Aleksi Heiskanen

ÄLYKKÄIDEN TIELIIKENNEJÄRJESTELMIEN HAASTEET JA NIIDEN RATKAISEMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Heiskanen, Aleksi
Älykkäiden tieliikennejärjestelmien haasteet ja niiden ratkaiseminen
Jyväskylä: Jyväskylän yliopisto, 2023, 38 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Riekkinen, Janne

Liikenteellä on suuri merkitys lähes jokaisen ihmisen elämälle ympäri maailmaa. Sen sujuvoittamiseen kehitetään jatkuvasti uusia teknisiä ratkaisuja, joista yhtenä ajankohtaisimpana voidaan pitää erilaisten älykkäiden järjestelmien hyödyntämistä. Uusien teknologioiden käyttöön voi kuitenkin liittyä monenlaisia haasteita. Tässä tutkielmassa pyrittiin selvittämään, millaisia nämä haasteet ovat älykkäiden tieliikennejärjestelmien osalta, ja miten kyseisiin haasteisiin voidaan vastata.

Tutkielma toteutettiin kirjalliskatsauksena hyödyntäen pääosin vertaisarvioituja tieteellisiä julkaisuja 2010- ja 2020-luvuilta. Tutkielman ensimmäisessä sisältöluvussa käytiin läpi liikenteenohjauksen ja ajoneuvojen automaatioon liittyvä teknologiaa, kuten koneoppimisen kaltaisia erilaisia tekoälymenetelmiä. Tämän jälkeen toisessa sisältöluvussa siirryttiin tarkastelemaan itse tutkimusongelmaa, eli esitellyn tieliikenneteknologian haasteita kyberturvallisista, eettisistä ja lainsäädännöllisistä näkökulmista. Kolmannessa eli viimeisessä sisältöluvussa puolestaan jatkettiin tutkimusongelman käsittelyä etsimällä erilaisia ratkaisukeinoja esiteltyihin haasteisiin.

Tutkielmassa havaittiin, että tieliikenteen älyjärjestelmiin liittyy monenlaisia haasteita. Olennaisiksi ongelmiksi nousivat erilaiset kyberhyökkäykset, kerätyn datan epäeettinen käyttö, moraalien noudattaminen itseohjautuvien ajoneuvojen osalta, sekä nykyisten tieliikennelainsäädäntöjen ristiriidat ajoneuvojen automaation kanssa. Ehdotettuja ratkaisuja olivat muun muassa erilaisten tietoturvamenetelmien implementointi osaksi älykkäitä liikennejärjestelmiä, datan käsittelyn läpinäkyvyyden lisääminen esimerkiksi lainsäädännön kautta, itseohjautuvien ajoneuvojen käytöksen rajoittaminen erilaisilla moraaliviitekehyksillä, sekä nykyisten lainsäädäntöjen selventäminen ajoneuvojen automaation osalta.

Tutkielman aiheen laajuuden vuoksi tutkielmassa kyettiin käymään läpi vain pieni osa erilaisista älykkäistä tieliikennejärjestelmistä ja niiden haasteista. Tutkimuksen ulkopuolelle jääneitä aihealueita olivat muun muassa esineiden internet ajoneuvoissa sekä sosiaalisten ja taloudellisten haasteiden läpikäynti. Informaatioteknologian alan ollessa jatkuvassa muutoksessa, on myös osa käytetystä lähdemateriaalista ollut mahdollisesti jo vanhentunutta tutkielmaa kirjoitettaessa. Mahdollista jatkotutkimusta ajatellen olisikin olennaista, että aihepiiriä rajattaisiin tarkemmin ja käytettäisiin tuoreempaa lähdemateriaalia, jotta tutkimuksesta saataisiin tarkempaa ja kattavampaa.

Asiasanat: tekoäly liikenteessä, ajoneuvojen automaatio, adaptiiviset liikennevalot, tekoälyn haasteet, liikenteen kyberturvallisuus

ABSTRACT

Heiskanen, Aleksi
The challenges of intelligent road transport systems and overcoming them
Jyväskylä: University of Jyväskylä, 2023, 38 pp.
Information Systems Science, Bachelor's Thesis
Supervisor: Riekkinen, Janne

This thesis aimed to explore the challenges intelligent road transport systems may face, and how they could be addressed. The thesis was conducted as a literature review, utilizing various peer-reviewed scientific publications from the 2010s and 2020s. The thesis' second chapter examined various technologies associated with the automation of vehicles and traffic management. The third chapter covered the challenges of the presented road transportation technologies, from the standpoints of cybersecurity, ethics, and legislation. Lastly, the fourth chapter handled the research problem by finding ways to address the presented challenges.

The challenges of transportation technologies identified in this study included various cyber-attacks, the misuse of collected user data, the implementation of moral standards for self-driving vehicles and the incompatibility of current road legislation with high level vehicle autonomy. Some of the proposed solutions for these challenges were, for example, the implementation of various cyber security methods for intelligent systems, the increase of data collection transparency, setting up moral constraints for vehicle behavior, and clarifying current road laws regarding autonomous vehicles.

Given the extensiveness of the topic, only a small portion of all the possible intelligent road transport systems and their challenges could be covered. And due to how rapidly the field of IT tends to change, some of the material used in this thesis may already have been outdated by the time of writing. To improve the coverage and accuracy of possible future research, the scope should be tightened, and more attention should be paid to the age of the material.

Keywords: artificial intelligence in transportation, vehicle automation, adaptive traffic lights, challenges of artificial intelligence, cyber security of transportation

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Liikenne on laaja ja meidän jokapäiväistä elämäämme koskettava käsite. Tyypillisesti liikenteellä tarkoitetaan ihmisten ja tavaroiden liikuttamista paikasta toiseen joko maalla, merellä tai ilmassa. Liikenteen eri muotoja on monia, mutta kaikelta liikenteeltä löytyy kolme yhdistävää elementtiä: ajoneuvot, erilaisten reittien, kuten maanteiden tai kiskojen, hyödyntäminen, sekä liikenteen kohtauspaikat, niin sanotut ”terminaalit”, vaikkapa parkkihalli tai tienristeys (Hall, 2003, s. 2). Yhtenä yhdistävänä tekijänä näiden kolmen elementin lisäksi voisi jossain määrin pitää myös tietynlaista tehokkuuteen pyrkimistä. Liikenteessä usein pyrkimyksenä on liikutella suurehkojakin ihmis- ja tavaramääriä mahdollisimman nopeasti ja pienellä vaivalla, ja tämän vuoksi onkin käynnissä jatkuva pohdinta siitä, miten liikennettä voisi tehostaa entisestään. Yhtenä ajankohtaisena esimerkkinä liikenteen tehostamisen keinoista voisi olla erilaisten älykkäiden liikennejärjestelmien hyödyntäminen.

Kuten aiemmin määritelty liikennekin, on myös älykkyys käsitteenä suhteellisen laaja. Tietotekniikan kontekstissa puhuttava älykkyyden käsite, niin sanottu ”tekoäly”, voi olla kuitenkin liikenteen käsitettä jokseenkin haastavampi määriteltävä. Tekoälyn määrittelyyn on olemassa monia eri lähestymistapoja, mutta ehkä yksi tärkeimmistä ja tunnetuimmista menetelmistä määritellä tekoäly on matemaatikko Alan Turingin vuonna 1950 esittämä Turingin testi. Russellin ja Norvigin (2009) tekoälyä käsittelevän kirjan mukaan testissä jokin kone asetetaan vastaamaan sille laadittuihin kysymyksiin, ja näin saatujen vastausten luonteen perusteella pyritään päättelemään, onko kysymyksiin vastannut kone vai ihminen. Testi koetaan läpäistyksi, jos koneen antamat vastaukset kävisivät ihmisen antamista. Testin läpäistäkseen tarvitsisi kone ihmismäistä ”ajattelua” ja käyttäytymistä, eli tekoälyn voisi siis ajatella olevan ihmismäisen ajattelun ja älykkyyden jäljittelemistä keinotekoisen, elottoman objektin toimesta (Russell & Norvig, 2009, s. 1–2).

Tekoälyn käyttömahdollisuudet liikenteessä ovat laajat. Tekoälyä voidaan soveltaa niin ajoneuvoissa, liikenteen kulun hallinnassa kuin Hallin (2003, s. 2) mainitsemissa terminaaleissakin. Tekoälyn hyödyntämisellä voidaan mahdollisesti vähentää ihmisten tekemän työn määrää, säästäen resursseja ja käytön

luonteesta riippuen myös parantaen turvallisuutta. Esimerkiksi automatisoiduissa henkilöajoneuvoissa tekoälyn avulla voidaan vähentää matkustusaikaa ja polttoaineen kulutusta valitsemalla optimaalisin ajoreitti, tai ylläpitämällä turvallista ajoetäisyyttä muihin ajoneuvoihin liikenteessä (Iyer, 2021).

Älykkään teknologian hyödyntäminen liikenteen kontekstissa ei kuitenkaan ole ongelmatonta. Vaikka teknologian käytön lisääminen voikin auttaa esimerkiksi vähentämään inhimillisten virheiden riskiä, voi se tuoda mukanaan myös teknologialle itselleen tyypillisiä haasteita, kuten tietoturvaongelmat ja erilaiset vikaantumiset. Liikenneonnettomuudet ovat yksi suurimmista kuolinsyistä maailmanlaajuisesti (World Health Organization [WHO], 2020), joten kaikkeen teknologiaan, joka voi osaltaan nostaa liikenneonnettomuuksien riskiä, olisi järkevää suhtautua erityisen vakavasti. Liikenne sitoo myös suuren määrän rahaa muun muassa ajoneuvojen, vakuutusten ja infrastruktuurin muodossa, joten mahdollisten rahallisten vahinkojen minimointi on sekin tärkeä näkökohta liikenteeseen sovellettavan uuden teknologian tarkastelussa. Älykkääseen liikenneteknologiaan liittyy lisäksi myös omat lailliset ja eettiset haasteensa, esimerkiksi nykyisten tieliikennelakien yhteensopivuuden varmistaminen älyteknologian kanssa, tai henkilökohtaisten tietojen eettinen käsittely älykkäiden liikennejärjestelmien, kuten automatisoitujen autojen, toimesta (Maurer ym., 2016). Jotta erilaisiin uhkatekijöihin voitaisiin vastata, täytyy ne kyetä ensin tunnistamaan ja määrittelemään. Tämän vuoksi onkin erityisten tärkeää, että aiheesta tehdään myös tieteellistä tutkimusta.

Tämän kandidaatintutkielman tarkoituksena on pureutua edellä mainittujen näkökohtien kaltaisiin ongelmiin, eli selvittää, millaisia riskejä ja haasteita älykkäisiin liikennejärjestelmiin voi käytännössä liittyä, ja miten niihin voidaan pyrkiä vastaamaan. Käsite ”älyteknologia” on todellisuudessa vielä tekoälyä laajempi aihealue, kattaen tekoälyn lisäksi myös esimerkiksi esineiden internetin, mutta tämän tutkielman tarkoituksena on tarkastella lähinnäkin tekoälyyn ja automaatioon liittyvää teknologiaa. Vaikka tutkielmassa pyritään keskittymään lähinnä tekoälyn negatiivisiin puoliin, ei tarkoituksena ole kuitenkaan maalata uhkakuvia uuden teknologian vaaroista, vaan tuoda esille rakentavia ratkaisumahdollisuuksia. Innokkuus uusien teknologioiden tuomista mahdollisuuksista voi helposti peittää alleen mahdollisten varjopuolten pohdinnan, ja koenkin tämän vuoksi tärkeäksi, että myös vähemmän miellyttäviä näkökulmia tutkitaan.

Kyseinen aihepiiri valikoitui tutkielman käsittelemäksi aiheeksi aiemmissa kappaleissa mainittujen syiden sekä tutkielman kirjoittajan oman mielenkiinnon vuoksi. Tekoäly ja älykkäät järjestelmät ovat tietotekniikan aiheena yhteyksissä myös tietojärjestelmätieteeseen, tehden aihepiiristä sopivan tutkimusaiheen alan tutkimusta varten. Tekoälyn suosion voidaan nähdä myös olevan jatkuvassa kasvussa, eli aihetta on mielekästä tutkia myös sen ajankohtaisuuden vuoksi.

Liikenteen ja älykkäiden järjestelmien ollessa hyvin laaja kokonaisuus aihepiirinä, keskitytään tässä tutkielmassa vain tieliikenteessä käytettyihin älykkäisiin järjestelmiin, erityisesti ajoneuvojen ja liikenteenohjauksen automaation teknologiaan. Tutkimuksen käsittelemä tutkimusongelma voidaan muotoilla kahteen tutkimuskysymykseen:

- Mitä haasteita ja riskejä liittyy älykkäisiin tieliikennejärjestelmiin?
- Miten älykkäisiin tieliikennejärjestelmiin liittyviin haasteisiin ja riskeihin voidaan pyrkiä vastaamaan?

Tutkielma on luonteeltaan kirjallisuuskatsaus, eli sen tarkoituksena ei ole luoda uutta empiiristä tietoa, vaan koota ja yhdistellä aiempaa tutkimusta aiheeseen liittyen. Informaatioteknologian alan ollessa jatkuvassa muutoksessa koin tärkeäksi, että tutkielman käyttämä materiaali olisi mahdollisimman tuoretta, joten tutkielman käyttämä materiaali on pääasiassa 2010- ja 2020-lukujen tutkimusta, muutamaa vanhempaa käsitteiden selittämiseen liittyvää lähdettä lukuun ottamatta. Julkaisuajankohdan lisäksi materiaalia valitessani kiinnitin huomiota muihinkin tyypillisesti luotettavuuteen vaikuttaviin tekijöihin, kuten julkaisujen viittausten määrään sekä Julkaisufoorumi-sivuston antamiin luokituksiin. Käytetyt lähteet koostuvat pääosin vertaisarvioiduista, vähintään 1. luokituksen Julkaisufoorumilta saaneista tieteellisistä julkaisuista sekä tutkimukselle olennaisesta kirjallisuudesta. Tutkimusmateriaali etsittiin erilaisia tieteellisten julkaisujen hakupalveluita ja -tietokantoja, muun muassa Google Scholaria, JYKDOKia sekä Scopusta hyödyntäen. Hakuehtoina käytettiin erilaisia yhdistelmiä muun muassa seuraavanlaisista tutkimukselle olennaisista sanoista: *artificial intelligence*, *transportation*, *risks*, *challenges*, *vehicle automation*, *traffic*, *problems*, *machine learning*, *adaptive traffic control*, *neural networks*. Materiaalin hakeminen tehtiin englanniksi, koska englannin kielen käyttäminen mahdollisti laajemmat ja monipuolisemmat hakutulokset kuin suomen kielen käyttäminen, englannin kielen ollessa informaatioteknologialle olennaisin kieli.

