisiä perustoimintojen kannalta. Näihin kuuluvat esimerkiksi jätehuolto, tuotanto, postipalvelut ja digitaaliset palvelut. Direktiivi laajennettiin koskemaan myös tiettyjä pieniä ja keskisuuria yrityksiä ja digitaalisia palveluntarjoajia, jotka ylläpitävät mm. pilvipalveluita, hakukoneita ja verkkokauppaalustoja. [17]

NIS2 keskittyy ensisijaisesti kyberturvallisuuteen, mutta auttaa täydentämään tietosuojaa turvaavaa yleisestä tietosuoja-asetusta. Direktiivillä varmistetaan toimijoiden vertailukelpoisten kyberturvallisuusstandardien ja -käytäntöjen noudattaminen, joita ovat esimerkiksi säännölliset riskinarvioinnit, pääsynhallinta, salausmenetelmät, häiriötilanteisiin varautuminen, selkeät vastuurakenteet organisaatiossa ja

liiketoiminnan jatkuvuussuunnittelu. [18]

Toisin kuin vuoden 1995 tietosuojadirektiivissä, NIS2-direktiivin noudattamatta jättämisestä seuraa ankaria seuraamuksia, jotka ovat verrattavissa yleisen tietosuoja-asetuksen mukaisiin sanktioihin. Huomattavien sakkojen tavoitteena on varmistaa, että toimijat asettavat kyberturvallisuuden ja säädettyjen standardien noudattamisen ensisijaiseksi, ja samalla jäsenvaltiot ovat itse vastuussa direktiivin vaatimukset täyttävän kansallisen lainsäädännön säätämisestä [16]. Kansallinen toimeenpano on kuitenkin edelleen epätasaista: osa jäsenvaltioista ei ole vielä aloittanut soveltamista lainkaan, toiset valmistelevat vasta lakiluonnoksia, ja joissakin maissa direktiivi on jo sisällytetty kansalliseen lainsäädäntöön. Siirtymäaikaa toimeenpanolle annettiin 18.10.2024 saakka, mutta viivästyminen ei ole EU:n sääntelyhistoriassa poikkeuksellista. Taulukossa 3.2 esitellään, miten NIS2-direktiivi ja yleinen tietosuoja-asetus liittyvät toisiinsa ja kuinka NIS2 voi tukea henkilötietosuojan periaatteiden toteutumista.

Taulukko 3.2: NIS2-direktiivin ja GDPR-asetuksen yhteneväisyydet

NIS2-vaatimus	**GDPR-ulottuvuus**	**NIS2-vaatimus**	**GDPR-ulottuvuus**
1. Riskianalyysit ja järjestelmien turvallisuus	Pääsynhallinta-, loukkausten hallinta ja riskienhallintapolitiikat	7. Kyberhygieniakäytännöt ja koulutus	Tietosuoja-koulutukset henkilötietoja käsitteleville toimihenkilöille
2. Poikkeamien käsittely	Henkilötietojen tietoturvaloukkaus	8. Salaus ja kryptografia	Henkilötietojen turvallinen käsittely ja säilytys
3. Jatkuvuuden hallinta		9. Henkilöstöturvallisuus ja pääsynhallinta	Toimittajien kelpoisuusarvioinnit, käyttöoikeudet, lokitus, omaisuudenhallinta
4. Toimitusketjun turvallisuus	Tilaaja-toimittaja -väliset vaatimukset: kelpoisuus, DPA-sopimus ja ohjeistus	10. MFA- ja muut todennukset	Käyttöoikeuksien ja identiteettien hallinta, pääsynvalvontapolitiikat
5. Verkko- ja tietojärjestelmät	Tietoturva- ja tietosuojakoulutus ohjelmistojen kehittäjille	11. Raportointivelvoite	Ilmoitukset poikkeamista viranomaisille
6. Riskienhallintatoimenpiteiden tehokkuus	Sääntelyn noudattamisen säännöllinen arviointi, kuten käsiteltävien henkilötietojen tarpeellisuuden arviointi	12. Hallinnolliset sakot ja johdon rikosoikeudellinen vastuu	Hoitamattomista velvoitteista voi kummassakin kehyksessä tulla seuraamismaksuja

