Sampo Sillgren

TEKNOLOGISEN KEHITYKSEN JA YKSITYISYYDEN-SUOJAN VÄLISET RISTIRIIDAT ÄLYKAUPUNGEISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Sillgren, Sampo
Teknologisen kehityksen ja yksityisyydensuojan väliset ristiriidat älykaupungeissa
Jyväskylä: Jyväskylän yliopisto, 2024, 27 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Vuorinen, Jukka

Teknologinen kehitys on tuonut mukanaan lukemattomia mahdollisuuksia luoda uudenlaisia elinympäristöjä. Yhä useammasta kaupungista on tulossa teknologian lisääntyneen käytön myötä älykaupunkeja. Tämän seurauksena on kuitenkin syntynyt täysin uudenlaisia uhkia yksilöiden yksityisyydensuojalle ja tietoturvalle. Tässä kanditutkielmassa tarkasteltiin älykaupungeissa esiintyviä konflikteja sekä niiden mahdollistajia. Tutkielman tarkoituksena oli myös pyrkiä käsittelemään erilaisia ratkaisuja niiden lieventämiseksi. Tutkielma toteutettiin kirjallisuuskatsauksena, jonka menetelmin pyrittiin muodostamaan ajankohtainen käsitys aiheesta. Tutkimuskirjallisuuden perusteella löydetyt tutkimustulokset osoittivat konfliktien aiheutuvan lähinnä laajasta esineiden internetin laitteistosta sekä puutteellisista suojausmekanismeista.

Asiasanat: älykaupunki, esineiden internet, yksityisyydensuoja, tietoturva, vastuullisuus

ABSTRACT

Sillgren, Sampo
Conflicts between technology development and privacy protection in smart cities
Jyväskylä: University of Jyväskylä, 2024, 27 pp.
Information Systems Science, Bachelor's Thesis
Supervisor: Vuorinen, Jukka

Technological development has brought countless opportunities to create new innovative types of habitats. More cities are becoming smart cities due to the increased use of technology. However, this has resulted in completely new kinds of threats to the privacy and security of individuals. This bachelor's thesis examined the conflicts in smart cities as well as their enablers. The thesis also aimed to address various solutions to mitigate them. The research was carried out as a literature review, which aimed to form a topical understanding of the subject. According to the findings derived from the reviewed literature, conflicts in smart cities primarily arise due to the extensive deployment of Internet of Things hardware and a lack of protection mechanisms.

Keywords: smart city, internet of things, privacy protection, data security, responsibility

TAULUKOT

SISÄLLYS

1 JOHDANTO

Teknologinen kehitys on muuttanut merkittävästi ihmisten arkipäiväistä elämää sekä elinympäristöjen kehitystä. Yhä useammasta kaupungista on tulossa teknologian kehityksen myötä älykaupunkeja, tarjoten täysin uudenlaisia ratkaisuja ja mahdollisuuksia kaupunkien toimintaan. Älykaupunkien perimmäisenä tavoitteena voidaan nähdä olevan asukkaiden elämänlaadun parantaminen teknologisten innovaatioiden kautta (Koo & Kwon, 2017).

Teknologian nopean kehityksen myötä emme kuitenkaan aina täysin ymmärrä sen aiheuttamia vaikutuksia, ja siksi on tärkeää tutkia miten voimme hyödyntää teknologiaa vastuullisesti. Älykaupunkien hyödyntäessä teknologiaa ja suuria määriä dataa, saattaa herätä huoli yksityisyydensuojasta ja tietoturvasta mainitsee Zoonen (2016). Yleisen turvallisuuden ja yksityisyydensuojan välisen tasapainon löytäminen on elintärkeää, jotta älykaupungit voidaan suunnitella tulevaisuudessa suojelemaan yksilöiden oikeuksia, tarjoten samalla tehokkaita ja innovatiivisia palveluita (Zoonen, 2016).

Tässä tutkielmassa käsitellään älykaupunkien käsitettä ja siihen liittyviä aiheita, kuten datanhallintaa, esineiden internetiä (IoT), yksityisyydensuojaa ja tietoturvaa. Tutkielmassa käsitellään älykaupungeissa toistuvia konflikteja, uhkia sekä niiden aiheuttajia ja mahdollistajia. Älykaupunkien ja niiden sisällä tapahtuvien konfliktien tutkiminen on ajankohtaista ja tärkeää, jotta älykaupunkien kehitys pysyisi myös tulevaisuudessa oikeudenmukaisena sekä turvallisena. Ymmärtämällä yhteiskunnallista eriarvoisuutta, yksityisyyskysymyksiä, teknologisia haasteita ja kansalaisten sitoutumista koskevia huolenaiheita, päättäjät sekä kaupunkisuunnittelijat voivat luoda kestäviä ja asuttavia ympäristöjä, jotka palvelevat sen asukkaita taaten samalla puitteet kasvulle ja kehitykselle.

Tutkielma käsittelee myös sitä, miten älykaupungeissa voidaan puuttua konflikteihin ja niistä mahdollisesti aiheutuviin riskeihin, edistäen samalla yhteisöllisyyttä ja sosiaalista hyvinvointia. Tarkoituksena on osoittaa, että teknologiset innovaatiot ja yksilöiden oikeudet eivät ole toisiaan poissulkevia, vaan ne voivat täydentää toisiaan vastuullisen päätöksenteon kautta. Tämä lähestymistapa tekee tutkielman aiheesta merkittävän ja ajankohtaisen.

Tutkielman perimmäiset tutkimuskysymykset, johon pyritään vastaamaan ovat ”Millaisia riskejä ja konflikteja älykaupungeissa esiintyy liittyen

yksityisyydensuojaan sekä tietoturvaan?” ja ”Millaisia ratkaisuja on olemassa, joita voidaan soveltaa mahdollisten riskien ja konfliktien lieventämiseksi?”. Tutkielmassa käsitellään konfliktien monipuolisuutta, sekä sitä, miten konfliktit vaikuttavat mahdollisesti yksityisyydensuojaan. Tutkielmassa selvitetään myös, miten älykaupungit voivat vähentää mahdollisia konflikteja esimerkiksi vahvistamalla tietoturvaa ja yksityisyydensuojaa. Braunin ym. (2018) mukaan nämä voivat sisältää turvallisten tiedonsiirtokäytäntöjen luomista, salausprotokollien käyttöönottoa sekä valvottuja pääsyrajoituksia arkaluonteisiin tietoihin. Toimenpiteet, jotka tähtäävät tietoturvan ja yksityisyydensuojan parantamiseen, voivat samalla auttaa ennaltaehkäisemään konflikteja ja vähentämään riskejä.

Tutkielma on toteutettu kirjallisuuskatsauksena, joten sen tulokset pohjautuvat aikaisempaan kirjallisuuteen. Tutkielmassa käytettiin laajaa valikoimaa lähdemateriaalia, joka kattoi monenlaisia näkökulmia älykaupunkien toimintaan, teknologiseen kehitykseen, datanhallintaan, yksityisyydensuojaan ja tietoturvaan liittyen. Tutkielmassa hyödynnettiin tieteellisiä artikkeleita, IEEE-konferenssijulkaisuja sekä muita akateemisia lähteitä, jotka tarjoavat kattavasti tietoa tutkielman aihepiiristä. Lähdemateriaalin hakemiseen on käytetty pääasiassa Google Scholar hakupalvelua ja JYKDOK-tietokantaa.

Aineiston valinnan perusteena on toiminut myös lähteiden luotettavuuden arviointi, perustuen niiden julkaisuympäristöihin sekä viittausmääriin. Luotettavuutta on tutkittu myös julkaisufoorumien tason perusteella osassa tutkielmassa hyödynnetyissä aineistoissa. Lisäksi lähteitä hyödynnettäessä ollaan pyritty ottamaan huomioon niiden julkaisuajankohta, jotta pystyttäisiin takaamaan lähteiden ajankohtaisuus.