Tutkielma noudattaa tyypillistä kandidaatintutkielman rakennetta, eli se sisältää tiivistelmän, johdannon, sisältöluvut ja yhteenvedon. Seuraavassa eli toisessa luvussa perehdytään älyteknologian käyttöön tieliikenteessä, eli esitellään aihepiiriä tarkemmin. Luvussa kolme puolestaan pyritään etsimään, mitä haasteita ja riskejä luvussa kaksi esiteltyihin käyttötapoihin liittyy, eli siirrytään tarkastelemaan aihepiiriä tutkimusongelman näkökulmasta. Luvussa neljä jatketaan tutkimusongelman käsittelyä, eli pyritään löytämään ratkaisutapoja luvussa kolme havaittuihin ongelmiin tekoälyyn liittyen. Lopuksi yhteenvetoluvussa kootaan yhteen aiempien sisältölukujen päähavainnot, ja tehdään niistä tarvittavat johtopäätökset.

2 ÄLYKKÄIDEN JÄRJESTELMIEN HYÖDYNTÄMINEN TIELIIKENTEESSÄ

Erilaisia älyteknologioita voidaan hyödyntää liikenteessä monin tavoin. Tekoälyä voidaan pitää, kuten johdannossa jo määriteltiinkin, ihmismäisen käytöksen ja älykkyyden jäljittelynä, liikenteen ollessa puolestaan tavaroiden ja ihmisten liikuttelua paikasta toiseen. Tieliikenne koostuu laajasta joukosta monimutkaisia järjestelmiä, joten tekoälyn tuoman ihmismäisen, monitahoisen ongelmanratkaisukyvyn yhdistämistä konemaiseen toistettavuuteen ja automaatioon voidaan pitää loogisena ratkaisuna moniin liikenteen pulmiin. Tämän luvun tarkoituksena on syventyä kyseiseen aiheeseen tarkemmin, eli esitellä tekoälyä sen eri alikuntien kautta, ja miten tekoälyä voidaan soveltaa tieliikenteen kontekstissa.

2.1 Liikenteenohjaus ja -hallinta

Yksi älyteknologioiden käyttöalueista tieliikenteessä on liikenteenohjaus ja -hallinta. Liikenteenohjauksen ja -hallinnan pyrkimyksenä on esimerkiksi havaita ja ennakoida onnettomuuksia ja mahdollistaa mahdollisimman ruuhkaton liikenteen sujuvuus (Mandal ym., 2020). Liikenteenohjaukseen liittyy paljon suunnittelua ja päätöksentekoa siitä, miten liikenteen kulkua voidaan tehostaa ja ylläpitää. Tämän toteuttamista varten tarvitaan liikennedataa, jota voidaan kerätä erilaisia sensoreita ja kameroita hyödyntäen (Kumarage ym., 2018).

Datan käsittely ja siten liikenteen hallinnointi manuaalisesti on kuitenkin ihmistyöntekijöille hyvin kuormittavaa. Samanaikaisesti tarkkailtavana olevia ajoneuvoja voi olla valtavia määriä, joten esimerkiksi automaation lisäämisellä voi olla suuri positiivinen vaikutus työn kuormittavuuden ja inhimillisten virheiden vähentämisessä (Mandal ym., 2020). Biologisilla aivoilla on vain rajallinen kapasiteetti, ja niiden tehokas toiminta on luonnollisten tarpeiden, kuten unen ja ravinnon saannin, varassa. Koneilla ei sen sijaan ole vastaavia rajoitteita, joten ne kykenevät toimimaan tehokkaammin vastaavanlaisissa työtehtävissä.

Yksi keskeisimmistä tekoälyn osa-alueista on niin sanottu koneoppiminen. Koneoppiminen on nimensä mukaisesti jonkin koneen toimesta tapahtuvaa ”oppimista”; konetta ”harjoitetaan” syöttämällä sille dataa, jonka perusteella se luo ennakoivia malleja, joiden mukaan toimia (Zhou, 2021, s. 2–4). Näin ollen mitä tuoreempaa ja todenmukaisempaa dataa koneelle syötetään, sitä parempia myös koneen luomat mallit ovat.

Koneoppimisen piiriin kuuluu myös muita tekoälyn alikuntia, kuten neuroverkot ja syväoppiminen (International Business Machines Corporation [IBM], 2023). Graupe (2013) kertoo neuroverkkojen jäljittelevän biologisia aivoja, kuten ihmisaivoja, pyrkimällä simuloimaan neuronien eli hermosolujen välistä päätöksentekoprosessia. Tällä menettelyllä voidaan ajatella olevan useita hyötyjä. Siinä missä monien tavallisten koneiden toiminta voi kaatua yhden komponentin pettämiseen, ei tällaista ongelmaa välttämättä esiinny neuroverkkojen kohdalla. Tämä johtuu Graupen (2013) mukaan siitä, että neuroverkkojen yksittäisillä neuroneilla ei ole suurta merkitystä koneen kokonaistoiminnan kannalta, minkä ansiosta koneen viansietokyky kasvaa. Neuroverkot ovat myös hyvin skaalautuvia, sillä neuroverkkojen laskennallisen monimutkaisuuden voidaan ainakin teoriassa ajatella myötäilevän käsiteltävien ongelmien monimutkaisuutta (Graupe, 2013, s. 1–3).

Syväoppiminen on vahvasti sidoksissa edellä mainittuihin neuroverkkoihin, sillä sen voidaan ajatella olevan neuroverkkojen alikunta (IBM, 2023). Erona syväoppimisen ja neuroverkkojen välillä voidaan pitää niiden rakennetta: neuroverkot koostuvat tyypillisesti kolmesta eri neuronikerroksesta, kun taas syväoppimisen kohdalla kerroksia voi olla huomattavasti enemmän (Zhou, 2021, s. 15). IBM:n (2023) mukaan nämä lisäkerrokset mahdollistavat kolmea kerrosta tehokkaamman ja laajemman kyvyn ”oppia”, minkä vuoksi syväoppimisen avulla voidaan luoda tarkempia malleja kuin pelkkiä neuroverkkoja käyttäen. Syväoppimisen monimutkaisuuden vuoksi kuitenkin myös tarvittavan prosessointitehon määrä kasvaa (IBM, 2023).

Koneoppimisen sekä sen kautta myös neuroverkkojen ja syväoppimisen kyky luoda ennakoivia malleja tekee niistä hyvin soveltuvia muun muassa onnettomuuksien ja liikenteen kulun arvioimiseen (Abduljabbar ym., 2019). Tästä esimerkkinä voidaan pitää esimerkiksi Doganin ja Akgüngörin (2013) laatimaa tutkimusta junaliikenteen lisäämisen vaikutuksista tieliikenteen onnettomuuksien määrään. Tutkimuksessa erilaisille ennustusmalleille syötettiin ensin dataa Turkissa tapahtuneista liikenneonnettomuuksista ja loukkaantumisista 27 vuoden ajalta, minkä jälkeen mallien avulla saatuja tuloksia vertailtiin toisiinsa. Tutkimuksessa havaittiin, että neuroverkkoja hyödyntäneet mallit suoriutuivat ennustamisessa tehokkaammin kuin vertailukohteena toimineet usean muuttujan epälineaarisen regressioanalyysin (nonlinear multiple regression) mallit. Käytettyjen mallien avulla saatiin selville, että junaliikenteen käytön lisäämisellä oli tieliikenneonnettomuuksien määrää vähentävä vaikutus, eli tutkimuksen perusteella neuroverkkoja voidaan onnistuneesti soveltaa liikenteen käyttäytymisen ennustamiseen (Dogan & Akgüngör, 2013).

Onnettomuuksien määrän arvioinnin lisäksi neuroverkkojen avulla voidaan pyrkiä havaitsemaan myös itse onnettomuuksia. Lu ym. (2012) tutkimuksessa selvitettiin, miten neuroverkkoja voidaan yhdistää osittaisen pienimmän neliösumman (Partial Least Squares, PLS) metodiin liikenneonnettomuuksien havainnoinnissa. Tutkimuksessa PLSNN-mallille (PLS + neuroverkot, NN) annettiin alankomaalaisen moottoritien liiketunnistussensorien keräämää dataa onnettomuuspaikoista, käytetyistä ajokaistoista sekä onnettomuuksien kestosta. Tutkimuksessa havaittiin, että vaikka PLSNN-menetelmää käyttämällä niin sanottujen väärien hälytysten määrä kasvoi hieman, saavutettiin kyseisellä menetelmällä kuitenkin huomattavasti suurempi onnettomuuksien havaitsemisnopeus kuin vain PLS-metodia käyttäen (Lu ym., 2012). Näin ollen voidaan tehdä johtopäätös, että neuroverkkoja voidaan onnistuneesti hyödyntää liikenneonnettomuuksien havainnoinnissa, ja että eri menetelmiä yhdistämällä on mahdollista saavuttaa mieluisampia tuloksia kuin yksittäisillä menetelmillä.

Älyteknologioista voi olla apua myös tieliikenteen sujuvoittamiseen. Ruuhkien vähentämisestä on mahdollista saada huomattavaa hyötyä, sillä Boukerche ym. (2020) tutkimuksen mukaan vuonna 2000 Yhdysvaltojen 75 suurimmassa kaupungissa käytettiin arviolta noin 3,6 miljardia tuntia tieliikenneruuhkissa, joissa kulutettiin yli 21 miljardia litraa polttoainetta. Boukerche ym. (2020) kertovat, että ruuhkien vähentämiseen ja tieliikenteen sujuvoittamiseen voidaan käyttää erilaisia ennakoivia tai reaaliaikaisia toimenpiteitä. Ennakoiviin keinoihin kuuluu esimerkiksi liikenteestä kerätyn datan analysointi ja käyttäminen erilaisissa mallinnuksissa, kun taas reaaliaikaisia, suoria keinoja ovat muun muassa adaptiiviset liikennevalot, ruuhkien havaitseminen ja liikenteen kulun hallinta (Boukerche ym., 2020).

Esimerkkinä edellä mainituista ennakoivista menetelmistä voidaan pitää Mandal ym. (2020) tutkimuksessa esitettyä liikennedatan analysointia. Mandal ym. (2020) tutkimuksessa testattiin liikkuvien ja paikallaan olevien ajoneuvojen havaitsemista sekä niiden lukumäärän laskemista syöttäen liikennekameroiden tallentamaa kuvaa muun muassa Faster R-CNN-, YOLO- ja CenterNet-syväoppimisalgoritmeille, jotka erikoistuvat kohteiden tunnistamiseen. Tutkimuksessa havaittiin, että käytetyt kohteentunnistusalgoritmit kykenivät havaitsemaan ajoneuvojen liikennejonoja yli 90 % tarkkuudella, vaikkakin esimerkiksi auringonpaiste ja kohteiden kaukaisuus häiritsivät kohteentunnistuksen tehokkuutta (Mandal ym., 2020). Tällaisella liikennedatan analysoinnilla voisi olla mahdollista sujuvoittaa liikenteen kulkua, jos sitä hyödynnettäisiin liikenteenohjauksessa yhdessä reaaliaikaisten toimenpiteiden, kuten adaptiivisten liikennevalojen, kanssa.

Ruuhkaantumisen vähentämiseen ja ajoneuvojen reittien optimointiin voidaan hyödyntää myös useita niin sanotun parviälyn (Swarm Intelligence) muotoja, kuten Ant Colony Optimisation (ACO) ja Bee Colony Optimisation (BCO), jotka ottavat mallia luonnosta muun muassa hyönteisten ruoanetsimiskäyttäytymisestä (Abduljabbar ym., 2019). Esimerkiksi muurahaiset jättävät ruokaa etsiessään jälkeensä feromoneja, jotka houkuttelevat muita muurahaisia samalle reitille, vahvistaen entisestään saman reitin valintaa (Ahmed & Glasgow, 2012).

Vastaavanlaista käytöstä voidaan havaita myös ihmisten kohdalla, sillä sosiaalisena lajina ihmisten on usein tapana hakeutua sinne, missä on muitakin ihmisiä.

Qureshin (2013) mukaan toinen reittioptimoinnin menetelmä, sumean logiikan malli (Fuzzy Logic Model), kykenee puolestaan arvioimaan tekijöitä, jotka vaikuttavat saatavilla olevien reittivaihtoehtojen kulkuun käytettyyn aikaan, ja siten valitsemaan sopivimman reittivaihtoehdon. Sumea logiikka perustuu nimensä mukaisesti niin sanottujen ”sumeiden” vaihtoehtojen tarkasteluun, eli kun vaihtoehtoja ei voida luokitella karkeasti esimerkiksi muodossa ”tosi” tai ”epätosi”, vaan ne ovat jotain siltä väliltä (Qureshi ym., 2013). Parviälyn tapaan myös sumeaa logiikkaa voidaan hyödyntää liikenneruuhkien vähentämisessä, sillä kuten Abduljabbar ym. (2019) kirjallisuuskatsauksessa todettiin, ne soveltuvat etenkin dynaamisiin liikennetilanteisiin liittyvien ongelmien ratkaisemiseen. Tällainen dynaaminen liikennetilanne voisi olla vaikkapa sopivimman reitin valitseminen tilanteessa, jossa pituudeltaan lyhyin reitti ei kuitenkaan ole välttämättä nopein reitti, esimerkiksi reitillä olevan tietyömaan vuoksi.