3.2.3 Kyberresilienssisäädös

Kyberresilienssisäädös on yksi Euroopan uusimmista voimaan astuvista säädöksistä, ja sen soveltamisen on määrä alkaa 11. joulukuuta 2027. CRA pyrkii parantamaan digitaalisia komponentteja sisältävien tuotteiden kyberturvallisuutta edellyttämällä valmistajia ja vähittäismyyjiä varmistamaan tuotteidensa turvallisuus koko niiden elinkaaren ajan. [19]

Tuotteiden suunnittelun, kehittämisen ja valmistamisen tulee tukea hyökkäysten estämistä sekä lieventää hyväksikäytön vaikutuksia soveltuvin mekanismein ja tekniikoin [16]. Myytävissä tuotteissa ei saa olla tunnettuja haavoittuvuuksia, ja valmistajien on varmistettava tuotteiden tietoturva myös jatkossa tietoturvapäivityksin. Tuotteet on lisäksi voitava palauttaa turvalliseen oletustilaan, eli tehdasasetuksil-

le. CRA helpottaa kuluttajia tunnistamaan kyberturvallisuusvaatimukset täyttävät laitteisto- ja ohjelmistotuotteet, sillä vaatimukset sidotaan jatkossa CE-merkintään [19]. Asetus koskee kaikkia tuotteita, jotka on liitetty suoraan tai välillisesti toiseen laitteeseen, joten sillä on merkittävä vaikutus IoT-ympäristössä.

Kaikki IoT-laitteet eivät kuitenkaan ole keskenään samanarvoisia. Digitaalisia elementtejä sisältävät tuotteet jaotellaan neljään luokkaan, joita säännellään eritasoisten vaatimusten mukaan. Vakiotuotteet käsittävät alhaisen turvallisuusriskin tuotteita, kuten älytelevisioita. Tärkeät tuotteet jaetaan kahteen tasoon, joista ensimmäinen koskee esimerkiksi reitittimiä, käyttöjärjestelmiä ja älylukkoja, kun taas toinen luokka kattaa muun muassa palomuurit. Neljännen luokan muodostavat kriittiset tuotteet, kuten älymittarien yhdyskäytävät tai kryptografisiin suojaustoimintoihin erikoistuneet laitteet, jotka vaativat korkeaa suojaustasoa. Ei olisi tarkoituksenmukaista edellyttää älytelevisioilta yhtä korkeaa tietoturvatasoa kuin esimerkiksi tuotteilta, jotka käsittelevät salausavaimia. [20]

CRA edellyttää esimerkiksi valmistajia laatimaan komponenttiluettelon, joka sisältää kattavat tiedot käytetyistä komponenteista, ohjelmistokirjastoista ja kolmannen osapuolen osista. Lisäksi vaatimustenmukaisuus on osoitettava joko itsearvioinnilla tai riippumattoman tahon varmennuksella, ja kansalliset viranomaiset valvovat säädöksen toteutumista. Sääntelyn rikkomisesta voi tulla merkittäviä seuraamuksia, jotka ovat suuruudeltaan verrattavissa GDPR:n ja NIS2-direktiivin sanktioihin. [16]

4 IoT-teknologian tietoturvan kehityssuunnat ja tulevaisuus

Läpinäkyvyys on keskeinen oikeudellinen ulottuvuus vastuullisuudessa teknisten järjestelmien osalta. IoT-ympäristöissä vastuu liittyy usein siihen, miten teknologia toimii ja miten sen tuottamat tiedot liikkuvat ja vaikuttavat fyysiseen maailmaan. Haittoihin johtaneissa tapauksissa teknologian tuottajalla on velvollisuus osoittaa toimineensa kohtuudella. Tämä vaatimus koskee myös tilanteita, joissa osapuolten välillä on sopimus. Oikeudellinen vastuu ei useinkaan johdu teknologian puutteista, vaan siitä, miten tietoa on käsitelty ja mitä seurauksia sillä on ollut. [21]