Tutkielma etenee johdannon jälkeen loogisesti. Toisessa pääluvussa käsitellään älykaupunkia sekä siihen liittyvää datanhallintaa. Luvussa otetaan tarkasteluun myös esineiden internet, sekä kuinka se liittyy älykaupunkien toimintaan. Luvun tarkoituksena on käydä läpi käsitteet, niiden ajankohtaisuus, sekä kuinka aiheet liittyvät toisiinsa. Kolmannessa pääluvussa käsitellään millaisia ristiriitoja älykaupungeissa esiintyy, liittyen yksityisyydensuojaan sekä tietoturvaan. Pääluvussa esitellään myös millaista dataa yksilöistä kerätään, ja miten se vaikuttaa yksityisyydensuojaan sekä tietoturvaan. Neljännessä pääluvussa esitetään ratkaisuja siihen, kuinka konflikteihin sekä riskeihin voidaan puuttua sekä vaikuttaa erilaisten teknologioiden sekä päätöksenteon avulla. Viimeisessä pääluvussa, joka toimii yhteenvetona, käsitellään vielä keskeisiä tuloksia, niiden merkitystä sekä tutkielman perusteella löydettyjä mahdollisia jatkotutkimusaiheita.

2 ÄLYKAUPUNKI JA DATANHALLINTA

Tässä pääluvussa selitetään käsitteet älykaupunki sekä siihen liittyvä datanhallinta. Tarkoituksena on määritellä älykaupungille ominaisia piirteitä sekä siihen liittyvää datanhallintaa. Luvussa käsitellään myös esineiden internetin käsitettä sekä sen merkitystä. Tarkoituksena on myös kuvata käsitteiden ajankohtaisuutta sekä tutkia niiden välisiä suhteita.

2.1. Älykaupunki

Batty ym. (2012) mukaan älykaupunki termillä tarkoitetaan nykyaikaista kaupunkia jossa teknologiaa hyödynnetään jo olemassa olevan perinteisen infrastruktuurin kanssa. Tarkoituksena on hyödyntää tieto- ja viestintätekniikkaa osana kaupungin palveluita, kuten liiketoimintaa, liikennettä, terveydenhuoltoa, viestintää sekä energianjakelua (Batty ym., 2012). Älykaupungin tarkoituksena voidaan täten nähdä olevan ihmisten elämänlaadun parantaminen sekä palveluiden tehostaminen (Mustonen., ym 2015; Neirotti ym., 2014).

Kunzmannin (2014) mukaan taas nykykäsitys älykaupungista ylittää kuitenkin pelkän teknologisen aspektin, sillä älykaupunkien toiminnassa korostetaan jatkuvasti enemmän ihmisen roolia sekä sosiaalisen pääoman merkitystä. Teknologia on siis vain väline, jota hyödyntämällä pystymme tekemään kaupungeistamme tehokkaampia sekä toimivampia kokonaisuuksia (Kunzmann, 2014). Älykaupunkien kehittämisessä onkin tärkeää huomioida, miten teknologia voidaan integroida kaupunkilaisen arkeen tavalla, joka edistää yhteisöllisyyttä ja parantaa täten elämänlaatua.

Teknologian jatkuvan kehittymisen kannalta älykaupunkeihin liittyen tulee kuitenkin huomioida vastuullisuus ja kestävyys. Tulevaisuuden älykaupunkihankkeissa on keskiössä teknologioiden integrointi keskenään sekä jo olemassa olevan infrastruktuurin kanssa. Kirrimtat ym. (2020) mukaan tieto- ja viestintätekniikalla tulee olemaan ratkaiseva merkitys kaupunkielämän eri osa-alueiden yhdistämisessä. Erilaisten integraatioiden tavoitteena on luoda tehokkaita sekä

saumattomia ratkaisuja, jotka johtavat parempaan hallintoon, liikkuvuuteen, ympäristön kestävyyteen sekä sosiaaliseen kestävyyteen (Kirrimtat ym., 2020).

Älykaupungit keräävät jatkuvasti dataa ja päämääränä on hyödyntää sitä tehokkaasti. Rathore ym. (2016) mukaan kerättävä data toimii keskeisessä roolissa etenkin päätösten teon parantamisessa, kaupunkisuunnittelussa ja toimivan infrastruktuurin ylläpitämisessä. Kun päätöksentekoa parannetaan, valtiot ja kaupungit voivat kehittyä entistä paremmin ja nopeammin, sillä aiempaa laadukkaampia ja tehokkaampia ratkaisuja pystytään tekemään nopeammin (Rathore ym., 2016).

Kuzlu ym. (2022) mainitsevat älykaupunkien keräämän datan tulevan pääosin hyvin laajasta esineiden internetin (IoT) verkostosta. Nämä laitteet keräävät reaaliaikaista tietoa liikenteestä, ympäristöolosuhteista, yleisestä turvallisuudesta sekä infrastruktuurin käytöstä. Tiedot ovat välttämättömiä kaupungin resurssien tehokkaan seurannan ja hallinnan kannalta. (Kuzlu ym., 2022).

2.2. Esineiden internet

Whitmore ym. (2015) määrittelevät esineiden internetin (IoT) konseptiksi, jossa arkipäivän teknologiset esineet on varustettu tunnistus-, verkko- ja prosessointiominaisuuksilla, joiden avulla ne voivat kommunikoida keskenään muiden laitteiden sekä palveluiden kanssa internetin välityksellä saavuttaakseen jonkin tietyn tavoitteen. Esineiden internet termillä siis viitataan suurimmaksi osaksi kaikkiin laitteisiin, jotka pystyvät mittaamaan, tunnistamaan tai prosessoimaan dataa sekä olemaan yhteydessä internetiin.

Risteska ym. (2017) huomauttavat, että laitteiden välillä on paljon vaihtelevuutta ja laitteet vaihtelevat yksinkertaisista antureista aina monimutkaisiin reitittimiin ja palvelimiin, jotka käsittelevät kerättyä dataa. Tämän seurauksen syntyy asetelma, jossa laitteet reagoivat entistä älykkäämmin ympäristöön (Risteska ym., 2017). Seurauksena tästä, laitteet pystyvät toimimaan automaattisesti kerätyn datan perusteella, vähentäen ihmisten väliintuloa.

Hyvin monipuolisen laitevalikoiman integrointi tuo kuitenkin mukanaan haasteita erityisesti turvallisuuden ja yksityisyyden kannalta. Mosenia ja Jha (2017) mainitsevat tutkielmassaan esineiden internetin verkossa vaihdettavan datan valtavan määrän aiheuttavan merkittäviä haavoittuvuuksia juurikin yksityisyydensuojan kannalta. Laitteiden automaattista toimintaa on hyvin vaikea valvoa, ja laitteiden monimuotoisuuden vuoksi se on myös erittäin monimutkaista (Mosenia & Jha, 2017).

Älykaupunkien toimintaan liittyen esineiden internetillä on hyvin kriittinen rooli ylläpitämässä infrastruktuuria sekä muita palveluita yllä. Esineiden internetiin liittyy kuitenkin hyvin paljon uhkia kun laitteet integroituvat jatkuvasti syvemmälle ihmisten jokapäiväiseen elämään. Mayerin ja Baeumnerin (2019) mukaan hyvin monista IoT-laitteista puuttuu kriittiset tietoturvaominaisuudet, joka luo mahdollisuuden erilaisille kyberhyökkäyksille. Laitteiden suuri määrä ja niiden monipuolinen verkosto, lisäävät siis tietomurtojen sekä luvattoman käytön riskiä (Mayer & Baeumner, 2019). Laitteiden turvallisuus ja yksityisyyden

suojaaminen ovat tulevaisuuden haasteita, sillä teknologian kehitys ja kaupungistuminen jatkuvat yhä kovempaa vauhtia.

2.3. Datanhallinta

Datanhallinta käsittää Ridleyn ja Stokerin (2001) mukaan kaikki prosessit ja strategiat, jotka liittyvät datan tehokkaaseen käsittelyyn erilaisten toimijoiden kesken. Tämä sisältää tehtäviä, kuten datan hankinta, tallentaminen ja saatavuuden varmistaminen toiminnan ja päätöksenteon tukemiseksi mainitsevat Ridley ja Stoker (2001). Datanhallinnan tavoitteena on tarjota valtavien tietomäärien, datan ja tietämyksen saumaton saatavuus ja yhdistäminen reaaliaikaisessa ympäristössä sekä tukea erilaisten toimijoiden toimintoja ja prosesseja. Asianmukainen datanhallinta on ratkaisevan tärkeää, jotta voidaan tarjota luotettavia ja laadukkaita datakokonaisuuksia, sekä varmistaa tietoturvastandardien säilyminen.