Kuten aiemmin jo mainittiinkin, yhtenä tieliikenteen sujuvoittamisen reaaliaikaisista toimenpiteistä voidaan pitää adaptiivisten liikennevalojen käyttöä. Adaptiiviset liikennevalot vaihtelevat valojen vaihtumisen tiheyttä reaaliaikaisesti sen perusteella, kuinka paljon liikennettä sattuu olemaan, siinä missä perinteisten liikennevalojen kohdalla valojen vaihtuminen tapahtuu vakiovälein (Wagner, 2016). Vakiovälein tapahtuvan valojen vaihtumisen ongelmana voidaan pitää sen joustamattomuutta, sillä liikenteen määrän ollessa suuri voi liikennevalojen mukautumattomuus johtaa ruuhkien syntymiseen.

Adaptiivisissa liikennevaloissa voidaan hyödyntää useita eri tekoälymenetelmiä. Wang ym. (2016) tutkimuksessa luotiin NeverStop-niminen järjestelmä, joka hyödynsi sumeaa logiikkaa ja geneettisiä algoritmeja liikennesensoreilta kerätyn datan kanssa. Geneettisillä algoritmeilla tarkoitetaan algoritmeja, jotka ottavat mallia luonnossa esiintyvästä, sukupolvelta toiselle tapahtuvasta biologisesta perinnästä, yhdistettynä mahdollisiin luonnollisiin mutaatioihin (Lambora ym., 2019). Wang ym. (2016) tutkimuksen NeverStop-järjestelmä kykeni vähentämään ajoneuvojen liikennevaloissa odottamiseen käyttämää keskivertoaikaa huomattavasti verrattuna perinteisiin liikennevaloihin. Tämä saatiin aikaan muuttamalla valojen vaihtumisen tiheyttä automaattisesti sensorien keräämän datan perusteella. NeverStop-järjestelmä suoriutui ajoneuvojen liikennevaloihin saapumisen nopeudesta riippuen 20–50 % tehokkaammin kuin tavalliset liikennevalot (Wang ym., 2016). Tästä voidaan päätellä, että adaptiivisilla liikennevaloilla voi olla huomattava merkitys ruuhkautumisen vähentämisessä.

2.2 Ajoneuvojen automaatio

Ajoneuvojen automaatiota voidaan pitää kenties kaikkein ilmeisimpänä tekoälyn käyttökohteena älykkäistä tieliikennejärjestelmistä puhuttaessa. Itseohjautuvien ajoneuvojen konsepti ei sinänsä ole kovinkaan uusi asia, esimerkiksi itseohjautuvia metrojunia on ollut käytössä jo 1960-luvulta asti, mutta erityisesti

itseohjautuvien henkilöajoneuvojen teknologia on ollut vahvassa nousussa lähivuosikymmeninä (Yagdereli ym., 2015). Erilaisia automatisoivia älyominaisuuksia on nykyään havaittavissa jo edullisempienkin hintaluokkien henkilöautoissa, ja niiden hyödyntämisen odotetaan lisääntyvän lähitulevaisuudessa vielä entisestään (Yagdereli ym., 2015).

Ajoneuvojen automaatiosta puhuttaessa voi helposti syntyä kärjistetty mielikuva, jossa ajoneuvot eritellään joko perinteisiin, ihmisten ohjaamiin autoihin, tai täysin automatisoituihin robottiautoihin. Todellisuus on kuitenkin hieman moniulotteisempi, sillä henkilöautojen automaation voidaan ajatella koostuvan eri tasoista. Automaation tason voidaan ajatella nousevan ajamista automatisoivien järjestelmien kasaantuessa, eli mitä pidemmälle automaatio viedään, sitä pienempi rooli kyydissä olevilla henkilöillä on ajoneuvon ohjaamisen suhteen. Oheinen taulukko (taulukko 1) kuvaa hyvin tätä vaiheittaisuutta, eli miten tieliikenneajoneuvojen automaatio pystytään jakamaan porrastetusti viiteen eri tasoon (Yagdereli ym., 2015).

Levels of Autonomy	Existing Examples	
1. Driver only	The vehicle is entirely under human control but may have some automated systems.	Cruise control; electronic stability control; anti-lock brakes.
2. Driver assistance	The steering and/or acceleration are automated but the driver must control the other functions.	Adaptive cruise control: distance to car in front maintained; Pparking assistant: steering is automated, driver controls accelerator and brakes.
3. Partial autonomy	The driver does not control steering or acceleration but is expected to be attentive at all times and take back control instantaneously when required.	Adaptive cruise control with lane keeping.; Ttraffic jams assistance.
4. High autonomy	Vehicles are able to operate autonomously for some portions of the journey. Transfer of control back to the human driver when a warning happens. Similar to cruise control systems employed today's cars.	Oxford's Robot car project and, early prototypes of Google's Driverless Car which allows a human driver to take control of the car by stepping on the brake or turning the wheel.
5. Full autonomy	The vehicle is capable of driving unaided for the entire journey with no human intervention, potentially without a human in the car.	Driverless cars, which have no steering wheel, gas pedal, or brakes; 100% autonomous.

TAULUKKO 1 Tieliikenneajoneuvojen automaation vaiheittaisuus (Yagdereli ym., 2015)

Oheisen taulukon (taulukko 1) esittelemät viidennen tason täysin automatisoidut henkilöautot ovat vielä toistaiseksi korkeintaan prototyyppivaiheessa, mutta tasojen yhdestä kolmeen luokiteltuja osittain automatisoituja ajoneuvoja on saatavilla markkinoilla jo laajalti. Erilaisia älyteknologiaa hyödyntäviä ominaisuuksia, joita voidaan kutsua yläkäsitteellä Advanced Driver Assistance Systems (ADAS), ovat muun muassa erilaiset mukautuvat vakionopeudensäätimet (Adaptive Cruise Control, ACC), navigointijärjestelmät, pysäköintiavustimet sekä kaistanhallintajärjestelmät (Yagdereli ym., 2015; Hasan ym., 2020; Amoozadeh ym., 2015). Näiden ominaisuuksien toiminta perustuu laitteiston, kuten erilaisten

sensorien ja kameroiden, sekä näiltä saatavaa dataa käsittelevien ohjelmistojen, yhteistyöhön.

ACC:t ovat toiminnaltaan hyvin samanlaisia kuin perinteiset vakionopeudensäätimet (Cruise Control, CC). Shaoutin & Jarrahin (1997) mukaan CC lukitsee ajonopeuden joko mekaanisesti tai ohjelmistoa käyttäen haluttuun määrään ja pitää sen siellä, kun taas ACC säätelee ajonopeutta edessä kulkevan ajoneuvon mukaisesti. ACC:n ohjelmisto käyttää ajoneuvon kameroilta saatavaa dataa ajonopeuden säätämiseen, mutta ne eivät kuitenkaan aina hyödynnä tekoälyä. Milanesin (2013) tutkimuksen mukaan Cooperative Adaptive Cruise Control (CACC) on puolestaan edistynyt versio mukautuvasta vakionopeudensäätimestä. Milanes (2013) kertoo, että ACC:n ottaessa huomioon vain edellä ajavan ajoneuvon, muodostaa CACC ajoneuvojen verkon, joka kattaa muut ympärillä olevat ajoneuvot sekä mahdollisesti myös jonossa kauempana sijaitsevat ajoneuvot. Nämä verkottuneet ajoneuvot (Connected Vehicle) viestivät oman sijaintinsa toisilleen langattomasti (ajoneuvolta ajoneuvolle, Vehicle-to-Vehicle, V2V) sijainnistaan, auttaen ylläpitämään turvallista etäisyyttä ja välttämään yhteentörmäyksiä (Milanes ym., 2013).

3 ÄLYKKÄIDEN TIELIIKENNEJÄRJESTELMIEN HAASTEET JA RISKIT

Älyteknologioiden käyttö tuo mukanaan monia hyötyjä ja mahdollisuuksia. Edellisessä luvussa käytiin läpi, millaisin eri tavoin esimerkiksi tekoälyä voidaan hyödyntää tieliikenteen eri käyttökohteissa, kuten liikenteenhallinnassa ja henkilöautoissa.

Hyötyjen tavoin myös mahdollisia haittoja ja riskejä on monia. Kyberhyökkäyksen kohteeksi joutumisen riski on lähes aina läsnä tietotekniikkaa hyödynnettäessä, ja teknisillä laitteilla on luonnostaan taipumusta myös erilaisille teknisille vioille. Tällaisten ongelmien ilmetessä vilkkaassa tieliikenteessä voivat mahdolliset seuraamukset olla kohtalokkaita, sillä erilaiset tieliikenneturmat ovat yksi suurimmista kuolinsyistä ympäri maailmaa (WHO, 2020). Tekniikkaan liittyvien haasteiden lisäksi kenties vähemmän ilmeisiä haittoja ovat myös erilaiset eettiset ja lailliset ongelmat, kuten henkilökohtaisten tietojen väärinkäyttö ja lainsäädännön yhteensopivuus itseohjautuvien ajoneuvojen kanssa.

Tämän luvun tarkoituksena on syventyä edellä mainitun kaltaisiin ongelmiin, eli millaisia kyberturvallisia, eettisiä sekä laillisia haasteita ja riskejä älykkäisiin tieliikennejärjestelmiin voi liittyä.

3.1 Kyberhyökkäykset

Eräs ilmeisimmistä uhkista, joita älyteknologiaan ja tietotekniikkaan yleensäkin liittyy, ovat erilaiset tietoturvaongelmat, eli haavoittuvuus kyberhyökkäyksille. Yagdereli ym. (2015) kertovat tutkimuksessaan, että kyberhyökkäykset voidaan karkeasti jakaa passiivisiin ja aktiivisiin hyökkäyksiin. Tutkimusen mukaan passiiviset hyökkäykset, kuten salakuuntelu (eavesdropping) ja liikenteen analysointi (traffic analysis) ovat nimensä mukaisesti passiivisia, eli hyökkääjä ei osallistu suoraan datan muuttamiseen vaan tyytyy salaa keräämään hyökkäyskohteen tietoja erilaisia haavoittuvaisuuksia hyödyntäen. Aktiiviset hyökkäykset, kuten palvelunestohyökkäykset (Denial-of-Service, DoS) ja viestien muokkaus

(message modification), ovat puolestaan passiivisia hyökkäyksiä aggressiivisempia, eli niissä hyökkääjä tunkeutuu muokkaamaan tai uudelleenohjaamaan dataa, aiheuttaen häiriötä ja mahdollisesti vahinkoa hyökkäyskohteelle (Yagdereli ym., 2015).

Tieliikenteessä kyberhyökkäysten kohteena voivat olla esimerkiksi automatisoidut ajoneuvot sekä liikenteenohjauksen järjestelmät (Khatoun & Zeadally, 2017). Automatisoiduissa ajoneuvoissa alttiina ovat erityisesti ajoneuvojen kommunikaatiojärjestelmät, esimerkiksi laajalti käytetty Controller Area Network (CAN) -väylä. Pöyhösen (2019) mukaan CAN-väylä on automaatioväylä, jota käytetään datan reaaliaikaiseen siirtämiseen ajoneuvon järjestelmien välillä, esimerkiksi ABS-jarruille tai moottorin ohjausyksikölle. Väylä on altis mahdollisille hyökkäyksille, sillä sen viestintä on viiveettömyytensä vuoksi todentamatonta (Pöyhönen ym., 2019). Automatisoitujen ajoneuvojen ollessa täysin niiden sensorien ja ohjelmiston toiminnan varassa, voi hyökkäys CAN-väylään lamauttaa koko ajoneuvon.

Kommunikaatiojärjestelmiin kohdistuvia hyökkäyksiä ovat tärkeitä huomioitavia etenkin verkottuneiden ajoneuvojen kohdalla. CAN-väylän viestintä tapahtuu enimmäkseen fyysisesti, joten etähyökkäykset sitä kohtaan vaativat hyökkääjältä suhteellisen paljon vaivannäköä. Koscher ym. (2010) tutkimuksen mukaan ajoneuvojen fyysisiin yhteyksiin kohdistuvien hyökkäysten tulisi tapahtua joko kytkemällä fyysinen laite suoraan ajoneuvoon, tai hyökkäämällä ajoneuvoon langattomasti yhdistettyjen laitteiden kautta, jotta hyökkäys onnistuisi. Fyysisten yhteyksien voidaan siis ajatella olevan langattomia yhteyksien haastavampia hyökkäyskohteita. Verkottuneiden ajoneuvojen toiminta perustuu pitkälti nimenomaan langattomaan viestintään ajoneuvon ympäristön, eli pääosin muiden ajoneuvojen, kanssa, mikä tekee etähyökkäyksistä todennäköisesti helpompia toteuttaa.

Amoozadeh ym. (2015) tutkimuksessa kerrotaan, että verkottuneita ajoneuvoja kohtaan on mahdollista hyökätä sekä passiivisesti että aktiivisesti, ja hyökkäysten laajuus voi kattaa useita verkkoon kuuluvia ajoneuvoja. Tutkimuksen mukaan hyökkääjä voi esimerkiksi kerätä tietoa ajoneuvojen sijainnista, ylikuormittaa kommunikaatioyhteyksiä DoS-hyökkäyksillä tai syöttää vanhentunutta tietoa edellä olevan ajoneuvon nopeudesta. Näistä jälkimmäisen tapainen skenaario voi olla jopa hengenvaarallinen, sillä se voi johtaa verkkoon kuuluvien ajoneuvojen yhteentörmäyksiin (Amoozadeh ym., 2015).

Amoozadeh ym. (2015) tutkimuksessa suoritettiin tähän liittyen simulaatiokoe, jossa simuloitiin verkottuneiden ajoneuvojen välisen kommunikaation häirintää VENTOS-nimisen simulaatioalustan avulla. Simuloidut viestin väärentämishyökkäys ja radiosignaalin häirintä kykenivät horjuttamaan hyökättyjen ajoneuvojen verkon vakautta, hidastaen ajoneuvojen reaktionopeutta ja vaikuttaen niiden väliseen turvaväliin. Ajoneuvojen yhteyden kasvanut viive ja sen aiheuttama reaktionopeuden heikkeneminen on huomattavan vaarallinen erityisesti kiihdytystilanteissa, joissa perässä kulkevan ajoneuvon kykenemättömyys reagoida riittävän nopeasti edessä olevan ajoneuvon ajonopeuden muutokseen voi johtaa peräänajoon.