IoT-komponenttien hallinta jakautuu useille toimijoille, jotka sijaitsevat eri puolilla maailmaa ja toimivat omien intressiensä ja vastuidensa mukaisesti. Järjestelmille on tyypillistä dynaaminen toiminta; esimerkiksi älykello voi automaattisesti yhdistyä uuteen ympäristöön käyttäjän matkustaessa [21]. Teknologian kehittäjät tai käyttäjät eivät kuitenkaan aina kykene ennakoimaan kaikkia mahdollisia käyttötapoja, mikä tekee vastuullisuudesta monitulkintaista. Tutkijat ovat esimerkiksi kehittäneet menetelmän, joka mahdollistaa älypuhelimilla lähistöllä olevien Fitbit-älyrannekkeiden kuuntelun ja niiden yksilöivien laitetunnisteiden lähettämisen Fitbitin palvelimelle. Tämä mahdollistaa käyttäjien suostumuksettoman paikantamisen [22].

On tärkeää ymmärtää, että oikeudellinen sääntely kohdistuu ihmistoimijoihin,

ei teknologiaan itsessään [21]. Näin ollen vastuu liittyy erityisesti siihen, miten toimijat valitsevat, yhdistävät ja käyttävät IoT-komponentteja. Käyttäjät puolestaan kokevat teknologian usein "mustana laatikkona", jolloin heidän on vaikea arvioida siihen liittyviä riskejä. Esimerkkinä väärinkäytetyn teknologian hyödyntämisestä tietoturvasuojan rikkomisessa on tutkijoiden kehittämä älykelloihin kohdistuva hyökkäysmenetelmä MoLe (Motion Leaks through Smartwatch Sensors) [22]. MoLe onnistui hyödyntämään olemassa olevia liiketunnistinsensoreita tunnistaakseen käyttäjän kirjoittamia sanoja – näin rikkoen käyttäjän yksityisyyttä. Lainsäädäntö painottaa sitä, että teknologiantuottajalla tulisi olla riittävä tieto riskeistä etukäteen. Vaikka täydellistä läpinäkyvyyttä ei edellytetä, vastuu määräytyy sen mukaan, onko tuottaja ryhtynyt kohtuullisiin toimenpiteisiin riskien hallitsemiseksi [21].

IoT-teknologioiden tekninen läpinäkyvyys ei toistaiseksi ole lakisääteinen vaatimus, mutta sen säätäminen olisi merkittävä oikeudellinen uudistus. Nykytilanteessa käyttäjät voivat joutua kantamaan vastuuta teknologian väärinkäytöstä, vaikka heillä ei olisi realistista mahdollisuutta ymmärtää sen kaikkia toiminnallisuuksia. Tämä voi johtaa tilanteisiin, joissa vahingot jäävät korvaamatta. Toisaalta vastuu voi kohdistua myös tapauksiin, joissa teknologiaa käytetään selvästi suunnittelu- tai turvallisuusohjeiden vastaisesti. [21]

Vastuullisen IoT-teknologian kehittämiseen on esitetty useita lähestymistapoja. Ensimmäinen on ex ante -läpinäkyvyys, jossa teknologian toimintaperiaatteet pitäisi voida selittää käyttäjälle ennen käyttöönottoa. Tämä on kuitenkin usein epärealistista monimutkaisissa ja kehittyvissä järjestelmissä, joissa koneoppiminen ja dynaaminen käyttäytyminen rajoittavat ennakoitavuutta. Toinen vaihtoehto on ankara vastuu, jossa korvausvelvollisuus määräytyy vahingon, ei syyllisyyden perusteella. Tämä voisi soveltua erityisesti korkean riskin IoT-sovelluksiin, kuten itseajaviin ajoneuvoihin, joiden toiminta perustuu laajamittaiseen vuorovaikutukseen muiden järjestelmien kanssa. Vaikka tämä malli olisi juridisesti selkeä, pelkkä vastuujärjestelmä