Datanhallintaan liittyy eri näkökulmia ja se voidaan jakaa moneen eri tehtävään ja osa-alueeseen:

- Datahallinto, joka tarkoittaa tiedon saatavuuden valvontaa ja sen uudelleenkäyttöä ja integrointia. Tehokas hallinto edellyttää tietojen omistajuuden ymmärtämistä ja standardien ylläpitoa, jotka ovat ratkaisevan tärkeitä tietoturvan ja datana eheyden kannalta (Koh & Watson, 1998).
- Tietoturva, jolla pyritään suojaamaan dataa luvattomalta käytöltä ja varmistamaan yksityisyydensuoja. Tämä sisältää asianmukaisen valvonnan, erilaiset salaukset sekä säännölliset tietoturva-auditoinnit (Koh & Watson, 1998).
- Datan laadun varmistaminen, johon kuuluu laadukkaat datanhallintajärjestelmät, jotka varmistavat, datan laadun pysyvän johdonmukaisena sekä oikeellisena (Frugoli, Etger & Kuhar, 2010).
- Master datanhallinta (engl. Master Data Management tai MDM), joka tarkoittaa ydindatan ja kriittisen tiedon hallintaa (Chaki, 2015). MDM käsittää datanhallinnan ydinprosessit, linjaukset, standardit ja välineet, joiden avulla voidaan varmistaa datan yhdenmukaisuuden, hallinnan ja paikkansapitävyyden (Chaki, 2015).
- Datan tallentaminen ja integrointi. Datan jäsennelty tallentaminen helpottaa datan tehokasta hyödyntämistä ja integrointia. Datan integrointi eri lähteistä ja sen varmistaminen, että data on tallennettu yhteensopiviin formaatteihin, on olennaisen tärkeää kattavan tiedonhallinnan kannalta (Chaki, 2015).
- Datan arkistointi ja säilyttäminen, johon kuuluu asianmukaiset käytänteet datan säilyttämiseen liittyen (Joshi & Krag, 2010). Tämän avulla varmistetaan, että tietoihin pääsee käsiksi tarvittaessa ja ne on suojattu häviämiseltä. Tähän liittyy myös ohjeistus siitä, kuinka kauan erityyppisiä tietoja tulisi säilyttää ja miten hävittää data turvallisesti, mitä ei enää tarvita (Joshi & Krag, 2010).

Älykaupungit hyödyntävät hyvin paljon erilaista tietoa sekä dataa esineiden internetin avulla, tehokkuuden ja suorituskyvyn parantamiseksi. Teknologiset innovaatiot tarjoavat yhä enemmän mahdollisuuksia hyödyntää dataa analysoinnin avulla, jolla pyritään yhä tehostamaan tulevaisuuden kaupunkien toimintaa. Datanhallinnalla on merkittävä rooli älykaupungin toiminnan kehittämisen kannalta. (Radziszewska, 2023).

Fangi ym. (2021) mukaan turvallisuuden ja eheyden varmistaminen on kriittistä älykaupunkien kontekstissa, sillä data käsittelee hyvin sensitiivistä ja arkaluontoista tietoa yksityisistä ihmisistä. Luottamuspohjaiset turvajärjestelmät, -kehykset ja standardit auttavat hallitsemaan tietojen eheyttä jo tiedonkeruuprosessin aikana, puuttumaan mahdollisiin turvallisuusriskeihin ja varmistamaan, että päätöksenteko perustuu tarkkoihin ja luotettaviin tietoihin (Fang ym., 2021).

2.3.1 Datan elinkaaren hallinta

Liu ym. (2017) mukaan datalla ja tiedolla on oma elinkaarensa ja tätä usein kuvataan datan elinkaaren hallinnalla (DLCM). Älykaupungit hallitsevat tietoa sekä dataa sen toiminnasta ja datalla voidaan siis nähdä olevan elinkaari; eli mistä lähtien data on ollut olemassa ja mihin se siirtyy jatkuvasti. Älykaupunkien toiminnassa yritetään tähdätä datan eheyteen sekä anonymiteettiin juurikin datan elinkaaren hallinnan avulla (Liu ym., 2017).

Datan elinkaaren hallinnalla on hyvin keskeinen rooli älykapunkien toiminnan ja kestävyyden kannalta. Sinaeepourfard ym. (2016) mainitsevat datan elinkaaren hallinnan edellyttävän tiedonkulun hallintaa eri vaiheiden, kuten luomisen, tallennuksen, käytön ja poistamisen kautta, varmistaen sen säilymisen käyttökelpoisena ja turvallisena koko elinkaarensa ajan.

Hyvä esimerkki datan elinkaaren hallinnasta älykaupungeissa on Smart City Comprehensive Data Life Cycle (SCC-DLC) -malli, joka tarjoaa jäsennellyt puitteet datan käsittelyyn eri vaiheissa, heti luomisesta kulutukseen ja poistoon käyttäen Fog to Cloud (F2C) -resurssienhallintaa (Sinaeepourfard ym., 2016). Tämä malli paitsi parantaa tietojen saatavuutta ja luotettavuutta, myös varmistaa tietoturvan, joka on ratkaisevan tärkeää yleisen luottamuksen ylläpitämiseksi ja tietosuojamääräysten noudattamiseksi mainitsee Sinaeepourfard ym. (2016).

Tehokkaan datan elinkaaren hallinnan avulla älykaupungit voivat siis optimoida toimintojaan, tehostaa palvelutarjontaa ja edistää kestävää kehitystä tekemällä dataan perustuvia päätöksiä. Tämä kattava datan elinkaaren hallinta on olennainen osa älykaupunkien toimintaa ja resilienssiä, mikä osoittaa, kuinka teknologia ja tiedonhallinta pystyvät olemaan osana luomassa asuttavampia ja tehokkaampia tulevaisuuden kaupunkiympäristöjä (Sinaeepourfard ym., 2016).

3 YKSITYISYYTEEN JA TIETOTURVAAN LIITTYVÄT RISTIRIIDAT ÄLYKAUPUNGEISSA

Tässä pääluvussa selvitetään miten yksityisyydensuoja sekä tietoturva ilmenevät älykaupungeissa. Luvussa esitetään taulukon avulla millaista dataa yksilöistä kerätään ja miten sitä hyödynnetään. Lisäksi luvussa käsitellään yksityisyyteen ja tietoturvaan liittyviä riskejä, ristiriitoja sekä erilaisia konflikteja nykyaikaisen teknologian hyödyntämiseen liittyen.

3.1. Yksityisyydensuoja älykaupungeissa

Yksityisyydensuojalla tarkoitetaan Renaudin ja Galvez-Cruzin (2010) mukaan kattavia toimenpiteitä, joilla suojataan henkilötietoja luvattomalta pääsyltä, väärinkäytöltä, ja täten pyritään kunnioittamaan sekä ylläpitämään yksilön oikeutta yksityisyyteen. Yksityisyydensuoja on ihmisoikeus, ja jokaisella yksilöllä tulisi olla mahdollisuus pitää henkilökohtaiset sekä suojatut tietonsa henkilökohtaisina. Yksityisyydensuojan säilyttämiseen liittyy myös muu kuin tekninen puoli, sillä lainsäädännölliset sekä hallinnolliset päätökset ovat tärkeässä roolissa yksityisyydensuojan kannalta, valvoen datan keräämistä, käyttöä sekä jakelua (Renaud & Galvez-Cruz, 2010).

Yksityisyydensuojaan liittyy useita ulottuvuuksia ja niiden avulla voidaan käsitellä yksityisyydensuojaa monipuolisemmin. Yksilöillä itsellään on suuri vastuu oman yksityisyydensuojan suhteen ja tätä kuvataan yksilöllisellä ulottuvuudella Yuan ym. (2010) mainitsevat tutkielmassaan. Guardan ja Zannonen (2009) mukaan taas yksi merkittävistä ulottuvuuksista on oikeudellinen ulottuvuus, joka korostaa lakien ja asetusten noudattamista sekä oikeudellisten periaatteiden käsittelyä yksilöiden kohdalla. Teknologinen ulottuvuus taas keskittyy enemmän teknisiin ratkaisuihin, kuten datan salaukseen ja suojattuihin protokolliin, jotka edistävät yksityisyydensuojaa monin merkittävin tavoin (Hansen ym., 2015). Yhtenä merkittävänä ulottuvuutena voidaan pitää Coftan (2008) mainitsemaa yhteiskunnallista ulottuvuutta, joka tutkii yksityisyydensuojan sosiaalisia sekä kulttuurisia vaikutuksia. Eri ulottuvuuksien avulla pystytään

ymmärtämään paremmin ja laajemmin käsitettä yksityisyydensuoja, sillä ymmärrämme, kuinka se ilmenee erilaisissa konteksteissa ja ympäristöissä.