Erilaiset ajoneuvoihin kohdistuvat hyökkäykset voivat siis olla mahdollisesti hyvinkin vahingollisia liikenneturvallisuudelle, mutta myös liikenteenohjauksen järjestelmät ovat alttiita erilaisille hyökkäyksille. Nämä hyökkäykset ovat hyvin samankaltaisia kuin aiemmin mainitut ajoneuvoihin kohdistuvat hyökkäystyypit; muun muassa datan muokkaaminen ja kerääminen sekä DoS-hyökkäykset ovat mahdollisia (Arabi ym., 2021).

Kyseisten hyökkäysten kohteena voivat olla esimerkiksi adaptiiviset liikennevalot, jotka käyttävät reaaliaikaisesti saatua liikennedataa hyväkseen valojen vaihtumisen säätelyssä. Verkottuneiden ajoneuvojen tapaan myös adaptiivisille liikennevaloille voidaan syöttää esimerkiksi vanhentunutta tai muokattua dataa, mikä vaikuttaa negatiivisesti liikennevalojen tehokkaaseen vaihtumiseen (Arabi ym., 2021). Adaptiivisten liikennevalojen tarkoituksena on optimoida liikenteen kulkua vähentämällä ajoneuvojen hukkaan menevää odotteluaikaa liikennevaloissa. Kun liikennevalot saavat vääränlaista dataa, voi seurauksena olla tiekapasiteetin ylikuormittuminen ja ruuhkautuminen.

Chen ym. (2018) tutkimuksessa selvitettiin datanväärennyshyökkäysten vaikutusta sellaisiin liikennejärjestelmiin, joissa adaptiiviset liikennevalot ja verkottuneet ajoneuvot toimivat yhdessä. Tutkimuksessa analysoitiin ensiksi Yhdysvaltain liikenneministeriön tukeman Intelligent Traffic Signal System (I-SIG) -nimisen liikenteenohjausjärjestelmän tietoturvaheikkouksia ja mahdollisia siihen kohdistuvia hyökkäyksiä, minkä jälkeen kyseisiä hyökkäyksiä pyrittiin simuloimaan todenmukaista liikennedataa käyttäen (Chen ym., 2018).

Sekä tehty analyysi että simulaatiot osoittivat, että kyseiset hyökkäykset voivat heikentää liikenteen sujuvuutta tai jopa lamauttaa sen: liikenteen kulku oli hyökkäysten seurauksena jopa 23,4 % heikompaa verrattuna tavallisiin liikennevaloihin, ja ajoneuvot joutuivat käyttämään pahimmillaan jopa 14 kertaa enemmän aikaa liikenteessä olemiseen (Chen ym., 2018). Näiden havaintojen perusteella voidaan tehdä johtopäätös, että kyberhyökkäykset liikenteenohjausjärjestelmiä vastaan voivat osoittautua niiden laajojen vaikutustensa vuoksi jopa vahingollisemmiksi kuin yksittäisiin ajoneuvoihin kohdistuvat hyökkäykset. Kyberhyökkäysten mahdollisesti aiheuttamilla ruuhkilla ja turhalla odottamisella voi olla esimerkiksi merkittäviä taloudellisia seuraamuksia. Turhaan kulutetun polttoaineen lisäksi liikenneruuhkat aiheuttavat viivästyksiä toimitusketjuihin, ja säännölliset ruuhkautumiset voivat johtaa esimerkiksi taloudellisesti epäoptimaalisten reittien valintaan ja jopa yritysten toimipaikkojen vaihtumiseen (Sweet, 2011).

3.2 Eettiset ongelmat

Älyteknologioiden käyttöön voi liittyä monenlaisia eettisiä ongelmia. Leslie (2019) esittää kirjassaan, että useat tekoälyyn liittyvät eettiset ongelmat ovat yhteydessä datan epäeettiseen käyttöön. Leslien mukaan dataa voidaan esimerkiksi kerätä ja käyttää luvatta, ja kerättyä luottamuksellista dataa voidaan käsitellä virheellisesti tai huolimattomasti. Dataan liittyvien eettisten haasteiden lisäksi

Leslie (2019) nostaa esille myös esimerkiksi tekoälyn hyödyntämisestä johtuvan sosiaalisen vuorovaikutuksen vähentymisen ja siitä seuraavat sosiaaliset ja yhteiskunnalliset vaikutukset, sekä vastuussa olevan tahon määrittelemisen heikentyminen ongelmatapauksissa, kuten loukkaantumissa, tekoälyn käytön myötä (Leslie, 2019).

Älyteknologian käyttöön liittyvät eettiset ongelmat ulottuvat myös tieliikenteeseen. Linin (2016) mukaan yksi perinteinen liikenteeseen liittyvä eettinen dilemma on niin sanottu vaunuongelma (englanniksi trolley problem), jossa henkilön täytyy tehdä valinta siitä, muuttaako hän raitiovaunun kulkuraidetta, kun vaihtoehtoiseen raiteen valitseminen merkitsisi kuolonuhrien vähenemistä. Tällaiset ongelmat, joissa kaikista haitallisista vaihtoehdoista täytyisi valita vähiten haitallisin, ovat liikenteessä harvinaisia, mutta silti mahdollisia (Lin, 2016). Jos itseohjautuva, ilman kuljettajaa toimiva ajoneuvo joutuisi tällaisen dilemman eteen, voi herätä kysymys, että miten ajoneuvon tulisi toimia tilanteessa. Jotta ajoneuvon tekoäly voisi valita vähiten haitallisimman vaihtoehdon, tulisi sen siis olla kykenevä moraaliseen päätöksentekoon. Tämä ajoneuvon moraalikäsitys voi olla haasteellista toteuttaa, sillä eettisiin kysymyksiin on harvoin vain oikeita ja vääriä vastauksia, ja päätöksentekoon vaikuttavien tekijöiden määrä voi olla ylivoimaista jopa ihmisellekin.

Toinen ajoneuvon automaatioon liittyvä eettinen ongelma piilee osittaisen automaation tuomasta kuljettajan valppauden heikentämisessä (Wolf, 2016). Ajoneuvon automaation tarkoituksena on auttaa kuljettajaa, eli vähentää ajamiseen tarvittavaa työtä. Wolfin (2016) mukaan tässä piilee kuitenkin riski siitä, että ajoneuvon kuljettaja oppii luottamaan automaation antamiin apukeinoihin. Kuljettajan valppaus heikkenee, ja jos esimerkiksi äkillinen tekninen vika poistaa apukeinot käytöstä, ei kuljettaja välttämättä pysty enää tarpeeksi nopeaan päätöksentekoon. Periaatteessa kuljettajalla on velvollisuus huolehtia ajoneuvon hallinnasta, mutta toisaalta on ymmärrettävää, että arvaamattomiin muutoksiin ajotottumuksissa voi olla haastavaa sopeutua äkillisesti kesken ajotilanteen (Wolf, 2016).

Müllerin ja Zaltan (2021) mukaan tieliikenteeseen liittyviin eettisiin ongelmiin voi kuulua myös oman edun tavoitteleminen liikennesääntöjen sekä muiden ihmisten kustannuksella, esimerkiksi ajamalla ylinopeutta, jotta matkan päämäärä saavutettaisiin nopeammin. Müller ja Zalta (2021) kertovat, että mahdolliset automatisoidut ajoneuvot, jotka kykenevät operoimaan itsenäisesti ilman kuljettajaa, ohjelmoidaan tyypillisesti noudattamaan liikennesääntöjä ja siten muun muassa turvallisia ajonopeuksia ja ajoneuvojen ohituskäytäntöjä. Jos tätä ohjelmointia kuitenkin muutettaisiin, esimerkiksi palvelemaan omistajan omia intressejä, voisi tällainen itseohjautuva ajoneuvo teoriassa rikkoa liikennesääntöjä ja aiheuttaa mahdollisesti vahinkoa (Müller & Zalta, 2021).

Näiden eettisten haasteiden lisäksi myös aiemmin mainitut datan keräämiseen liittyvät eettiset riskit koskettavat tieliikennettä. Kumfer ym. (2016) tutkimuksen mukaan automatisoidut ajoneuvot tarvitsevat monenlaista dataa toimiakseen, joista osa voi olla peräisin ajoneuvon matkustajista. Kumfer ym. (2016) kertovat, että esimerkiksi automatisoidut taksit tai yritysten työsuhdeautot

voivat kerätä arkaluontoista dataa, kuten kotiosoitteita, lukuisista eri matkustajista pitkiltäkin aikaväleiltä. Tämän datan varastoinnissa ja käytössä on omat riskinsä, sillä datan luottamuksellisesta ja asianmukaisesta käytöstä ei välttämättä ole täydellisiä takeita, eli dataan käsiksi pääsemistä voidaan jo itsessään pitää eettisenä ongelmana (Kumfer ym., 2016).

3.3 Lailliset ongelmat

Teknologian kehittyminen ja lainsäädännölliset uudistukset tapahtuvat usein käsi kädessä, ja merkittävien teknologisten mullistusten kohdalla poliittinen väliintulo voi olla jopa välttämätöntä. Esimerkiksi kryptovaluuttojen nousu on johtanut rajuihinkin lainsäädännöllisiin muutoksiin, kuten Kiinassa vuonna 2021 laadittuun kryptovaluuttakieltoon (Griffith, 2023). Schreursin ja Steuwerin (2016) mukaan lainsäädännöllisten uudistusten lisäksi muutoksia voi esiintyä myös muun muassa lisensoinnissa sekä rahallisen ja poliittisen tuen määrissä ja kohteissa. Poliitikot voivat pyrkiä esimerkiksi edistämään tietynlaiseen teknologiaan liittyvää lainsäädäntöä, jos kyseinen teknologia koetaan hyödylliseksi sen hetkisten poliittisten linjausten kanssa (Schreurs & Steuwer, 2016). Tällaiseksi voidaan ajatella vaikkapa Euroopassa tapahtuvaa vihreän teknologian saaman tuen lisäämistä valtiollisten tahojen toimesta ilmastonmuutoksen torjumisen toimenpiteenä (European Environment Agency, 2019).

Schreursin ja Steuwerin tutkimuksen mukaan tieliikenteen automaatioon liittyvä lainsäädäntö on saanut maailmalla, erityisesti Euroopassa, tähän mennessä hyvin vähän huomiota. Tutkimuksessa kerrotaan. että Euroopan unionin tieliikenteen tulevaisuuteen liittyvän lainsäädännön painopisteenä on ollut pääasiassa ilmastonmuutoksen torjuminen ja siihen liittyvä teknologia, ja vaikka automaation lisääminen voi osaltaan auttaa tässäkin, ei asian selvittämiseen ole toistaiseksi käytetty paljoa vaivannäköä. Tieliikenteen automaation lainsäädäntö on kuitenkin ollut esillä useissa Yhdysvaltojen osavaltioissa, kuten Nevadassa ja Kaliforniassa (Schreurs & Steuwer, 2016).

Gasser (2016) kertoo tutkimuksessaan, että vaikka tieliikenteeseen liittyvä lainsäädäntö vaihteleekin maittain, voi tieliikenteen automatisoinnin kenties keskeisimmäksi ongelmaksi kiteyttää yleisen oletuksen siitä, että ajoneuvojen ohjaamisesta vastaa aina elävä ihminen, ja että kuljettajalla on velvollisuus pysyä valppaana liikenteessä. Eri maiden tämänhetkiset lainsäädännöt nojautuvat lähes täysin tähän olettamukseen, eli nykyisellään voimassa olevat tieliikennelait eivät joko juurikaan ota kantaa itseohjautuviin ajoneuvoihin, tai ne ovat ristiriidassa automatisoitujen ajoneuvojen kanssa kuljettajan valppauden suhteen (Gasser, 2016). Tämänhetkisten tieliikenneajoneuvojen automaation matalan tason vuoksi lakien muuttamiselle ei ole välttämättä ollut vielä akuuttia tarvetta, mutta ajoneuvojen automaatioon liittyvä teknologia kehittyy jatkuvasti. Tulevaisuudessa tieliikenteessä voidaan nähdä jopa täysin itsenäisesti ohjautuvia ajoneuvoja, jolloin lainsäädäntöä joudutaan todennäköisesti uudistamaan tavalla tai toisella.

Automatisoitujen ajoneuvojen kohdalla onnettomuuksissa ja liikennerikkomuksissa vastuussa olevien tahojen määritteleminen voi olla hankalaa. Gasserin (2016) tutkimuksen mukaan osittain automatisoidun ajoneuvon hallinta, kuten ajokurssin korjaavien liikkeiden suorittaminen, on loppujen lopuksi kuljettajan vastuulla, joten tällaisten ajoneuvojen kohdalla ei välttämättä löydy ristiriitoja nykyisten lainsäädäntöjen kanssa. Tutkimuksessa kerrotaan, että sen sijaan esimerkiksi täysin automatisoidut joukkoliikenteen ajoneuvot tai taksit voivat osoittautua haastavammiksi tapauksiksi, sillä niiden voidaan olettaa pystyvän ohjautumaan ilman matkustajan suoraa väliintuloa. Liikenteessä tapahtuvien mahdollisten ongelmien kohdalla voi olla epäselvää, kuka tai ketkä ovat lopulta laillisesti vastuussa. Gasserin (2016) mukaan tällaisia ongelmia voivat olla liikennesääntöjen rikkomiset, liikenneonnettomuudet tai vaikkapa tekniset viat. Automaation tason kasvaessa kuitenkin myös valmistajan vastuun määrä nousee. Valmistajan vastuu raukeaisi vain sellaisissa tilanteissa, joissa ajoneuvon käyttäjät ovat rikkoneet tieliikennelakeja tai ajoneuvon ominaisuuksille asetettuja käyttöohjeita (Gasser, 2016). Jotta mahdollisia tulkinnanvaraisuuksia ei syntyisi, tulisi näiden käyttöohjeiden olla selkeästi määriteltyjä.