ei välttämättä riitä yleisen hyväksynnän saavuttamiseksi. Käyttäjät saattavat siitä huolimatta vaatia ex ante -ymmärrystä teknologian päätöksenteosta eli tietoa kuinka lopputulokseen tultiin. Kolmas lähestymistapa on ex post -läpinäkyvyys, jossa teknologian toiminta selvitetään jälkikäteen esimerkiksi lokien tai auditointien avulla. Tämä vaatii, että järjestelmään on rakennettu teknisiä välineitä jälkiselvitystä varten. Vastuuta voitaisiin ohjata oletuksella valmistajan huolimattomuudesta, ellei tämä kykene osoittamaan toimineensa asianmukaisesti. Tämä malli voisi olla toimivin kehittyvissä ja vaikeasti ennakoitavissa ympäristöissä, joissa riskit tulevat kunnolla tunnetuksi vasta käytön myötä. [21]

Kuten aiemmin on todettu, henkilötiedon määritelmä ei ole yksiselitteinen. On olemassa erityisiin henkilötietoryhmiin kuuluva kategoria, johon sisältyy esimerkiksi terveyttä, uskontoa ja biometriikkaa koskevia tietoja. Lähes mikä tahansa tieto voi tietyssä kontekstissa täyttää henkilötiedon tunnusmerkit tai muuttua sellaiseksi, sillä soveltuva sääntely on yllättävän laaja-alainen. Mutta entä jos tilanne kehittyy toiseen suuntaan – jos tieto ei enää ole henkilökohtaista? Näin voisi teoriassa tapahtua esimerkiksi anonymisoinnin kautta. Tällöin ei ole selvää, sovelletaanko tietosuojalainsäädäntöä enää tähän kyseiseen tietoon. [21]

Sääntelyn kaksijakoisuus aiheuttaa ongelmia erityisesti IoT-järjestelmien kaltaisissa ympäristöissä, joissa tiedonkäsittely on jatkuvaa, monimutkaista ja usein hajautunutta. GDPR sisältää artiklan, joka takaa yksilölle oikeuden tulla unohdetuksi. Tällaisen oikeuden toteuttaminen voi kuitenkin osoittautua käytännössä mahdottomaksi massiivisissa ja hajautetuissa IoT-järjestelmissä, joissa tiedon sijainti ja omistajuus voivat olla epäselviä tai jakautua useille toimijoille. Täydellinen vaatimustenmukaisuus on todennäköisesti mahdotonta, mutta tietosuojalainsäädännön yhä vahvempi painotus vastuullisuuteen voi kannustaa kehittämään yksityisyydensuojaa tukevia ratkaisuja ja ohjata IoT-teknologioiden suuntaa kohti paremmin yksityisyyttä huomioivia käytäntöjä. Vastuuta ei tule pitää vain sanktiomekanismina,

vaan myös keinona ohjata teknologian kehittymistä kohti turvallisempaa ja läpinäkyvämpää suuntaa. [21]

5 Yhteenveto

Tässä tutkielmassa tarkasteltiin IoT-järjestelmien tietoturvan toteutumista laitteiden arkkitehtuuria ja asiaankuuluvaa lainsäädäntöä tutkien. Työn ensimmäinen tutkimuskysymys käsitteli IoT-järjestelmien datan hallinnan ja jakamisen haasteita teknisestä ja tietoturvanäkökulmasta. Kappaleessa kaksi havaittiin, että laitetasolla jatkuvasti tietoa keräävät sensorit ja komponentit vaikeuttavat kokonaiskuvan hallintaa, ja samalla laitteiden tekniset rajoitteet ovat haitanneet kehittyneiden suojaustoimien toteuttamista. IoT-arkkitehtuurin tarkastelu toi esiin keskeisiä riskitekijöitä, kuten puutteellisen salauksen, heikot todennuskäytännöt, riittämättömät ohjelmistopäivitykset ja haavoittuvat yhteydet. Lisäksi IoT-verkkojen hajautettu rakenne lisää hyökkäyksille alttiita pisteitä, sillä tieto kulkee useiden eri komponenttien ja verkkojen kautta. Nämä tekijät yhdessä muodostavat merkittävän haasteen riskienhallinnalle ja käyttäjien tietosuojalle.