Yksityisyydensuoja on keskeinen tekijä liittyen älykaupunkien vastuulliseen toimintaan sekä turvallisen infrastruktuurin ylläpitämiseen. Tämä näkyy monella tavalla yksilöiden tasolla. Braun ym. (2018) mukaan yksityisyydensuojan takaaminen johtaa parempaan yksilöiden osallistamiseen, sillä yksilöiden tulee kokea heidän yksityisyyden olevan turvassa. Yksilö voi muuten kokea haluttomuutta vaikuttaa yhteiskunnassa tai kokea olevansa turvattomassa asemassa infrastruktuurin keskellä. Tämä voi myös vaikutta negatiiviseti älykaupunkien eri teknolgoiden hyödyntämiseen, sillä niiden tarjoamaa dataa ei päästä hyödyntämään täydellä kapasiteetilla (Braun ym., 2018).

Eckhoffin ja Wagnerin (2018) mukaan yksityisyydensuojan puute voi johtaa syrjintään ja sosiaaliseen lajitteluun. Tämä luo eriarvoisen asetelman yhteiskuntaan, jossa yksilöitä voidaan kohdella eri tavalla heistä kerätyn tiedon perusteella. Tehokas yksityisyydensuoja auttaa ehkäisemään tätä asetelmaa, varmistaen oikeudenmukaisen ja tasapuolisen ympäristön kaikille yksilöille, katsomatta heidän taustaa jatkavat Eckhoff ja Wagner (2018).

Yksityisyydensuojan takaaminen on kriittistä kansalaisten ja kaupungin viranomaisten välisen luottamuksen säilyttämiseksi maintisee Qu ym. (2019). Luottamus on keskeistä älykaupunkialoitteiden hyväksymiselle ja onnistumiselle. Ilman sitä asukkaat saattavat suhtautua myös skeptisesti käyttöön otettuihin teknologioihin ja järjestelmiin, mikä mahdollisesti haittaisi niiden käyttöönottoa ja potentiaalista tehokkuutta (Qu ym., 2019).

Yksityisyydensuojan merkitys nousee jatkuvasti yhä tärkeämmäksi aiheeksi, sillä esineiden internetin kautta operoivat laitteet toimivat jatkuvasti ympärillämme yhä kasvavissa määrin. Esineiden internetin yleistyminen älykaupungeissa aiheuttaa merkittäviä uhkia juurikin yksilöiden yksityisyydelle, sillä sosiaaliset linkit sekä sijaintipalvelut tarjaovat hyvin paljon mahdollisuuksia päästä käsiksi sensitiiviseen tietoon (Fabrgue & Bogoni, 2023). Yksityisyydensuojan takaaminen vaikuttaa siis positiivisesti laajalti koko älykaupungin toimintaan, sillä se osallistaa yksilöitä, ja täten tuottaa tärkeää dataa sitä hyödyntäville elimille.

Zoonen (2016) esittelee älykaupungin datamaiseman taulukossa dataa, mitä yksilöistä kerätään älykapungeissa. Taulukosta käy hyvin ilmi millä tavoin dataa kerätään, mihin data liittyy ja kuinka sitä pyritään hyödyntämään (ks. Taulukko 1). Taulukko liittyy tiiviisti yksityisyydensuojaan, sillä se antaa selkeän kuvan datan hyödyntämisestä, sen eri lähteistä ja vaikutusalueista. Taulukon tietotyypit ja käyttökohteet ulottuvat eri sektoreille, mukaan lukien infrastruktuuri, kestävyys, terveys, yhteisö, liiketoiminta ja kokemus. Vaikka nämä tietotyypit tarjoavat mahdollisuuksia datan hyödyntämisen suhteen, ne aiheuttavat myös merkittäviä tietosuojariskejä yksilöille, mikäli datanhallinnassa ilmenee heikkouksia.

TAULUKKO 1 Älykaupungin datamaisema (mukaillen Zoonen, 2016, s. 474)

Sektori	**Vaikutusalue**	**Datan tyyppi**	**Käyttöesimerkki**
Infrastruktuuri	Liikenne ja omaisuuden hallinta, rakennettu ympäristö	Seurantadata, rekisteröintidata, geodata	Liikennemallit, reaaliaikaiset kojelaudat
Kestävyys	Energian käyttö, vesi, ympäristö, sää	Anturi- ja seurantadata, kansalaismittaustiedot	Ilmanlaadun valvonta ja saastevaroitukset
Terveys	Terveys, elämänlaatu, hyvinvointi, elinajanodote	Terveysdata, kyselydata, elämäntapadata	Paikkakohtaiset melutasot ja sosiaaliset tai terveydelliset ongelmat tietyillä alueilla
Yhteisö	Koulutus, sosiaalinen pääoma, muuttoliike, naapurustot, asuminen, rikollisuus	Kyselydata, kansalais- ja yhteisöverkkodata	Koulujen laatu tietyissä naapurustoissa
Liiketoiminta	Liiketoimintamahdollisuudet, markkinointi, sijaintiin perustuvat palvelut	Sosiaalisen median data, avoimen hallinnon data	Sijoituskartat uusien yritysten houkuttelemiseksi
Kokemus	Tapahtumat, vapaa-aika, yöelämä, matkailu, perintö	Sosiaalisen median data, arkistoitu data, anturidata	Reaaliaikaiset sosiaalisen median analytiikat väkijoukon hallintaan

3.2. Tietoturva ja sen harjoittaminen älykaupungeissa

Nykyaikainen näkemys tietoturvasta Solmsin ja Nikerkin (2013) mukaan ottaa huomioon laajemman kontekstin kyberturvallisuudessa, jossa tietoturva, verkot ja järjestelmät risteävät henkilökohtaisen turvallisuuden ja yksityisyyden kanssa. Tietoturvan pääpaino on suojautumisessa uhilta, jotka kohdistuvat yksilöihin, organisaatioihin sekä yhteiskuntaan. Solmsin ja Niekerkin (2013) määritelmä kuvastaa kokonaisvaltaista lähestymistapa, joka sisältää myös inhimilliset tekijät osana modernia sekä nykyaikaista tietoturvaa.

Tietoturva vaatii myös monitieteistä lähestymistapaa mainitsee Porter (2009), johon sisältyy elementtejä käyttäytymistieteistä, psykologiasta ja etiikasta, kokonaisvaltaisempien uhkien käsittelemiseksi. Tämä laajempi näkökulma osoittaa, että tehokkaissa turvatoimissa on otettava huomioon ihmisen käyttäytyminen sekä mahdolliset yhteiskunnalliset vaikutukset (Porter, 2009).

Tietoturvan moderni määritelmä kuvastaa siis kokonaisuutta, johon kuuluu kokonaisvaltainen näkemys tietoturvariskeistä, uusien teknologioiden integrointi osaksi yhteiskuntaa, inhimilliset tekijät sekä kokonaisvaltainen lähestymistapa tietojen, järjestelmien ja ihmisten suojaamiseen mahdollisilta uhilta.

Älykaupungit tukeutuvat vahvasti teknologiaan esineiden internetin avulla, parantaakseen kaupunkielämää sekä palveluilta, mikä tekee niistä haavoittuvia erilaisille turvallisuusuhille (Mayer & Baeumner, 2019).

Kuten yksityisyydensuojaan liittyvässä kappaleessa käytiin läpi, älykaupungit keräävät asukkailta valtavan määrän henkilökohtaisia ja arkaluontoisia tietoja, kuten liikennekuvioita, energiankäyttöä ja terveystietoja. Näiden tietojen suojaaminen on välttämätöntä yksityisyyden säilyttämiseksi ja luottamuksen rakentamiseksi kansalaisten keskuudessa. Ratkaisuja ovat salaus, turvalliset tietoliikenneprotokollat ja kulunvalvonta (Braun ym., 2018). Yksityisyydensuoja ja tietoturva ovat siis hyvin vahvasti toisiinsa sidoksissa.

Tietoturvaa harjoitetaan älykaupungeissa monilla eri menetelmillä, protokollilla sekä sääntelyn avulla. Dong ja kumppaneiden (2018) mukaan älykaupungeissa hyödynnetään monikerroksisia tietoturvakehyksiä, jotka käsittävät datanhallinnan, teknologian hyödyntämisen sekä eri käyttöjärjestelmät. Tämä tietoturvakehys tarjoaa jäsennellyn tavan käsitellä turvallisuutta eri tasoilla, mikä takaa kattavat sekä monipuoliset suojausmekanismit. (Dong ym., 2018).