Färberin (2016) tutkimuksen mukaan edellä mainittujen haasteiden lisäksi esimerkiksi liikennesääntöjen noudattaminen täysin automatisoitujen ajoneuvojen toimesta voi osoittautua hankalaksi, sillä liikenteeseen liittyy usein tietynlaista improvisaatiota, jota ajoneuvon tekoäly ei välttämättä kykene ymmärtämään ja soveltamaan. Esimerkiksi liikennepoliisin käsin viittomalla, suullisilla käskyillä ja kehon eleillä suorittaman liikenteen ohjaamisen noudattaminen voi osoittautua tekoälyn ohjaamalle ajoneuvolle liian haastavaksi, varsinkin jos liikennetilanteessa vallitsevissa olosuhteissa on epäselvyyksiä esimerkiksi huonon näkyvyyden tai kuuluvuuden vuoksi (Färber, 2016). Ihmisten välinen kommunikaatio on loppujen lopuksi hyvin monimutkaista, eikä tekoälyä hyödyntävillä ajoneuvoilla välttämättä koskaan tule olemaan kykyä ymmärtää tätä kokonaisvaltaisesti.

4 ÄLYKKÄIDEN TIELIIKENNEJÄRJESTELMIEN HAASTEISIIN JA RISKEIHIN VASTAAMINEN

Edellisessä kappaleessa esitellyt riskit ja haasteet älykkäisiin tieliikennejärjestelmiin liittyen ovat hyvin moninaisia, sillä eettiset, lailliset ja kyberturvallisuuteen liittyvät ongelmat ovat luonteeltaan hyvin erityyppisiä. Älykkäiden tieliikennejärjestelmin hyödyntäminen on myös pitkälti vasta alkuvaiheessa, ja monet tässä tutkielmassa esitellyt älyteknologioiden käyttökohteet, kuten täysin automatisoidut ajoneuvot, ovat vasta konseptitodistuksen tasolla. Tämä teknologinen keskeneräisyys tekee myös mahdollisten ratkaisujen löytämisestä haastavaa, sillä erilaisia ratkaisutapoja tulisi esimerkiksi pystyä testaamaan käytännön tasolla. Erityisesti tieliikenteen teknologiasta puhuttaessa tulisi testauksen olla hyvin perusteellista, jotta laajoilta ja mahdollisesti vakavilta lisäongelmilta vältyttäisiin. Lisäksi esimerkiksi eettisyyteen liittyviin haasteisiin voi olla haastavaa löytää selkeästi määriteltäviä ratkaisuja, sillä eettisiin pulmiin on harvoin olemassa vain oikeita ja vääriä vastauksia.

Moniin älykkäiden tieliikennejärjestelmien ongelmiin on kuitenkin jo olemassa suhteellisen pienellä vaivalla toteutettavissa olevia ratkaisuja, joista osaa sovelletaan käytännön tasolla jo tällä hetkellä. Tämän luvun tarkoituksena on tuoda esille, millaisia ratkaisutapoja voidaan pyrkiä soveltamaan edellisessä kappaleessa esiteltyihin haasteisiin ja riskeihin.

4.1 Kyberturvalliset ratkaisut

Vaikka älykkäät tieliikennejärjestelmät ovatkin osoittaneet vakavia haavoittuvuuksia tietoturvan suhteen, ovat monet kyberhyökkäykset pysyneet luonteeltaan yllättävänkin samankaltaisina vuosikymmenien ajan (Khatoun & Zeadally, 2017). Tämän vuoksi hyökkäyksiin kohdistuvia tietoturvatoimia ei välttämättä tarvitse lähteä kehittelemään täysin tyhjästä, minkä voidaan nähdä helpottavan huomattavasti uusien, tehokkaampien tietoturvatoimien kehittelyssä. Monet nykyäänkin käytössä olevat tietoturvatoimet ovat sellaisenaan riittäviä suojatoimia,

jos niitä sovelletaan tilanteeseen sopivasti tieliikennekäytössä (Yagdereli ym., 2015).

Yagdereli ym. (2015) laatiman tutkimuksen mukaan automatisoitujen ajoneuvojen erilaisten tietoturvatoimien tulisi täyttää vaatimukset viiden tietoturvalle olennaisen osa-alueen kannalta:

- Luottamuksellisuus (confidentiality): tietoa jaetaan vain tahoille, joilla on tietoon lupa
- Datan yhtenäisyys / johdonmukaisuus (data integrity / consistency): datan tarkkuus ja alkuperäisyys säilytetään taholta toiselle
- Todennus (authentication): tietoa käsittelemään pyrkivien tahojen oikeellisuus varmistetaan
- Saatavuus (availability): tietoa ollaan valmis jakamaan ajasta ja paikasta riippumatta
- Kiistämättömyys (non-repudiation): Tahojen antamia allekirjoituksia ja muita todennuksia ei pystytä väärentämään tai kiistämään

Näiden vaatimusten perusteella luotaisiin tietoturvan pohja, ja vaikka Yagdereli ym. (2015) tutkimus otti nämä vaatimukset esille nimenomaan ajoneuvojen tietoturvan kontekstissa, voidaan niitä pitää sen verran yleistasoisina, että niiden periaatteita kyettäisiin soveltamaan muuhunkin tieliikenteeseen, kuten adaptiivisiin liikennevaloihin. Esimerkiksi Stallingin (2017) kirja kryptografiasta ja nettiturvallisuudesta ottaa esille useita samoja Yagdereli ym. (2015) mainitsemia tietoturvavaatimuksia, kuten varmennuksen ja luottamuksellisuuden. Stallingin (2017) kirjan käsitellessä aihetta yleistasoisesti, voidaan olettaa, että nämä kyberturvallisuuden piirteet ovat sovellettavissa myös laajamittaisemmin useissa tietotekniikan käyttökohteissa.

Yagdereli ym. (2015) tutkimuksessa eriteltiin tietoturvaratkaisuehdotuksia myös hieman konkreettisemmin. Yhtenä päähuomiona tutkimuksessa nousi ajoneuvojen tietojärjestelmien hajauttaminen. Hajauttamisen periaatteena olisi se, että vaikka ajoneuvoon kohdistuva hyökkäys kykenisi lamauttamaan jonkin tietyn järjestelmän, voisi ajoneuvo kuitenkin jatkaa toimintaansa ainakin kriittisten ominaisuuksien, kuten pysäköimisen, osalta (Yagdereli ym., 2015).

Eräs toinen Yagdereli ym. (2015) tutkimuksen mainitsema tietoturvaa parantava ominaisuus, joka sekin liittyy hajauttamiseen, olisi viestiyhteyksien määrän kasvattaminen siten, että sama viesti lähetetään aina useamman kanavan kautta. Tutkimuksen mukaan tällöin kaikista kanavista suurimman osan tulisi sisältää täsmälleen sama viesti, jotta viestiä voitaisiin pitää todenmukaisena ja voimassa olevana. Jos jokin viesti tulisi esimerkiksi vain yhden kanavan kautta, määriteltäisiin kyseinen viesti hylätyksi, ja tämän seurauksena ajoneuvon järjestelmät asetettaisiin ”turvatilaan” mahdollisen hyökkäyksen pysäyttämiseksi (Yagdereli ym., 2015).

Yagdereli ym. (2015) tutkimuksen ehdottamia tietoturvavaatimuksia myötäileviä toimenpiteitä on esitetty useissa muissakin tutkimuksissa. Amoozadeh ym. (2015) esittävät verkottuneita ajoneuvoja käsittelevässä tutkimuksessaan

esimerkiksi ajoneuvojen sensoreille asetettavia parametreja, joiden avulla määriteltäisiin, millaiset sensorin havaitsemat arvot ovat normaalin rajoissa. Tutkimuksen mukaan sensorin havaitessa asetettujen parametrien ulkopuolisia arvoja, esimerkiksi vian tai kyberhyökkäyksen vuoksi, voidaan kyseiset arvot jättää huomioimatta tai hylätä. Amoozadeh ym. (2015) ehdottavat myös mahdollisten vaihtoehtoisten sensorien antaman datan hyödyntämistä, jos pääasiallinen sensori on vioittunut tai hyökkäyksen kohteena. Esimerkkinä tästä annettiin ajoneuvon moottorin sensorien käyttäminen, kun ajoneuvon renkaan nopeusanturi on vioittunut tai hyökkäyksen kohteena (Amoozadeh ym., 2015).

Petitin ja Shladoverin (2015) tutkimus automatisoituihin ajoneuvoihin kohdistuvista kyberhyökkäyksistä on sekin samoilla linjoilla edellä mainittujen Yagdereli ym. (2015) ja Amoozadeh ym. (2015) ehdotusten kanssa. Vääränlaisten arvojen ja käytöksen tunnistamisen lisäksi tutkimuksessa ehdotetaan käytettäväksi erilaisia varmennusmenetelmiä, joilla varmistetaan ajoneuvon vastaanottamien viestien oikeellisuus (Petit & Shladover, 2015).

Edellisessä luvussa automatisoitujen ajoneuvojen yhdeksi merkittävimmäksi ongelmaksi nousi ajoneuvon järjestelmien väliseen kommunikaatioon käytettävän CAN-väylän tietoturvan heikkous. Wangin ja Sawhneyn (2014) tutkimuksessa esitetään kyseiselle ongelmalle ratkaisuksi VeCure-nimistä tietoturvajärjestelmää. Tutkimuksen mukaan VeCure hankaloittaa vahingollisen datan syöttämistä CAN-väylälle säätelemällä viesteihin käsiksi pääsyä ja ottamalla käyttöön viestien todennuksen. Kyseisen järjestelmän etuna on sen yhteensopivuus jo olemassa olevien ajoneuvoalustojen kanssa, sekä viestien matala viive VeCurea käytettäessä verrattuna muihin vastaaviin järjestelmiin (Wang & Sawhney, 2014). Viiveen madaltamisen voisi katsoa olevan ensisijaisen tärkeää ajoneuvojen järjestelmissä, sillä viiveen kasvaessa ajoneuvon toiminnan kannalta olennaisten järjestelmien kohdalla, voi ajoneuvon käytettävyys mahdollisesti heikentyä. Esimerkiksi ajoneuvon ohjattavuuteen liittyvä viive voisi aiheuttaa mahdollisen yhteentörmäyksen, jos ajoneuvo ei kykene reagoimaan kuljettajan ohjausliikkeisiin riittävän nopeasti. Wangin ja Sawhneyn (2014) tutkimuksessa testattiin kyseistä VeCure-järjestelmää luomalla siitä konseptitodistus Freescalen valmistamia kehityspiirilevyjä käyttäen. Tutkimuksessa havaittiin, että järjestelmän avulla lähetetyillä ja vastaanotetuilla viesteillä oli vain 50 mikrosekunnin viive, minkä arvioitiin olevan jopa 20 kertaa nopeampi kuin aiemmin ehdotetuilla ratkaisuilla (Wang & Sawhney, 2014).

Choi ym. (2018) tutkimuksessa ehdotetaan puolestaan VoltageIDS-nimistä järjestelmää, jonka tarkoituksena on havaita CAN-väylään kohdistuvia hyökkäyksiä. Wangin & Sawhneyn (2014) VeCure-järjestelemän tavoin myös VoltageIDS on yhteensopiva tällä hetkellä käytössä olevien ajoneuvojen kanssa, minkä ansiosta sen voi ajatella olevan suhteellisen matalan kynnyksen ratkaisu toteutettavaksi. Tutkimuksen mukaan kyseisen järjestelmän toiminta perustuu ajoneuvon sähkönohjausyksikköjen (Electronic Control Unit, ECU) lähettämien sähköisten CAN-signaalien alkuperän tunnistamiseen. Tutkimuksessa kerrotaan, että jokainen ECU lähettää vain tietyn tyyppiseen toimintaan liittyviä signaaleja, eli jos järjestelmän vastaanottama signaali ei vastaa sen alkuperää, voidaan

signaali määrittää epäkelvoksi. Signaalien alkuperän väärentäminen vaatisi erillisen fyysisen laitteen asentamista hyökättävään ajoneuvoon, mikä poistaisi mahdollisten etähyökkäyksien mahdollisuuden (Choi ym., 2018).

Automatisoitujen ajoneuvojen lisäksi myös älykkäät liikenteenohjauksen järjestelmät, kuten adaptiiviset liikennevalot, tarvitsevat nekin osaltaan tehokasta tietoturvaa. Yen ym. (2021) tutkivat erilaisten simulaatiomallien ja kaavojen avulla tällaisten järjestelmien alttiutta viestien väärentämishyökkäyksille, ja miten torjua näitä hyökkäyksiä. Tutkimuksessa käytettiin kahta puolustusalgoritmia: niin sanottua ”huutokauppa-algoritmia” (Auction-Based Protection Algorithm, APA) ja ”hybridipohjaista algoritmia” (Hybrid-Based Protection Algorithm, HPA). Tutkimuksen mukaan APA:n avulla liikenteenohjausjärjestelmä jättää huomioimatta väärentämishyökkäyksille tyypillisen äärimmäisen korkeita arvoja sisältävän datan, kun taas HPA:n avulla järjestelmä vaihtaa liikenteenohjauksen algoritmityyppejä sen mukaan, millainen hyökkäys järjestelmään kohdistuu. Molempien puolustusalgoritmien havaittiin lieventävän hyökkäysten aiheuttamia negatiivisia vaikutuksia liikenteen kulkuun (Yen ym., 2021), eli niiden voisi katsoa olevan toimivia ratkaisuja liikenteenohjausjärjestelmien tietoturvaan liittyen.

4.2 Eettiset ratkaisut

Kyberturvallisuuden ongelmien ollessa luonteeltaan suhteellisen käytännönläheisiä, voi niiden ratkaiseminenkin olla varsin suoraviivaisesti hahmotettavissa. Eettiset ongelmat ovat, kuten edellisessä luvussa todettiinkin, sen sijaan tarkasteltavissa usein hyvin monelta eri kantilta, mikä voi tehdä ”objektiivisten” ratkaisujen löytämisestä haastavampaa.