Työn toinen tutkimuskysymys selvitti sitä, millä tavoin IoT-laitteiden toteutettu tietosuoja vastaa nykyistä lainsäädäntöä. Koska kansainvälistä lainsäädäntöä on paljon, rajoitettiin tarkastelu kappaleessa kolme Euroopan kannalta merkittävimpiin asetuksiin. Vaatimukset yksityisyyden suojaamiseksi ovat vahvistuneet yleisen tietosuoja-asetuksen, NIS2-direktiivin ja tulevan CRA-asetuksen myötä, mutta laitteiden toteutuneissa tietosuojakäytännöissä esiintyy edelleen merkittäviä puutteita. Vaikka GDPR takaa yksilöille oikeuksia, kuten oikeuden tulla unohdetuksi ja hallita omia tietojaan, monet IoT-sovellukset eivät kykene täyttämään näitä vaatimuksia

teknisten rajoitteiden vuoksi. Tiedonkeruu ja jakaminen ei ole käyttäjälle läpinäkyvää, eikä tiedonkäsittelyn tarkoituksen perusteita selitetä riittävästi. Teknologian hajautuneisuus ja monimuotoisuus tekevät sääntelyn soveltamisesta haastavaa, vaikka kiristyvät vaatimukset ja seuraamukset ohjaavatkin kehitystä kohti yksityisyyttä paremmin huomioivia ratkaisuja.

Tutkielmalle asetettu kolmas tutkimuskysymys käsitteli IoT-laitteiden tietosuojakäytäntöjen ja lainsäädännön keskeisiä puutteita ja kehitystarpeita, joita esiteltiin kappaleessa neljä. Lainsäädäntö ei ole vielä onnistuneesti ratkaissut keskeisiä ongelmia, jotka liittyvät läpinäkyvyyden puutteeseen, vastuunjaon epäselvyyteen ja teknisen tietoturvan heikkouksiin. Yksityisyydensuojasta tulisi huolehtia laitteen suunnittelusta lähtien, mutta lähitulevaisuudessa käyttöönotettavan CRA-asetuksen odotetaan tuovan tähän positiivista muutosta. Tulevaisuuden tietosuojakäytäntöjen keskeisistä kehitystarpeista tuotiin esille erityisesti sääntelyn selkeyttäminen sekä vastuun ja datan omistajuuden tarkempi määrittely. Näiden edistäminen on ratkaisevaa yksityisyyden suojan vahvistamiseksi osana kehittyviä IoT-ratkaisuja.

Lähdeluettelo

[1] J. Byabazaire, G. O'Hare ja D. Delaney, "Data Quality and Trust: Review of Challenges and Opportunities for Data Sharing in IoT", *Electronics*, vol. 9, s. 2083, 12 2020, ISSN: 2079-9292. DOI: 10.3390/electronics9122083.

[2] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum ja N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations", *IEEE Communications Surveys Tutorials*, vol. 21, s. 2702–2733, 3 huhtikuu 2019.

[3] T. S. Gopal, M. Meerolla, G. Jyostna, P. Reddy Lakshmi Eswari ja E. Magesh, "Mitigating Mirai Malware Spreading in IoT Environment", teoksessa *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, s. 2226–2230. DOI: 10.1109/ICACCI.2018.8554643.

[4] "Who Should Bear the Cost of IoT Security: Consumers or Vendors?" Viitattu 15.11.2024. (2018), url: https://insights.ubuntu.com/2017/02/07/who-should-bear-the-cost-of-iot-security-consumers-or-vendors/.

[5] S. H. Al-Awami, M. Mahfud Al-Aty ja M. F. Al-Najar, "Comparison of IoT Architectures Based on the Seven Essential Characteristics", teoksessa *2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, 2023, s. 305–310. DOI: 10.1109/MI-STA57575.2023.10169289.

[6] C. Li ja B. Palanisamy, ”Privacy in Internet of Things: From Principles to Technologies”, *IEEE Internet of Things Journal*, vol. 6, s. 488–505, 1 elokuu 2018.

[7] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider ja M. Hamdi, ”A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things”, *IEEE*, vol. 8, s. 4004–4022, 6 maaliskuu 2021.