Moshentenko ja Zhurakovski (2021) maintisevat tietoturvaan keskeisesti liittyviä suojausmekanismeja joita hyödynnetään älykaupungeissa olevan erilaiset viestintäprotokollat turvallisen tiedonsiirron varmistamiseksi. Näistä yleisimpi ovat muun muassa suojattu SSL-protokolla, siirtokerroksen suojausprotokolla TLS ja muut salausmenetelmät, jotka suojaavat tietojen eheyttä ja luottamuksellisuutta (Moshentenko & Zhurakovski, 2021).

Hierarkkisissa älykaupungeissa identiteettipohjaiset tietoturvakehykset käyttävät myös pseudonyymejä ja muita menetelmiä avaintenhallinnan turvaamiseksi ja yksittäisten haittakohtien poistamiseksi perinteisessä julkisen avaimen infrastruktuurissa (PKI) (Gokul & Sankaran, 2020).

Wu ym. (2020) mukaan älykaupunkien tehokkaita tietoturvakäytäntöjä ohjaavat loppujen lopuksi tiukat käytännöt, jotka käsittelevät tietoturvatoimenpiteiden muotoilua, toteutusta, ylläpitoa ja tehokkuutta. Nämä käytännöt ohjaavat kaupunkeja sekä organisaatioita turvallisten käytäntöjen toteuttamisessa ja korkeiden standardien mukaisessa tietoturvan ylläpitämisessä (Wu ym., 2020).

Yhteenvetona voidaan todeta, että älykaupunkien tietoturvaan liittyen tulee ottaa huomioon kokonaisvaltainen lähestymistapa tietojen suojaamiseen, yksityisyydensuojan varmistamiseen ja kriittisten järjestelmien eheyden ylläpitämiseen liittyen. Tietoturvan ylläpitäminen on nykypäivänä on hyvin moniulotteinen ja monimutkainen prosessi, sillä enää ei voida sivuuttaa yksilöiden sekä teknologian välisiä riippuvuussuhteita.

3.3. Yksityisyydensuojaan sekä tietoturvaan liittyvät riskit älykaupungeissa

Älykaupunkien sekä esineiden internetin tarjoamat mahdollisuudet voivat olla merkittävässä asemassa rakentamassa yhä parempia, kestävempiä sekä tehokkaampia kaupunkikokonaisuuksia. Makhdoom ym. (2019) mainitsevat, että datan ja teknologian merkitys kaupungeissa sekä sen käytön ja saatavuuden lisääntyminen altistavat yksilöt erilaisille mahdollisille uhille, kuten tietoturvaloukkauksille, yksityisyyteen liittyville hyökkäykselle ja kyberturvallisuusriskeille. Makhdoom ym. (2019) jatkavat, että älykaupunkien hyödyntäessä esineiden internetin laitteita ja valtavia tietomääriä, kasvaa mahdollisuus datan luvattomaan pääsyyn ja henkilötietojen väärinkäyttöön.

Makhdoom ja kummpanit (2019) maintisevat esineiden internetiin liittyvien uhkien kattavan analyysin paljastavan, että näitä riskejä voi esiintyä eri tasoilla teollisuuden ohjausjärjestelmistä terveydenhuoltoon, yksilöiden elämään ja yhteiskunnan yleiseen turvallisuuteen. Yksi yhteiskunnallisesti hyvin huomattava uhka on DDoS (Distributed Denial of Service) -hyökkäykset esineiden internetin bottiverkkojen kautta, mikä voi johtaa vakaviin järjestelmähäiriöihin ja palvelukatkoksiin (Makhdoom ym., 2019). Näihin riskeihin puuttuminen on ratkaisevan tärkeää sen varmistamiseksi, että älykaupungit pystyvät tarjoamaan asukkailleen turvallisia, luotettavia asuttavia ympäristöjä (Cui ym., 2018). Alla on listattu taulukkoon yksityisyydensuojaan ja tietoturvaan liittyviä riskejä älykaupungissa. Taulukon sisältämä data on kerätty useista eri lähteistä (ks. Taulukko 2).

TAULUKKO 2 Älykaupungeissa esiintyävät riskit ja uhat

Riski tai uhka	**Mahdollistaja**
Tietovuodot ja datan luvaton jakelu (Cui ym., 2018)	Suuret datamäärät, toimimattomat ja puutteelliset suojausmekanismit ja vanhentuneet protokollat (Cui ym., 2018)
Valvonnan kautta tapahtuvat yksityisyysloukkaukset (Koshy ym., 2021)	Kameroiden sekä esineiden internetin antureiden käyttö (Koshy ym., 2021)
Kyberturvallisuusuhat (Kitchin & Dodge, 2020)	Esineiden internetin kautta tapahtuvat DDoS (Distributed Denial of Service) ja ransomware-hyökkäykset (Kitchin & Dodge, 2020)
Identiteettivarkaudet (Wang ym., 2015)	Henkilötietoihin kohdistuvan datanhallinnan puutteet (Wang ym., 2015).
Tietojenkalastelu ja sosiaalinen manipulointi (engl. social engineering) (Caviglone ym., 2015)	Lisääntynyt hyökkäyspinta-ala (engl. attack surface) älykaupungeissa (Caviglone ym., 2015)
Kriittisen infrastruktuurin häiriöt (Braun ym., 2018)	Esineiden internetin kautta toimivat laitteet (Braun ym., 2018)
Datan yhdistäminen ja profilointi (Ismagilova ym., 2020)	Suurten datamäärien yhdistäminen yksilöihin (Ismagilova ym., 2020)
Luvaton tietojen kerääminen (Li ym., 2016)	Esineiden internetin kautta toimivat laitteet, sensorit sekä anturit (Li ym., 2016).
Kaupunkipalveluissa esiintyvät konfliktit ja häiriöt (Ma ym., 2016)	Teknologiset risteymät ja päällekkäisyydet (Ma ym., 2016)
Sosiaaliset linkitykset sekä sijaintipalvelujen hyödäntminen luvatta (Fabrgue & Bogoni, 2023)	Sijaintipalvelut, sosiaalinen media ja esineiden internet (Fabrgue & Bogoni, 2023)

4 YKSITYISYYDENSUOJAN JA TIETOTURVAN TAKAAMINEN ÄLYKAUPUNGEISSA

Tässä pääluvussa esitellään ratkaisuja, mitä älykaupunkien toiminnassa voitaisiin huomioida liittyen älykaupunkien riskeihin ja uhkiin, kun yksityisyydensuoja ja tietoturva otetaan huomioon. Lisäksi tarkastellaan älykaupungeissa tapahtuvaa päätöksentekoa ja sen tulevaisuutta. Päätöksentekoa käsitellään erilaisten vastuullisuusnäkökulmien kautta.

4.1. Ratkaisuja yksityisyydensuojan ja tietoturvan takaamiseen

Tutkielmassa aiemmin käsitellyissä kappaleissa ollaan käyty läpi älykaupungeissa hyödynnettävien teknologioiden aiheuttamia mahdollisia riskejä ja konflikteja. Näihin epäkohtiin voidaan puuttua useiden eri ratkaisujen avulla, ja tulevaisuuden kannalta se voidaan nähdä hyvin tärkeänä osana takaamassa yksilöille turvallisen älykaupunkiympäristön.

Braunin ja kumppaneiden (2018) mukaan yksi keskeinen strategia yksityisyydensuojaan liittyvien ongelmien ratkaisemiseksi on turvallisten tiedonjakokäytäntöjen luominen sekä ylläpitäminen. Tähän liittyy salausprotokollat, turvalliset viestintäkanavat ja valvottu pääsy arkaluonteisiin sekä sensitiivisiin tietoihin (Braun ym., 2018). Lisäksi älykaupunkien on puututtava ennalta mainittuihin kyberturvallisuusriskeihin ylläpitämällä jatkuvasti vahvoja toimenpiteitä, kuten tunkeutumisen estojärjestelmiä (IPS) ja säännöllisiä tietoturva-auditointeja (Elmaghraby & Losavio, 2014). Näillä toimenpiteillä pyritään suojautumaan ulkoisilta uhilta, sekä myös auttamaan rakentamaan luottamusta yksilöiden ja yhteiskunnan sidosryhmien kesken.