Erääksi suurimmista eettisistä ongelmista älykkäiden tieliikennejärjestelmien osalta voidaan kenties arvioida niin sanottu ”vaunuongelma”, eli vähiten haitallisimman vaihtoehdon valitseminen tilanteessa, jossa liikenneonnettomuuden tapahtuminen on väistämätön. Dennis ym. (2016) tutkimuksessa esitettiin, että automatisoiduille ajoneuvoille voidaan asettaa niin sanottuja ”moraalistandardeja” ohjaamaan ajoneuvon käytöstä ongelmatilanteissa. Tutkimuksessa esitellyn viitekehyksen perustana oli olettamus siitä, että ajoneuvo valitsisi aina vähiten epäeettisimmän ratkaisun. Tämä tarkoittaisi käytännössä sitä, että vaikka tehty valinta olisi epäeettinen, tehtiin valinta kuitenkin vain sen vuoksi, että kaikki muut vaihtoehdot olisivat olleet vieläkin epäeettisempiä (Dennis ym., 2016). Kyseisessä tutkimuksessa ei kuitenkaan eritelty, miten tällainen logiikka voitaisiin käytännössä implementoida osaksi automatisoituja ajoneuvoja.

Samaa aihealuetta pohdittiin myös Goodallin (2014) tutkimuksessa. Kyseinen tutkimus vei kuitenkin Dennis ym. (2016) ajattelua hieman pidemmälle esittämällä niin sanotun kolmen vaiheen lähestymistavan. Kyseisen lähestymistavan ensimmäinen vaihe sisältäisi Dennis ym. (2016) tutkimuksen standardien kaltaisten rajoitteiden asettamisen ajoneuvoille. Tutkimuksen mukaan rajoitukset olisivat yleisesti hyväksyttävissä olevia sääntöjä, esimerkiksi materiaalivahinkojen

suosiminen henkilövahinkojen sijaan, ja niistä voitaisiin päättää esimerkiksi lakimiesten, ajoneuvojen valmistajien ja etiikan asiantuntijoiden kanssa. Tutkimuksen lähestymistavan toiseen vaiheeseen kuuluisi puolestaan edistyneen tekoälyteknologian, kuten neuroverkkojen, hyödyntäminen moraalisten päätösten opettamisessa ajoneuvoille. Tutkimuksessa lisätään, että tämä oppiminen tapahtuisi ensimmäisen vaiheen asettamien rajoitteiden puitteissa. Lähestymistavan kolmannessa vaiheessa osaksi käytettyä tekoälyratkaisua implementoitaisiin teknologiaa, jonka avulla saataisiin selville, miksi tekoäly päätyi tekemään jonkin tietyn päätöksen (Goodall, 2014). Tutkimuksessa kuitenkin huomautettiin, että kahden jälkimmäisen vaiheen vaatimat teknologiat eivät ole vielä nykyisellään sillä tasolla, että niitä voitaisiin hyödyntää onnistuneesti.

Kuten edellisessä luvussa mainittiin, tieliikennevahinkojen vähentämisen lisäksi tärkeänä eettisenä ongelmana voidaan pitää datan väärinkäyttöä ja yksityisyyden suojan puutteita. Älykkäitä tieliikennejärjestelmiä tuottavien tahojen toimintaa näiden ongelmien suhteen voivat ohjata muun muassa lainsäädäntö, pyrkimys ylläpitää tahojen mainetta sekä erilaiset standardoinnit.

Stahlin ja Wrightin (2018) tutkimuksen mukaan datan käyttöön ja yksityisyyden ylläpitämiseen on olemassa aluekohtaisia lainsäädäntöjä ja asetuksia, esimerkiksi Euroopassa toimiva yleinen tietosuoja-asetus (General Data Protection Regulation) määrää Euroopan unionin jäsenmaiden tietosuojakäytänteitä. Näihin käytänteisiin kuuluvat muun muassa taloudellisten sanktioiden langettaminen rikkomustapauksissa, tietomurroista ilmoittaminen sekä ”lupa tulla unohdetuksi” (right to be forgotten) (Stahl & Wright, 2018). On kuitenkin hyvä ottaa huomioon, että jokainen Euroopan unionin ulkopuolinen valtio määrää itse omat tietosuojakäytäntönsä, eli Euroopan unionin säädösten tapaisia käytänteitä ei välttämättä ole käytössä sen ulkopuolisilla alueilla.

Vaikka lainsäädäntö ei vaikuttaisikaan älykkäiden tieliikennejärjestelmien valmistajien tietosuojakäytänteisiin, on valmistajien itsensä etu, että tietosuojasta välitetään. Smithin (2020) tutkimuksessa otetaan esille yritysten velvollisuus asiakkaiden luottamuksen ansaitsemisessa. Asiakkaiden silmissä luotettavana toimijana pysyminen vaatii yrityksiltä läpinäkyvyyttä ja lupausten pitämistä (Smith, 2020). Vaikka tutkimus otti kantaa varsinaisen tietosuojan sijasta ajoneuvojen automaatioon yleensäkin, voidaan tehdä olettamus, että läpinäkyvyys ja lupausten pitäminen myös asiakkaiden tietojen käsittelystä on luotettavuutta lisäävä tekijä.

Muita edellisessä luvussa esille nousseita eettisiä ongelmia olivat automatisoitujen ajoneuvojen väärinkäyttö itsekkäiden käyttäjien toimesta sekä ajoneuvojen käyttäjien valppauden heikkeneminen apujärjestelmien aiheuttaman ”puutumisen” seurauksena. Automatisoitujen ajoneuvojen ohjelmoinnissa noudatetaan oletettavasti käyttöalueen liikennelainsäädäntöä, mutta ajoneuvon käyttäjä voi osatessaan muuttaa ohjelmointia esimerkiksi sallimaan ylinopeuden ajamisen (Lin, 2016). Tällaiseen väärinkäyttöön on haastavaa löytää varmaa ratkaisua, sillä kyberhyökkäykset ovat lähes väistämättömiä tietotekniikkaa käytettäessä. Ilmiötä lieventämään on kuitenkin olemassa erilaisia tietoturvaratkaisuja, kuten edellisessä kyberturvallisuutta käsittelevässä alaluvussa esitettiinkin.

Teknisiä ratkaisuja ehdotetaan myös apujärjestelmien aiheuttamaan kuljettajan valppauden heikkenemisen torjumiseen. Kumfer ym. (2016) ehdottavat tutkimuksessaan, että automatisoituihin ajoneuvoihin tulisi soveltaa vakiintuneita turvastandardeja. Tutkimuksen mukaan ajoneuvojen tulisi pystyä ilmoittamaan ajoneuvon käyttäjälle, jos ajoneuvon toiminnassa tapahtuu sellaisia poikkeamia, jotka mahdollisesti vaatisivat käyttäjän manuaalista väliintuloa. Tasa-arvoisuuden ja eettisyyden nimissä täytyisi myös taata, että erilaisia rajoitteisuuksia, esimerkiksi kuulo- tai näkövamman, omaavien henkilöiden olisi mahdollista huomata nämä ilmoitukset, mikä tarkoittaisi muun muassa auditiivisten, visuaalisten ja haptisten ilmoitusten mahdollisuuden lisäämistä ajoneuvoihin (Kumfer ym., 2016).

Erilaisten eettisten standardien kehittelyyn ja käyttöönottamiseen liittyy kuitenkin myös omat ongelmansa. Papadimitriou ym. (2022) huomauttavat tutkimuksessaan, että vaikka vakituisuus ja johdonmukaisuus ovat tyypillisiä ominaisuuksia erilaisille standardeille, on standardeilla tärkeä löytyä myös tietyn verran joustavuutta. Tutkimuksessa muistutetaan, että kukin standardi heijastaa määrittelyhetkellä vallinneita arvoja ja etiikkaa, eikä niiden pysyvyydestä tulevaisuudessa ole takeita. Tämä on mielestäni erittäin oleellinen havainto, sillä informaatioteknologian yhtenä ominaispiirteenä voidaan pitää sen nopeaa muuttuvuutta.

4.3 Lainsäädännölliset ratkaisut

Kyberturvallisuuden ja eettisyyden lisäksi älykkäiden tieliikennejärjestelmien kehittyminen on herättänyt keskustelua myös niihin liittyvien laillisten haasteiden osalta. Erilaisia tarkasteltuja laillisia näkökulmia ovat olleet muun muassa vastuutahojen määrittely ongelmatilanteissa, nykyisen tieliikennelainsäädännön muuttaminen sekä liikennesääntöjen noudattaminen automatisoitujen ajoneuvojen toimesta. Näiden näkökulmien tarkastelu yleisellä tasolla voi osoittautua haasteelliseksi, sillä jokainen valtio noudattaa omia lainsäädäntöjään.

Vaikka automatisoitujen ajoneuvojen arvioidaan luovan vähemmän onnettomuuksia kuin aiheuttavan niitä, ei tieliikenneonnettomuuksilta voida välttyä kokonaan (Maurer, 2016). Kuten Gasserin (2016) tutkimuksessa havaittiin, on vastuu osittain automatisoitujen ajoneuvojen onnettomuuksien kohdalla kuljettajalla itsellään. Älykkäitä apujärjestelmiä käytettäessä on kuljettajan siis silti pysyttävä valmiina ottamaan ajoneuvo takaisin hallintaan vähäisellä varoitusajalla. Gasserin (2016) tutkimuksessa nousi esille kuitenkin huomio, että korkean automaation kohdalla vastuiden määritteleminen ei ole aivan yhtä selkeää. Tutkimuksen mukaan yleisesti ottaen nykyisiä tieliikennelakeja säädettäessä on vallinnut olettamus, että ajoneuvon ohjaamisesta vastaa ensikädessä elävä ihminen. Korkean automaation kohdalla ongelmaksi nouseekin se, että ohjaaminen siirtyy kuljettajan sijaan itse ajoneuvon tehtäväksi (Gasser, 2016). Vellingan (2019) tutkimuksessa esitetään erilaisia lähestymistapoja tähän pulmaan liittyen. Kaikista käytännöllisimmäksi näistä nousi ajoneuvon valmistajan asettaminen vastuussa

olevaksi tahoksi, sillä se olisi vähiten ristiriidassa nykyisten lainsäädäntöjen, erityisesti vuonna 1968 laaditun Wienin tieliikenteen yleissopimuksen, kanssa, ja koska korkean automaation kohdalla ajoneuvon käyttäjällä ei ole todellista valmiutta ohjata ajoneuvoa (Vellinga, 2019). Jotta vastuunjako olisi selkeää, olisi vastuut kuitenkin merkittävä selvästi lainsäädäntöön väärinymmärrysten välttämiseksi.

Vastuutahojen määrittelyn lisäksi lainsäädäntöä tulisi miettiä myös automatisoitujen ajoneuvojen testaamisen suhteen. McGehee ym. (2016) raportin mukaan Yhdysvalloissa Nevadan, Michiganin ja Kalifornian osavaltioiden tapauksessa automatisoitujen ajoneuvojen testaamiselle yleisillä teillä on jo myönnetty lupia, joten testaamiseen liittyvästä laillisesta menettelystä on jo olemassa käytännön esimerkkejä. Raportissa kerrotaan, että kyseisissä osavaltioissa automatisoitujen ajoneuvojen testaamisen edellytyksenä on se, että ajoneuvon kuljettajalla on koko testaamisen ajan tarpeen tullen kyky ottaa ajoneuvo takaisin hallintaansa. Lisäksi Nevadan osavaltiossa testaamisluvan saamista edeltää hakemusprosessi, johon kuuluu testaamiseen kuuluvien tietyyppien ja maaston listaaminen (McGehee, 2016). Samankaltaisia toimenpiteitä voidaan havaita myös Australiassa, jossa testaamislupaan liittyy muun muassa testipaikasta ja testattavasta teknologiasta raportoiminen, sekä kuljettajan läsnäolo testattavan ajoneuvon käytössä (Lee & Hess, 2020). Laissa määrätyn raportoinnin voisi katsoa olevan hyvä käytäntö, sillä sen lisäämän läpinäkyvyyden voisi ajatella lisäävän myös luottamusta uuden teknologian käyttöä kohtaan.

McGehee ym. (2016) raportin mukaan Nevadan ja Michiganin tapauksessa testattaville automatisoiduille ajoneuvoille vaaditaan myös erillistä rekisterikilpeä (kuvio 1), joka kertoo ajoneuvon mahdollisuudesta käyttää automaatioteknologian ominaisuuksia. Mielestäni tällaisten automaattisen ajoneuvon tunnistamiseen liittyvien visuaalisten merkkien lisääminen voisi muutenkin olla toimiva ja tieliikenneturvallisuutta parantava käytäntö, sillä muu liikenne kykenisi ottamaan automaattiset ajoneuvot huomioon omassa liikennekäyttäytymisessään, vähentäen mahdollisia epäselvyyksiä.