[8] M. Al-Zyoud, T. Atkison ja J. Carver, ”An Overview of Emerging Privacy Issues in the Internet of Things”, teoksessa *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2016, s. 212–217. DOI: 10.1109/CSCI.2016.0047.

[9] K. U. Echenim ja K. P. Joshi, ”IoT-Reg: A Comprehensive Knowledge Graph for Real-Time IoT Data Privacy Compliance”, teoksessa *2023 IEEE International Conference on Big Data (BigData)*, 2023, s. 2897–2906. DOI: 10.1109/BigData59044.2023.10386545.

[10] F. Z. Berrehili ja A. Belmekki, ”Privacy Preservation in the Internet of Things”, teoksessa *Advances in Ubiquitous Networking 2*, R. El-Azouzi, D. S. Menasche, E. Sabir, F. De Pellegrini ja M. Benjillali, toim., Springer Nature Singapore, 2017, s. 163–175, ISBN: 978-981-10-1627-1.

[11] G. Y. Lee, K. J. Cha ja H. J. Kim, ”Designing the GDPR Compliant Consent Procedure for Personal Information Collection in the IoT Environment”, teoksessa *2019 IEEE International Congress on Internet of Things (ICIOT)*, 2019, s. 79–81. DOI: 10.1109/ICIOT.2019.00025.

[12] K. Ider, ”Assessment of the quality of user awareness of GDPR in healthcare IOT”, teoksessa *2021 International Conference on Biomedical Innovations and Applications (BIA)*, 2022, s. 25–28. DOI: 10.1109/BIA52594.2022.9831287.

[13] Euroopan unionin julkaisutoimisto. ”Henkilötietojen suojelu”. Viitattu 04.07.2025. (Viimeisin päivitys 08.03.2014), url: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=legissum%3Al14012.

[14] P. Hustinx, ”123EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation”, teoksessa *New Technologies and EU Law*, Oxford University Press, kesäkuu 2017, ISBN: 9780198807216. DOI: 10.1093/acprof:oso/9780198807216.003.0005.

[15] T. R. Chhetri, A. Kurteva, R. J. DeLong, R. Hilscher, K. Korte ja A. Fensel, ”Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent”, *Sensors*, vol. 22, nro 7, 2022, ISSN: 1424-8220. DOI: 10.3390/s22072763.

[16] A. Sänn, ”How does the Cyber Security Regulation for Processes and Products go hand in hand for Europe?”, teoksessa *IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society*, 2024, s. 1–5. DOI: 10.1109/IECON55916.2024.10905887.

[17] Uniqkey A/S. ”NIS2 Fines - Get an overview of the potential penalties for NIS2 non-compliance.” Viitattu 08.04.2025. (2025), url: https://nis2directive.eu/nis2-fines/.

[18] Euroopan komissio. ”NIS 2 -direktiivi: verkko- ja tietojärjestelmien kyberturvallisuutta koskevat uudet säännöt”. Viitattu 08.04.2025. (2025), url: https://digital-strategy.ec.europa.eu/fi/policies/nis2-directive.

[19] Euroopan komissio. ”Kyberresilienssisäädös”. Viitattu 24.04.2025. (2025), url: Kyberresilienssis%C3%A4%C3%A4d%C3%B6s.

[20] P. Voigt ja S. Alexander. ”The Cyber Resilience Act (CRA) has been published: What does it mean for businesses?” Viitattu 24.04.2025. (2024), url:

https://www.taylorwessing.com/en/insights-and-events/insights/2024/11/the-cyber-resilience-act-published.

[21] J. Singh, C. Millard, C. Reed, J. Cobbe ja J. Crowcroft, "Accountability in the IoT: Systems, Law, and Ways Forward", *Computer*, vol. 51, nro 7, s. 54–65, 2018. DOI: 10.1109/MC.2018.3011052.

[22] A. Subahi ja G. Theodorakopoulos, "Ensuring Compliance of IoT Devices with Their Privacy Policy Agreement", teoksessa *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2018. DOI: 10.1109/FiCloud.2018.00022.