Lin ja kumppaneiden (2016) mukaan toinen yksityisyydensuojan kannalta keskeinen aihe on datan ylikeräyksen estäminen. Älykaupunkien toiminnassa tulisi toteuttaa sääntelyä, joka rajoittaa datan keräämisen vain siihen, mikä on välttämätöntä älykaupunkien kehittämisen ja sen palveluiden ylläpitämisen kannalta (Li ym., 2016). Tietoisuuden lisääminen Zhang ym. (2017) mukaan

auttaisi yksityisyys- ja tietoturvallisuuskysymyksiin myös yksilöitä ymmärtämään mahdollisia riskejä sekä epäkohtia paremmin. Kansalaisten kouluttaminen näihin tietoturvallisuusasioihin liittyen voisi siis edistää yksityisyydensuojaa ja turvallisuuden kulttuuria (Zhang ym., 2017). Yksilöiden kouluttaminen ja tietoisuuden lisääminen voisi toimia myös osana datan ylikeräyksen estämistä, sillä yksilöt voisivat itse ottaa kantaa heistä kerätyn datan määrään ja laatuun.

Kuten aikaisemmin käytiin läpi yksilöiden kouluttamista, yksi keskeinen seikka on käyttäjien suostumuksen varmistaminen heistä kerätyn datan käyttöön (Witti & Konstantas, 2018). Antamalla käyttäjien hallita omaa dataa, älykkaupungit voivat lisätä täten kansalaisten luottamusta.

Yksityisyyttä lisäävien teknologioiden käyttöönotolla on Eckhoffin ja Wagnerin (2018) mukaan merkittävä rooli yksityisyydensuojan ja tietoturvan parantamisen kannalta. Nämä teknologiat, kuten datan anonymisointi ja erotettu yksityisyys (engl. differential privacy), ovat keskeisessä roolissa sen varmistamisessa, että arkaluontainen data pysyy suojattuna samalla kun älykaupungit voivat jatkaa toimintaansa tehokkaasti. Näiden teknologioiden avulla voidaan estää luvaton pääsy henkilötietoihin ja vähentää yksityisyydensuojan loukkausten määrää (Eckhoff & Wagner, 2018). Innovaation ja yksityisyydensuojan välinen tasapaino on merkittävässä roolissa älykaupunkien toiminnassa, ja näillä teknologisilla ratkaisulla pystytään löytämään toimivia ratkaisuja siihen liittyen.

Esineiden internetillä on myös merkittävä rooli takaamassa nykyaikaiset käytänteet liittyen yksityisyydensuojaan ja tietoturvaan, sillä yhteiskunnan toiminta liittyy jatkuvasti yhä vahvemmin teknologioiden tuomiin mahdollisuuksiin. Yksi kriittinen strategia on turvallisten viestintäkanavien luominen. Esineiden internet pohjaisten älykaupunkien suhteen tiedonsiirto tapahtuu useiden laitteiden välillä, mikä lisää luvattoman käytön riskiä. Toteuttamalla jo aiemmin mainittua salausta ja suojattuja tietoliikenneprotokollia kaupungit voivat vähentää näitä riskejä (Elmaghraby & Losavio, 2014).

Älykaupungit voivat harjoittaa myös kontekstitietoista tietoturvaa, jonka avulla tietoturvatoimia voidaan säätää sen mukaan, missä kontekstissa tietoja mahdollisesti käytetään. Tämä lähestymistapa vastaa hyvin nykyaikaisiin yksityisyys- ja tietoturvatarpeisiin esineiden internet ympäristöissä (Sylla ym., 2019).

Cui ym. (2018) mukaan yksityisyydensuojaan ja tietoturvaan puuttuminen älykaupungeissa on ratkaisevan tärkeää luottamuksen rakentamiseksi ja älykaupunkien pitkän aikavälin tavoitteiden varmistamiseksi. Aiempien konfliktien sekä riskien huomioonottaminen on tärkeää, jotta vältytään historiallisten virheiden toistamista, ottaen samalla käyttöön vankat sekä toimivaksi todetut tietosuojakäytännöt. Näin älykaupungit voivat luoda turvallisemman ja asuttavan ympäristön, edistäen innovointia ja kestävää kasvua, vastaten samalla tulevaisuuden haasteisiin (Cui ym., 2018).

4.2. Vastuullinen päätöksenteko

Älykaupunkien toiminnassa käsitellään vastuullisuuskysymyksiä ja harjoitetaan vastuullisuutta erilaisten sääntelyiden sekä päätöksenteon kautta. Tulevaisuuden kannalta päätöksenteolla tulee olemaan vielä merkittävämpi rooli, sillä nopeasti kehittyvillä teknologioilla, kuten tekoälyllä, tulee olemaan yhä suurempi rooli ihmisten arkipäiväisessä elämässä.

Älykaupunkien yksityisyydensuojaan liittyvät vastuullisuusnäkökulmat keskittyvät lähinnä sen varmistamiseen, että yksilöt, teknologian tarjoajat ja kehittäjät sekä muut merkittävät sidosryhmät ovat yhdessä vastuussa kansalaisten yksityisyydensuojasta. Näiden käytäntöjen tarkoituksena on lähinnä edistää luottamusta, avoimuutta ja eettisten standardien noudattamista.

Finch ja Tene (2018) mainitsevat tutkielmassaan päätöksenteon ja datanhallinnan näkyvyyden olevan merkittävä tekijä. Seattlen ja Barcelonan kaltaiset kaupungit toteuttavat jo avoimen datan kehyksiä ja läpinäkyvyyttä varmistaakseen vastuullisen datanhallinnan, edistäen samalla luottamusta eri sidosryhmien välillä.

Edwardsin (2018) mukaan yksityisyydensuojan periaatteiden integrointi älykaupunki-infrastruktuurin kehittämiseen on keskeinen vastuullisuusnäkökulma jota harjoitetaan. Tällä lähestymistavalla varmistetaan, että yksityisyydensuojaan liittyviin huolenaiheisiin puututaan heti alusta alkaen minimoiden tietosuojariskit ja varmistaen tietosuojalakien, kuten EU:n yleisen tietosuoja-asetuksen (GDPR), noudattaminen. Tällaisten määräysten noudattaminen edellyttää jatkuvia arviointeja ja päivityksiä yksityisyyden suojan varmistamiseksi (Edwards, 2016). EU:lla on tärkeä rooli toimia vastuullisena päätöksentekijänä myös tulevaisuudessa.

Christofi ym. (2019) mainitsevat yhdeksi merkittäväksi päätöksenteon vastuullisuusnäkökulmaksi, jota harjoitetaan, olevan kansalaisten osallistumis- ja yksityisyysvaikutusten arvioinnit. Vastuullinen yksityisyydensuojan harjoittaminen älykkäissä kaupungeissa tarkoittaa kansalaisten osallistamista ja yksityisyyden vaikutusarviointien (PIA) suorittamista yksityisyydensuojaan liittyvien riskien tunnistamiseksi (Christofi ym., 2019). PIA on yhteistyöprosessi, jonka avulla sidosryhmät voivat arvioida älykaupunkihankkeiden mahdollisia yksityisyysvaikutuksia ja tehdä muutoksia tietosuojan parantamiseksi (Christofi ym., 2019). SPECTRE-hankkeessa korostetaan älykaupunkiympäristön vastuullisuuden lisäämistä osallistavien PIA-lakien ja yhteistoiminnallisten sääntelykehysten avulla (Christofi ym., 2019).

Bartlozzi ja kumppanit (2015) nostavat kanssa keskeiseksi tekijäksi kansalaisten osallistamisen päätöksentekoprosesseissa. Päätöksentekoa tukevat järjestelmät (engl. Decision Support Systems tai DSS) voivat olla keskeisessä roolissa, jolloin kaupungit voivat ottaa kansalaisia mukaan päätöksentekoon digitaalisten alustojen ja osallistavan suunnittelun kehysten kautta (Bartolozzi ym., 2015). Tämä lähestymistapa kannustaa yhteisöä sitoutumaan ja edistää vastuullisuutta sekä yhteisöllisyyttä teknologisten innovaatioiden kautta.

Älykaupungeissa harjoitetaan päätöksentekoa erilaisten vastuullisuusnäkökulmien kautta, mutta merkittävä esille nouseva asia on juurikin

läpinäkyvyys sekä kansalaisten osallistaminen. Tulevaisuuden kannalta nämä voivat olla juurikin kriittisiä avaintekijöitä älykaupunkien vastuullisen toiminnan ylläpitämisessä.