KUVIO 1 Nevadan osavaltion rekisterikilpi automatisoiduille ajoneuvoille (McGehee ym., 2016)

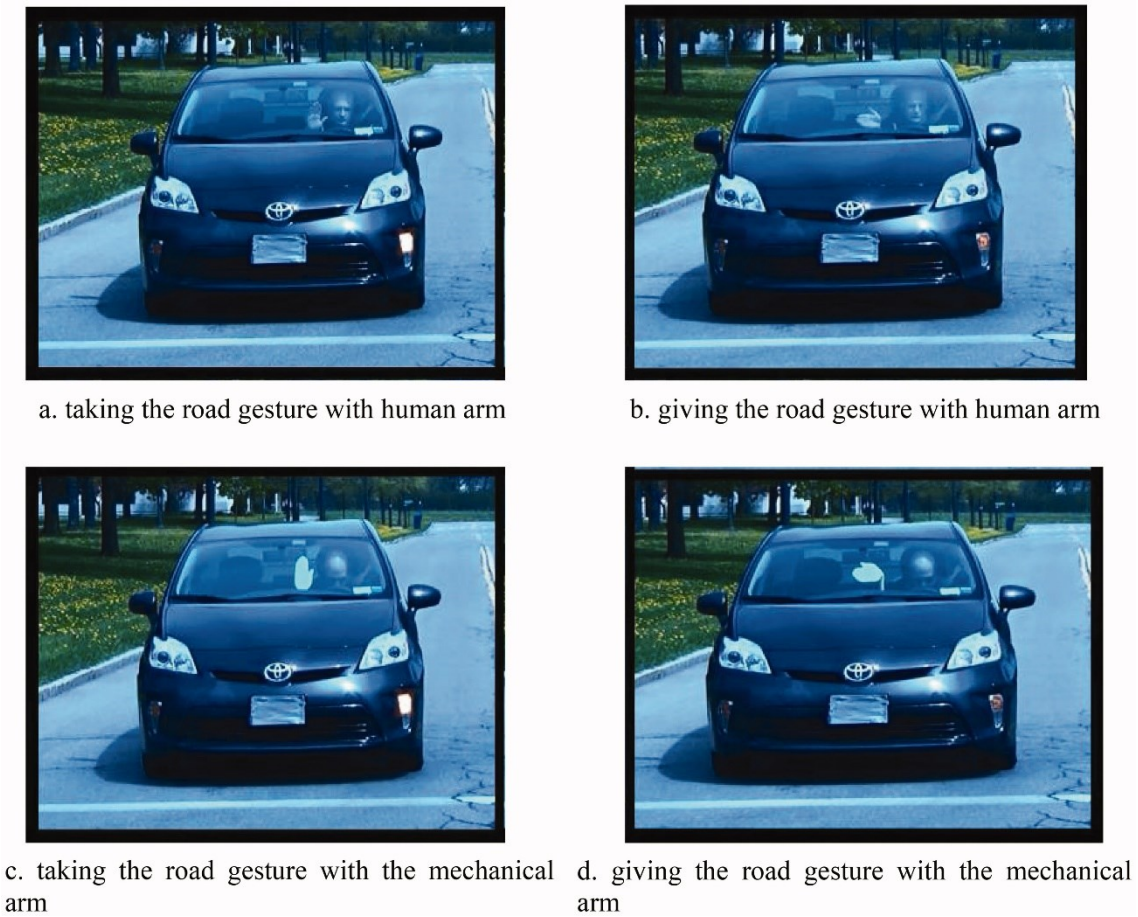
Itse lainsäädännön pohtimisen lisäksi tulisi myös varmistaa, että ajoneuvot kykenevät noudattamaan tieliikenteen lakeja. Yhdeksi edellisessä luvussa esille nousseeksi ongelmaksi ilmeni tieliikenteelle ominaiset improvisaatiotilanteet ja epäformaali käytös, kuten liikenteen ohjaaminen liikennepoliisin viittilöimänä

tai muiden autoilijoiden kehon eleiden lukeminen. Epke ym. (2021) tutkimuksen mukaan nykyiset korkean automaation ajoneuvot kykenevät jo tunnistamaan liikenteessä esiintyvät muut ajoneuvot sekä jalankulkijat ilman suurempia ongelmia, mutta esimerkiksi sanattoman viestinnän ymmärtäminen ja tuottaminen koetaan vielä haasteelliseksi. Ihmistenväliseen kommunikointiin kuuluu monia hienovaraisia piirteitä, kuten erilaisia sosiaalisia ja kulttuurillisia olettamuksia tai pieniä kasvojen ja kehon eleitä, joita voi olla lähes mahdotonta opettaa kehittyneimmällekään tekoälylle. Tämän perusteella voisi arvioida, että automatisoituja ajoneuvoja varten tarvittaisiin korostetumpia kommunikaatiokeinoja, kuten selvästi tunnistettavien käsimerkkien käyttöä.

Käsimerkkien tunnistamiseen ajoneuvojen toimesta onkin jo olemassa suhteellisen toimivia ratkaisuja. Guo ym. (2015) tutkimuksessa esitetään visuaalisia sensoreita hyödyntävä algoritmi, joka kykenee tunnistamaan kirkkaanväristä liiviä käyttävän henkilön, kuten liikennepoliisin, ja siten mallintamaan tunnistetun henkilön ylävartalon ruumiinosien sijainnin. Tämän mallinnuksen avulla voidaan puolestaan havaita tunnistetun henkilön käden asento ja siten päättelemään, näyttääkö henkilö jotain käsimerkkiä (Guo ym., 2015).

Gengin ja Yinin (2020) tutkimuksessa ehdotetaan hyvin samankaltaista menetelmää ihmisten eleiden tunnistamiseen. Tutkimuksessa YOLO-V3-syväoppimisalgoritmia opetettiin infrapunakameran ja Saliency Mapping-teknologian yhdistelmällä otettujen kuvien avulla ihmisten tunnistamista eri asennoista. Tutkimuksessa havaittiin, että kyseinen tunnistamisalgoritmi kykeni tunnistamaan ihmisten asentoja eri etäisyyksiltä ja kuvakulmista tyydyttävällä tarkkuudella. Etuna tällä algoritmilla verrattuna Guo ym. (2015) menetelmään oli se, että tunnistettavan henkilön ei tarvinnut pitää yllään kirkasta liiviä, jotta algoritmi toimisi. Infrapunakameran antaman lämpökuvan ansiosta algoritmi ei ollut myöskään riippuvainen valon määrästä tai säästä (Geng & Yin, 2020).

Ihmisten eleiden tunnistamisen lisäksi ajoneuvojen tulisi kyetä myös kommunikoimaan liikenteessä ihmisten kanssa. Yhdeksi vaihtoehdoksi tämän ongelman ratkaisemiseen on esitetty mekaanisen ”käden” lisäämistä osaksi ajoneuvoa. Zhang ym. (2022) tutkivat tällaisen menetelmän pätevyyttä tutkimuksessa, jossa tarkkailtiin 30. tavallista autoa ohjaavien testihenkilöiden reaktionopeutta ja -tarkkuutta mekaanisen käden suorittamaan viittilöintiin eri nopeuksilla. Tutkimuksessa verrattiin mekaanisen käden suorittamia eleitä oikean ihmisen eleisiin (kuvio 2), ja havaittiin, että koehenkilöt reagoivat mekaanisen käden nopeatempoiseen viittilöintiin lähes yhtä nopeasti ja tarkasti kuin tilanteissa, joissa viittilöinti tapahtui oikean ihmisen toimesta. Tutkimuksessa kuitenkin huomautetaan myös kyseiseen menetelmään liittyvistä ongelmista, kuten mekaanisen käden eleiden rajallisuudesta sekä huonosta näkyvyydestä epäsuotuisissa olosuhteissa. Kyseisen menetelmän etuna voisi puolestaan pitää sen viestinnän yleiskäyttöisyyttä, sillä viittilöintiä voidaan ymmärtää kuljettajan puhumasta äidinkielestä riippumatta (Zhang ym., 2022).



KUVIO 2 Mekaaninen viittilöinti verrattuna aidon ihmisen viittilöintiin (Zhang ym., 2022)

Eräänä toisena ajoneuvojen kommunikaatiomenetelmänä esitettiin niin sanottu tekstipohjainen ulkoinen rajapinta (external human-machine interface, eHMI) Epke ym. vuonna 2021 julkaistussa tutkimuksessa, jossa selvitettiin jalankulkijoiden ja automatisoitujen ajoneuvojen välistä kommunikaatiota tienylitystilanteissa. Tutkimuksessa koehenkilöinä toimineet jalankulkijat nostivat ajoneuvolle kättä tienylityksen merkiksi, jonka jälkeen ajoneuvon eHMI, käytännössä digitaalinen näyttö, ilmoitti jalankulkijan havaitsemisen merkiksi tekstipohjaisen viestin. Tutkimuksessa havaittiin, että eHMI:n käyttäminen teki ajoneuvon käyttäytymisestä ennalta-arvattavampaa, mikä puolestaan lisäsi jalankulkijoiden luottamusta ajoneuvoa kohtaan. Kaikkein tehokkaimman kommunikaation saavuttamiseksi vaadittaisiin siis sekä ajoneuvon että jalankulkijan osallistumista vuorovaikutukseen (Epke ym., 2021).

5 YHTEENVETO

Tämän kandidaatintutkielman tutkimuskohteena olivat älykkäät tieliikennejärjestelmät. Tutkielman tutkimusongelmana pyrittiin selvittämään, millaisia haasteita ja riskejä älykkäiden tieliikennejärjestelmien käyttöön liittyy, ja millaisia ratkaisuja näihin pulmiin voisi soveltaa. Tämä toteutettiin kirjallisuuskatsauksena tutkien aiempia vertaisarvioituja tieteellisiä julkaisuja aiheeseen liittyen.

Monet älyteknologiatyypit, kuten niin sanottu tekoäly, ovat olleet ajankohtainen puheenaihe informaatioteknologian alalla viime aikoina. Erilaiset älyteknologiat voivat auttaa tieliikennettä esimerkiksi vähentämällä inhimillisten virheiden määrää, mutta uuden teknologian käyttöönottoon liittyy myös omat haasteensa. Liikenne on oleellinen osa ihmisten jokapäiväistä elämää ympäri maailmaa, ja tämän vuoksi on tärkeää, että siihen liittyvän teknologian tuomia mahdollisia negatiivisia vaikutuksia tutkitaan. Kun ongelmakohdat ovat selvillä, on myös helpompaa löytää mahdollisia ratkaisuja niihin.

Tutkielman runko rakentuu kolmesta sisältöluvusta, joista ensimmäisessä pyrittiin kartoittamaan, millaisin eri tavoin älyteknologiaa voidaan soveltaa tieliikenteessä. Lisäksi luvussa otettiin esille tieliikennejärjestelmille olennaisia tekoälyn alikuntia. Aihepiirin laajuuden vuoksi tutkielman käsittelemä näkökulma rajattiin kahteen olennaiseen osa-alueeseen: liikenteenhallinnan ja ajoneuvojen automaatioon. Liikenteenhallinnan menetelmissä, kuten liikenneonnettomuuksien ennustamisessa ja adaptiivisissa liikennevaloissa, keskeisenä teknologiana havaittiin käytettävän tekoälyn alikuntiin kuuluvaa koneoppimista sekä siihen liittyvää syväoppimista ja neuroverkkoja. Ajoneuvojen automaatiosta havaittiin puolestaan, että automaation kehittyneisyys pystyttiin jakamaan viiteen eri tasoon. Näistä matalan automaation eli tasojen 1–3 menetelmiä olivat esimerkiksi jo tällä hetkellä kaupallisesti saatavilla olevat ajoavustimet, kuten mukautuvat vakionopeudensäätimet ja kaistanvaihdon hallintaan liittyvät järjestelmät. Tasojen 4–5 korkean automaation menetelmien, kuten itseohjautuvien ja yhdistettyjen ajoneuvojen, havaittiin olevan vielä laajalti kehityksen alla.

Toisessa sisältöluvussa tarkasteltiin ensimmäisessä luvussa esiteltyjä tieliikennejärjestelmiä tutkielman tutkimusongelman näkökulmasta, eli tutkittiin, millaisia haasteita tieliikenteen älyjärjestelmien käyttöön liittyy. Luvun sisältö

jaettiin kolmeen alalukuun käsiteltyjen haasteiden luonteiden mukaan: kyberturvallisuuteen, eettisyyteen ja lainsäädäntöön liittyviin haasteisiin. Sekä automatisoitujen ajoneuvojen että liikenteenhallinnan järjestelmien havaittiin olevan alttiita erilaisille kyberhyökkäyksille. Erityisen haavoittuvaisia havaittiin olevan ajoneuvojen kommunikaatiojärjestelmät, kuten laajalti käytetty CAN-väylä. Niihin kohdistuvien hyökkäysten arvioitiin olevan erityisen haitallisia mahdollisesti aiheutuvien liikenneonnettomuuksien vuoksi. Liikenteenohjaamiseen kohdistuvien hyökkäysten arvioitiin puolestaan aiheuttavan ruuhkautumista, jonka myötä myös liikenneonnettomuuksien mahdollisuus kasvaa.

Kyberhyökkäysten jälkeen käsiteltiin eettisiä haasteita, joita havaittiin muun muassa älykkäiden liikennejärjestelmien keräämän datan väärinkäyttö sekä automatisoitujen ajoneuvojen menettely ongelmatilanteissa, joissa niiden täytyy tehdä vähiten vahinkoa aiheuttava valinta. Luvun lopussa käsitellyistä laillisista haasteista kävi ilmi, että ne keskittyivät laajalti ajoneuvojen automaation ja nykyisten lainsäädäntöjen ristiriitoihin, sillä nykyisellään tieliikennelainsäädäntö on laadittu manuaalisesti ohjattavia ajoneuvoja ajatellen. Automatisoitujen autojen joutuessa liikenneonnettomuuteen voi olla hankalaa löytää vastuussa olevaa tahoa, sillä ajoneuvon kuljettaja ei välttämättä ole itse ohjannut autoa. Ajoneuvoilla voi olla myös vaikeuksia noudattaa liikennesääntöjä esimerkiksi improvisaatiota vaativissa tilanteissa, kuten liikennepoliisin ohjatessa tieliikennettä liikennevalojen sijasta.

Kolmannessa eli viimeisessä sisältöluvussa keskityttiin toisen luvun haasteiden ratkaisemiseen. Toisen luvun mukaisesti myös tässä luvussa käsitellyt asiat jaettiin omiin alalukuihinsa niiden luonteiden perusteella. Luvussa kyberhyökkäysten uhkaan ehdotettiin erilaisia teknisiä ratkaisuja, kuten viestien todennusmenetelmät ja CAN-väylän tietoturvaa vahvistavat järjestelmät VeCure ja VoltageIDS. Eettisiin ongelmiin ehdotettiin puolestaan erilaisten ”moraalistandardien” käyttöönottamista osaksi älyjärjestelmien ohjelmointia. Dennis ym. (2016) tutkimuksessa ehdotettiin niin sanottua kolmen vaiheen lähestymistapaa eettistä päätöksentekoa varten, jossa automatisoidut ajoneuvot oppisivat priorisoimaan tietynlaisia moraalisia päätöksiä, kuten materiaalivahinkojen suosimista henkilövahinkojen sijaan. Luvussa viimeisenä esille otettiin laillisten haasteiden ratkaiseminen. Keskeisinä ratkaisukeinoina vastuuongelmiin esitettiin ajoneuvojen valmistajien vastuussa pitämistä korkean automaation kohdalla, kun taas matalan automaation kohdalla vastuu siirtyisi ajoneuvon kuljettajalle. Liikenteessä tapahtuvaan improvisaatioon, kuten liikennepoliisin viittilöinnin tunnistamiseen, ehdotettiin syväoppimisalgoritmien ja infrapunakameroiden yhdistelmää, jonka avulla ajoneuvo kykenisi tunnistamaan ihmisen eleitä epäselvissäkin olosuhteissa.