Alawadhi ja Scholl (2016) mainitsevat tutkielmassaan älykkäiden hallintomallien käyttöönoton olevan älykaupunkien päätöksenteon kriittisiä elementtejä. Näissä malleissa yhdistyvät teknologia, yhteisöllisyys sekä eri virastojen yhteistyö. Älykkäiden hallintomallien käyttöönotossa esiintyy taas merkittävänä tekijänä yhteisöllisyys, joka voi lisätä kansalaisten avoimuutta sekä luotettavuutta älykaupunkien toimintaa kohtaan.

Carli ym. (2017) esittelevät tutkielmassaan näkökulman, jossa älykaupunkien tulisi ottaa osaksi päätöksentekoa erilaisia innovatiivisia päätöksentekostrategioita, jotka tukevat älykaupungin konseptin mukautuvaa ja reagoivaa luonnetta. Tähän voi liittyä kriittisten kaupunkitoimintojen päätöksentekostrategioita, jotka mahdollistavat jäsennellyn ja läpinäkyvän toiminnan päätöksentekoprosesseissa (Carli ym., 2017).

Tutkielmista löydettyjen havaintojen pohjalta voidaan todeta, että vastuullinen päätöksenteko älykaupungeissa edellyttää monien eri perspektiivien huomioimista.Yhteistyön, hallintomallien, kansalaiskeskeisyyden ja innovatiivisten strategioiden kautta voidaan saada aikaan kattavia tuloksia. Näiden keskeisten näkökulmien avulla älykaupungit voivat varmistaa, että päätöksentekoprosessit ovat läpinäkyviä, osallistavia ja tukevat vastuullista kaupunkikehitystä sekä päätöksentekoa. Vastuullinen päätöksenteko palvelee myös älykaupunkien kehittämistä, sekä takaavat hyvän pohjan mahdolliselle tulevaisuuden kasvulle.

5 YHTEENVETO

Kasvavan teknologisen kehityksen myötä, yhä useammasta kaupungista tulee tulevaisuudessa älykaupunki, jossa teknologiaa hyödynnetään jo olemassa olevan perinteisen infrastruktuurin kanssa (Batty ym., 2012). Älykaupunkien merkitys tulee kasvamaan entisestään myös tulevaisuudessa, sillä kaupunkien keräämä data tulee vaikuttamaan yhä useamman yksilön elämään tavalla tai toisella. Älykaupunkien hyödyntämä teknologia altistaa yksilöt monille riskeille alttiiksi, sillä emme ymmärrä vielä aivan täysin kuinka hyödyntää teknologiaa vastuullisesti, taaten samalla otolliset olosuhteet innovatiiviselle kehitykselle ja kasvulle.

Tutkielmassa tarkasteltiin älykaupungin käsitettä ja siihen liittyvää datanhallintaa, erityisesti keskittyen yksityisyydensuojaan ja tietoturvaan. Älykaupungin toiminnassa otettiin tarkasteluun myös esineiden internet (engl. Internet of Things tai IoT). Tutkielmassa pyrittiin käsittelemään tällä hetkellä toteutettavia ratkaisuja siihen, miten älykaupungeissa eri teknologioiden tuomiin riskeihin sekä konflikteihin voidaan vastata kattavasti. Lisäksi tutkielmassa listattiin älykaupungeissa esiintyviä riskejä ja konflikteja, sekä niiden mahdollistajia.

Yksi tutkielman kannalta keskeisistä oletuksista oli, että älykaupungit keräävät jatkuvasti suuria määriä dataa eri lähteistä. Battyn ja kumppaneiden (2012) mukaan data on välttämätöntä kaupunkipalvelujen kehittämisen kannalta. Kuitenkin suurten datamäärien kerääminen tuo mukanaan erilaisia riskejä, kuten tietovuodot, tietoturvaloukkaukset ja yksityisyydensuojan loukkaukset (Mayer & Baeumner, 2019). Tutkielma osoitti, että nämä riskit voivat luoda merkittäviä riskejä yhteiskunnalle, sillä älykaupunkien keräämä data on hyvin sensitiivistä.

Tutkielman tulokset korostavat myös turvallisten tietosuojakäytäntöjen tärkeyttä (Sinaeepourfard ym., 2016). Tutkielma osoitti myös, että esimerkiksi salausprotokollat, turvalliset viestintäkanavat ja valvottu pääsy sensitiivisiin tietoihin voivat auttaa estämään tietoturva- sekä yksityisyysloukkauksia. Zhang ym. (2017) mukaan lisäksi kansalaisten tietoisuuden lisääminen yksityisyydensuojasta ja tietoturvasta on olennainen osa toimivien älykaupunkien kehittämistä. Tutkielman pohjalta voidaan todeta tärkeäksi tekijäksi yksilöiden ymmärtävän miten heidän tietojaan käytetään. Tutkielman tuloksissa nousi

jatkuvasti esille yhteisöllisyys sekä päätöksenteon läpinäkyvyys. Nämä seikat ovat merkittävässä roolissa pitämässä luottamusta yllä älykaupungeissa tapahtuvan päätöksenteon suhteen.

Tutkielman tuloksissa tulee ilmi, että vaikka älykaupunkien tarjoamat teknologiset innovaatiot voivat merkittävästi parantaa kaupunkien toimintaa ja kehitystä, ne edellyttävät myös ajankohtaisia käytäntöjä sekä vastuullista päätöksentekoa. Eckhoffin ja Wagnerin (2018) mukaan salaus ja tietojen anonymisointi ovat keskeisiä työkaluja, jotka auttavat suojaamaan yksityisyyttä ja varmistamaan, että data pysyy luottamuksellisena. Näiden protokollien lisäksi älykaupungit voivat hyödyntää monikerroksisia tietoturvakehyksiä, jotka käsittävät datanhallinnan, teknologian ja eri käyttöjärjestelmien väliset suhteet (Dong ym., 2018).

Yksi tutkielman kannalta merkittävistä johtopäätöksistä on kuitenkin todeta, että älykaupungeissa esiintyy lukematon määrä erilaisia konflikteja ja riskejä. Tutkielman pohjalta voidaan myös mainita, että niiden ratkaisemiseksi on olemassa hyvin suuri joukko erilaisia protokollia, suojausmekanismeja sekä käytäntöjä. Emme voi siis olettaa konflikteihin löytyvän helposti mitään yhtä oikeaa ratkaisua, vaan niiden lievittämiseksi tulee harjoittaa pitkäjänteisesti monipuolisia menetelmiä.

Tutkielmassa löydettyjä tuloksia voidaan soveltaa tulevaisuudessa osana vastuullista älykaupunkisuunnittelua ja teknologian inhimillistä kehitystä. Turvalliset tiedonsiirtokäytännöt, datan ylikeräyksen estäminen ja kansalaisten suostumuksen varmistaminen ovat konkreettisia toimia, joita voidaan hyödyntää älykaupunkien riskien vähentämiseksi myös tulevaisuudessa.

Tutkielman perusteella tulevissa tutkimuksissa voisi olla hyvä syventyä datanhallintaan ja erityisesti siihen, kuinka dataa voidaan turvallisesti säilyttää ja käsitellä sen koko elinkaaren ajan. Lisäksi tulevaisuuden tutkimuksissa voitaisiin tutkia esineiden internetin laitteiden turvallisuutta ja kehittää parempia protokollia niiden suojaamiseksi erilaisilta haavoittuvuuksilta, sillä erilaisia internetin välityksellä toimivia laitteita ilmaantuu yhä enemmän ihmisten keskuuteen tulevaisuudessa. Kansalaisten tietoisuuden lisääminen tietoturvasta ja yksityisyydensuojasta voisi myös olla yksi jatkotutkimuksen aiheista, sillä sen avulla voidaan parantaa merkittävästi luottamusta älykaupunkien ja sen kansalaisten välillä.

Huomioitavaa arvioidessa tämän tutkielman tuloksia on muistaa, että tutkielma on suoritettu kirjallisuuskatsauksena, eikä jokaiselle väitteelle löydy aivan yksimielistä selitystä. Aihealueen ollessa suhteellisen laaja, lähdemateriaaleissa toistuvien aiheiden määrittely poikkeaa toisistaan myös jonkin verran. Tutkielmassa on käytetty lähinnä tietojärjestelmätieteen sekä informaatioteknologian alan lähteitä, joten poikkeavuuksia muiden alojen tutkielmien kanssa saattaa esiintyä tiettyjä aihealueita käsiteltäessä. Kuitenkin tulee muistaa se, että teknologiset termit ja käsitteet elävät jatkuvasti, ja ne tulevat kehittymään tulevaisuudessa. Tulevaisuuden kannalta tutkielma antaa kuitenkin hyviä näkökulmia tutkia aihetta lisää ja hieman tarkemmista sekä rajatummista näkökulmista.

LÄHTEET

Alawadhi, S., & Scholl, H. J. (2016). Smart governance: A cross-case analysis of smart city initiatives. 49th Hawaii international conference on system sciences (HICSS), 2953-2963. IEEE.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G., & Portugali, Y. (2012). Smart cities of the future. *The European Physical Journal Special Topics*, *214*(1), 481–518.

Bartolozzi, M., Bellini, P., Nesi, P., Pantaleo, G., & Santi, L. (2015, December 1). A Smart Decision Support System for Smart City. IEEE.

Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. Sustainable Cities and Society, 39, 499–507.

Caviglione, L., Lalande, J.-F., Mazurczyk, W., & Wendzel, S. (2015). Analysis of Human Awareness of Security and Privacy Threats in Smart Environments. Lecture Notes in Computer Science, 165–177.

Carli, R., Dotoli, M., & Pellegrino, R. (2016). A hierarchical decision-making strategy for the energy management of smart cities. IEEE Transactions on Automation Science and Engineering, 14(2), 505-523.

Christofi, A., Heyman, R., Vandercruysse, L., Verdoodt, V., Buts, C., Dooms, M., ... & Valcke, P. (2019). Smart city privacy: Enhancing collaborative transparency in the regulatory ecosystem. CTTE-FITCE: Smart Cities & Information and Communication Technology (CTTE-FITCE), 1-5. IEEE.

Cofta, P. (2008). Confidence-compensating privacy protection. Sixth Annual Conference on Privacy, Security and Trust, 65-74. IEEE.

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. IEEE access, 6, 46134-46145.

Edwards, L. (2016). Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. European Data Protection Law Review (EDPL), 2, 28.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of Advanced Research, 5(4), 491–497.

Fabrègue, B. F. G., & Bogoni, A. (2023). Privacy and Security Concerns in the Smart City. Smart Cities, 6(1), 586–613.

Fang, W., Cui, N., Chen, W., Zhang, W., & Chen, Y. (2020). A trust-based security system for data collection in smart city. IEEE Transactions on Industrial Informatics, 17(6), 4131-4140.

Finch, K., & Tene, O. (2018). Smart Cities: Privacy, Transparency, and Community (E. Selinger, J. Polonetsky, & O. Tene, Eds.). Cambridge University Press; Cambridge University Press.Saumya, C. (2015). Components of Enterprise Information Management. *Apress EBooks*, 15–24.

Frugoli, J., Etgen, A. M., & Kuhar, M. (2010). Developing and Communicating Responsible Data Management Policies to Trainees and Colleagues. Science and Engineering Ethics, 16(4), 753–762.

Gokul, N. B., & Sankaran, S. (2020). Identity Based Security Framework For Smart Cities. 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 1-4. IEEE.

Guarda, P., & Zannone, N. (2009). Towards the development of privacy-aware systems. Information and Software Technology, 51(2), 337-350.

Hansen, M., Jensen, M., & Rost, M. (2015, May 1). Protection Goals for Privacy Engineering. IEEE.

Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Information Systems Frontiers, 24.

Joshi, M., & Krag, S. S. (2010). Issues in Data Management. Science and Engineering Ethics, 16(4), 743–748.

Kirimtat, A., Krejcar, O., Kertesz, A., & Tasgetiren, M. F. (2020). Future Trends and Current State of Smart City Concepts: A Survey. IEEE Access, 8, 86448–86467.

Kitchen, R., & Dodge, M. (2020). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. Smart cities and innovative Urban technologies, 47-65. Routledge.

Koh, C. E., & Watson, H. J. (1998). Data management in executive information systems. Information & Management, 33(6), 301-312.

Koo, Y. D., & Kwon, O. Y. (2017). A Trend Analysis of Smart City Technology Development. Applied Mechanics and Materials, 872, 425-429.

Koshy, A. S., Fatima, N., Alankar, B., Kaur, H., & Chauhan, R. (2021). Security and Privacy Issues in Smart Cities. Transforming the Internet of Things for Next-Generation Smart Systems, 64-75.

Kunzmann, K. (2014). SMART CITIES: A NEW PARADIGM OF URBAN DEVELOPMENT. Haettu 12.4.2024 osoitteesta https://www.carocci.it/files/riviste/digitali/01_kunzmann.pdf.

Kuzlu, M., Kalkavan, H., Gueler, O., Zohrabi, N., Martin, P. J., & Abdelwahed, S. (2022). An End to End Data Collection Architecture for IoT Devices in Smart Cities: 2022 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2022. 2022 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2022.

Li, Y., Dai, W., Ming, Z., & Qiu, M. (2016). Privacy Protection for Preventing Data Over-Collection in Smart City. IEEE Transactions on Computers, 65(5), 1339–1350.

Liu, X., Heller, A., & Nielsen, P. S. (2017). CITIESData: a smart city data management framework. Knowledge and Information Systems, 53(3), 699–722.

Ma, M., Preum, S. M., Tarneberg, W., Ahmed, M., Ruiters, M., & Stankovic, J. (2016). Detection of runtime conflicts among services in smart cities. IEEE International Conference on Smart Computing (SMARTCOMP), 1-10. IEEE.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675.

Mayer, M., & Baeumner, A. J. (2019). A Megatrend Challenging Analytical Chemistry: Biosensor and Chemosensor Concepts Ready for the Internet of Things. Chemical Reviews, 119(13), 7996–8027.

Mosenia, A., & Jha, N. K. (2017). A Comprehensive Study of Security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586–602.

Moshenchenko, M., Zhurakovskyi, B. (2021). Information protection in "smart city" technologies. Cybersecurity: Education, Science, Technique, 3(11), 100–109.

Qu, Y., Nosouhi, M. R., Cui, L., & Yu, S. (2019). Privacy preservation in smart cities. In Smart cities cybersecurity and privacy, 75-88. Elsevier.

Radziszewska, A. (2023). Data-Driven Approach in Knowledge-Based Smart City Management. European Conference on Knowledge Management, 24(2), 1090–1098.

Renaud, K., & Gálvez-Cruz, D. (2010). Privacy: Aspects, definitions and a multi-faceted privacy preservation approach. Information Security for South Africa, 1-8. IEEE.

Ridley, M. N., & Stoker, C. (2001). Data Management Tools. OSTI OAI (U.S. Department of Energy Office of Scientific and Technical Information).

Risteska, B., Stojkoska, L., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140(3), 1454–1464.

Saumya, C. (2015). Components of Enterprise Information Management. Apress EBooks, 15–24.

Sinaeepourfard, A., Garcia, J., Masip-Bruin, X., Marin-Tordera, E., Yin, X., & Wang, C. (2016). A data lifeCycle model for smart cities. In 2016 international conference on information and communication technology convergence (ICTC), 400-405. IEEE.

Sylla, T., Mohamed Aymen Chalouf, Krief, F., & Karim Samaké. (2020). Towards a Context-Aware Security and Privacy as a Service in the Internet of Things. Lecture Notes in Computer Science, 240–252.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Wagner, I., & Eckhoff, D. (2018). Technical Privacy Metrics: a Systematic Survey. ACM Computing Surveys, 51(3), 1–38.

Wang, P., Ali, A., & Kelly, W. (2015). Data security and threat modeling for smart city infrastructure. 2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC), 1-6. IEEE.

Whitmore, A., Agarwal, A., & Da Xu, L. (2014). The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 17(2), 261–274.

Witti, M., & Konstantas, D. (2018). A Secure and Privacy-preserving Internet of Things Framework for Smart City. Proceedings of the 6th International Conference on Information Technology: IoT and Smart City - ICIT 2018.

Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart City Development in Taiwan: From the Perspective of the Information Security Policy. Sustainability, 12(7), 2916.

Yuan, M., Chen, L., & Yu, P. S. (2010). Personalized privacy protection in social networks. Proceedings of the VLDB Endowment, 4(2), 141–150.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. IEEE Communications Magazine, 55(1), 122–129.

Zoonen, L. (2016). Privacy concerns in smart cities. Government Information Quarterly, 33(3), 472–480.