Tutkielmassa esiteltyjen havaintojen perusteella voidaan todeta, että älykkäiden tieliikennejärjestelmien käytön haasteet ovat hyvin moninaisia, kattaen kyberturvalliset, eettiset ja lailliset näkökulmat. Erityisen haastavina näistä voidaan pitää kyberturvallisuuteen liittyviä ongelmia, sillä niillä on suurin mahdollisuus aiheuttaa konkreettista vahinkoa esimerkiksi henkilö- ja materiaalivahingon muodossa. Onnistunut kyberhyökkäys voi häiritä esimerkiksi ajoneuvojen

toimintaa siten, että ajoneuvojen väliset turvavälit järkkyvät ja toiminnan viiveet kasvavat (Amoozadeh ym., 2015). Vaarallisten seuraamusten vuoksi voidaan arvioida, että tietoturvasta ei juurikaan voida tinkiä tieliikenteen älyjärjestelmien suhteen. Kyberhyökkäysten torjumisesta on kuitenkin olemassa paljon tutkimusta, ja esimerkiksi Wang & Sawhneyn (2014) sekä Choi ym. (2018) ehdottamat tietoturvajärjestelmät voisivat tarjota tutkitusti toimivia ratkaisuja ilman suurta rahallista investointia ajoneuvovalmistajien toimesta.

Kuten tutkimuksessa huomattiin, myös lailliset ja eettiset haasteet vaativat osaltaan huomiota. Vaikka eri maiden lainsäädännöillä on eroja, voidaan kuitenkin sanoa kokoavasti, että nykyisellään tieliikennelainsäädäntö on räätälöity nimenomaan perinteisiä ajoneuvoja varten. Tämän takia olisi tärkeää, että esimerkiksi korkeaan automaatioon liittyen tehtäisiin lakimuutoksia mahdollisten epäselvyyksien kitkemiseksi. Automaatio on ollut yksi jatkuvassa nousussa olleista autoteollisuuden suuntauksista, joten lakimuutosten pohtiminen tulee joka tapauksessa vastaan ennemmin tai myöhemmin. Näitä lakeja pohdittaessa tulisi keskustelun tapahtua sekä lainsäätäjien että ajoneuvojen kehittäjien välillä, jotta laillisten näkökulmien lisäksi myös tekniset näkökulmat osattaisiin ottaa huomioon. Kuten Schreursin ja Steuwerin (2016) tutkimuksessa kerrottiinkin, on itseohjautuvien ajoneuvojen testaamiseen liittyvien lakien toimeenpanoa nähty jo esimerkiksi joissain Yhdysvaltojen osavaltioissa, kuten Nevadassa ja Kaliforniassa, joten edistysaskelia tullaan luultavasti näkemään jo lähitulevaisuudessa.

Eettisten haasteiden ratkaisemisen osalta yhtenä tärkeimpänä asiana voisi pitää läpinäkyvyyden lisäämistä. Jos älyjärjestelmien halutaan yleistyvän, täytyy ihmisillä olla mahdollisuus luottaa siihen, että heidän oikeuksiaan esimerkiksi yksityisyyteen liittyen, kunnioitetaan. Lisäksi tulisi varmistaa, että automatisoidut tieliikennejärjestelmät kykenevät noudattamaan vallitsevia moraalikäsityksiä. Vaikka etiikka onkin suhteellisen tulkinnanvaraista, pystytään näitäkin ongelmia lievittämään säätämällä lakeja ja sopimuksia sovituilla tavoilla.

Vaikka tutkielmassa pyrittiin selvittämään älykkäiden tieliikennejärjestelmien haasteita ja niiden ratkaisukeinoja mahdollisimman kattavasti, löytyy siitä kuitenkin myös paljon puutteita. Tutkielman läpikäymät havainnot vastaavat vain murto-osaa kaikesta mahdollisesta tutkimuksesta, koska aihepiiri on valitun rajauksen puitteissa liian laaja käytäväksi läpi yhdessä kandidaatintutkielmassa. Käsiteltyihin älykkäisiin tieliikennejärjestelmiin olisivat voineet kuulua myös esimerkiksi erilaiset ajoneuvojen käyttämät esineiden internetin laitteet ja niin sanotut ”älytiet”. Nämä jäivät tämän tutkielman osalta täysin tarkastelematta. Tutkielmassa käytiin myös läpi vain kyberturvallisuuteen, eettisyyteen ja lainsäädäntöön liittyviä ongelmia, eli esimerkiksi sosiaaliset ja taloudelliset näkökulmat jäivät huomioimatta.

Tutkielman aiheen pinnallisen käsittelyn lisäksi ongelmana oli myös käytetyn aineiston mahdollinen vanhentuneisuus. Vaikka aineistoa valitessa pyrittiinkin suhteelliseen tuoreuteen ottamalla huomioon lähinnä 2010- ja 2020-lukujen tutkimuksia, on esimerkiksi vuosien 2010 ja 2023 uusimpien teknologioiden välillä suuriakin eroja. Nämä puutteet huomioon ottaen ehdottaisin, että mahdollinen jatkotutkimus tehtäisiin esimerkiksi korkeintaan viisi vuotta vanhaa

tutkimusta hyödyntäen, ja rajaten aihepiiriä lisää, esimerkiksi koskemaan vain jonkin tietyn tieliikenteen älyjärjestelmätyypin haasteita jonkin tietyn haasteluokan näkökulmasta.

LÄHTEET

Abduljabbar, R., Dia, H., Liyanage, S. & Bagloee, S.A. (2019). Applications of Artificial Intelligence in Transport: An Overview. *Sustainability*, *11*(1). https://doi.org/10.3390/su11010189

Ahmed, H.R. & Glasgow, J.I. (2012). *Swarm Intelligence: Concepts, Models and Applications*. Queen's University, School of Computing Technical Reports, Kingston, Ontario, Canada. http://dx.doi.org/10.13140/2.1.1320.2568

Amoozadeh, M., Raghuramu, A., Chuah, C.-N., Ghosal, D., Zhang, H.M., Rowe, J. & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, *53*(6), 126–132. https://doi.org/10.1109/MCOM.2015.7120028

Arabi, N.S., Halabi, T. & Zulkernine, M. (2021). Reinforcement Learning-driven Attack on Road Traffic Signal Controllers. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece, 218–225. https://doi.org/10.1109/CSR51186.2021.9527951

Boukerche, A., Tao, Y. & Sun, P. (2020). Artificial intelligence-based vehicular traffic flow prediction methods for supporting intelligent transportation systems. *Computer Networks*, *182*, artikkeli 107484. https://doi.org/10.1016/j.comnet.2020.107484

Chen, Q.A., Yin, Y., Feng, Y., Mao, Z.M. & Liu, H.X. (2018). Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control. *Network and Distributed System Security (NDSS) Symposium 2018*, San Diego, CA, USA. http://dx.doi.org/10.14722/ndss.2018.23222

Choi, W., Joo, K., Jo, H.J., Park, M.C. & Lee, D.H. (2018). VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System. *IEEE Transactions on Information Forensics and Security*, *13*(8), 2114–2129. https://doi.org/10.1109/TIFS.2018.2812149

Dennis, L., Fisher, M., Slavkovik, M. & Webster, M. (2016). Formal verification of ethical choices in autonomous systems. *Robotics and Autonomous Systems*, *77*, 1–14. https://doi.org/10.1016/j.robot.2015.11.012

Dogan, E. & Akgüngör, A.P. (2013). Forecasting highway casualties under the effect of railway development policy in Turkey using artificial neural networks. *Neural Computing and Applications*, *22*(5), 869–877. https://doi.org/10.1007/s00521-011-0778-0

Epke, M.R., Kooijman, L. & de Winter, J.C.F. (2021). I See Your Gesture: A VR-Based Study of Bidirectional Communication between Pedestrians and Automated Vehicles. *Journal of Advanced Transportation*, *2021*, artikkeli 5573560. https://doi.org/10.1155/2021/5573560

European Environment Agency. (2019). *The European environment – State and outlook 2020 : knowledge for transition to a sustainable Europe.* Publications Office. https://data.europa.eu/doi/10.2800/96749

Färber, B. (2016). Communication and Communication Problems Between Autonomous Vehicles and Human Drivers. Teoksessa M. Maurer, J.C. Gerdes, B. Lenz & H. Winner (toim.), *Autonomous Driving Technical, Legal and Social Aspects* (s. 523–551). Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48847-8_7

Gasser, T.M. (2016). Fundamental and Special Legal Questions for Autonomous Vehicles. Teoksessa M. Maurer, J.C. Gerdes, B. Lenz & H. Winner (toim.), *Autonomous Driving Technical, Legal and Social Aspects* (s. 523–551). Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48847-8_25

Geng, K. & Yin, G. (2020). Using Deep Learning in Infrared Images to Enable Human Gesture Recognition for Autonomous Vehicles. *IEEE Access*, *8*, 88227–88240. https://doi.org/10.1109/ACCESS.2020.2990636

Goodall, N.J. (2014). Ethical Decision Making During Automated Vehicle Crashes. *Transportation Research Record: Journal of the Transportation Research Board*, 2424(1), 58–65. https://doi.org/10.3141/2424-07

Graupe, D. (2013). *Principles of Artificial Neural Networks*. 3. painos, World Scientific. https://doi.org/10.1142/8868

Griffith, T. & Clancey-Shang, D. (2023). Cryptocurrency regulation and market quality. *Journal of International Financial Markets, Institutions and Money*, *84*, artikkeli 101744. https://doi.org/10.1016/j.intfin.2023.101744

Guo, F., Tang, J. & Zhu, C. (2016). Gesture Recognition for Chinese Traffic Police. *2015 International Conference on Virtual Reality and Visualization (ICVRV), Xiamen, China*, 64–67. https://doi.org/10.1109/ICVRV.2015.52

Hall, R. W. (2003). *Handbook of Transportation Science*. 2. painos, Springer New York, NY. https://doi.org/10.1007/b101877

International Business Machines Corporation. (2023). *What is machine learning?* Haettu 9.6.2023 osoitteesta What is Machine Learning? | IBM

Iyer, L. S. (2021). AI enabled applications towards intelligent transportation. *Transportation Engineering, 5*, artikkeli 100083. https://doi.org/10.1016/j.treng.2021.100083

Khatoun, R. & Zeadally, S. (2017). Cybersecurity and Privacy Solutions in Smart Cities. *IEEE Communications Magazine*, *55*(3), 51–59. https://doi.org/10.1109/MCOM.2017.1600297CM

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. & Savage, S. (2010). Experimental Security Analysis of a Modern Automobile. *2010 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 447–462. https://doi.org/10.1109/SP.2010.34

Kumarage, S.P., Rajapaksha, R.P.G.K.S., De Silva, D., Bandara, J.M.S.J. (2018). Traffic flow estimation for urban roads based on crowdsourced data and machine learning principles. Teoksessa T. Kovacikova, L. Buzna, G. Pourhashem, G. Lugano, Y. Cornet & N. Lugano (toim.), *Intelligent Transport Systems – From Research and Development to the Market Uptake* (s. 263–273). Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-93710-6_27

Kumfer, W.J., Levulis, S.J., Olson, M.D. & Burgess, R.A. (2016). A Human Factors Perspective on Ethical Concerns of Vehicle Automation. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting 2016*, *60*(1), 1844–1848. https://doi.org/10.1177/1541931213601421

Lambora, A., Gupta, K. & Chopra, K. (2019). Genetic Algorithm – A Literature Review. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*. https://doi.org/10.1109/COMITCon.2019.8862255

Leslie, D. (2019) Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. *The Alan Turing Institute*. https://doi.org/10.5281/zenodo.3240529

Lin, P. (2016). Why Ethics Matters for Autonomous Cars. Teoksessa M. Maurer, J.C. Gerdes, B. Lenz & H. Winner (toim.), *Autonomous Driving Technical, Legal and Social Aspects* (s. 69–85). Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48847-8_4

Lu, J., Chen, S., Wang, W. & van Zuylen, H. (2012). A hybrid model of partial least squares and neural network for traffic incident detection. *Expert Systems with Applications*, *39*(5), 4775–4784. https://doi.org/10.1016/j.eswa.2011.09.158

Mandal, V., Mussah, A.R., Jin, P. & Adu-Gyamfi, Y. (2020). Artificial Intelligence-Enabled Traffic Monitoring System. *Sustainability*, *12*(21). https://doi.org/10.3390/su12219177

Maurer, M., Gerdes, J.C., Lenz, B. & Winner, H. (2016). *Autonomous Driving Technical, Legal and Social Aspects*. Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48847-8

McGehee, D.V., Brewer, M., Schwarz, C., Smith, B.W. (2016). *Review of automated vehicle technology: policy and implementation implications*. University of Iowa, Public Policy Center. https://rosap.ntl.bts.gov/view/dot/30702

Milanes, V., Shladover, S.E., Spring, J., Nowakowski, C., Kawazoe, H. & Nakamura, M. (2013). Cooperative Adaptive Cruise Control in Real Traffic Situations. *IEEE Transactions on Intelligent Transportation Systems*, *15*(1), 296–305. https://doi.org/10.1109/TITS.2013.2278494

Müller., V.C. & Zalta, E.N. (2021). Ethics of Artificial Intelligence and Robotics. *The Stanford Encyclopedia of Philosophy* (Summer 2021 Edition). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2021/entries/ethics-ai/

Papadimitriou, E., Farah, H., van de Kaa, G., de Sio, F.S., Hagenzieker, M. & van Gelder, P. (2022). Towards common ethical and safe 'behaviour' standards for automated vehicles. *Accident Analysis & Prevention*, *174*, artikkeli 106724. https://doi.org/10.1016/j.aap.2022.106724

Pöyhönen, J., Kotilainen, P., Poikolainen, J., Kalmari, J. & Neittaanmäki, P. (2019). Cyber Security of Vehicle CAN bus. Teoksessa T, Cruz. & Simoes, P. (toim.), *ECCWS 2019: Proceedings of the 18th European Conference on Cyber Warfare and Security* (s. 354–363). Academic Conferences International. Proceedings of the European conference on information warfare and security. http://urn.fi/URN:NBN:fi:jyu-202001071036

Qureshi, M.F., Shah, S.M.A. & Al-Matroushi, G.I. (2013). A Comparative Analysis of Multi-Criteria Road Network. *European Journal of Computer Science and Information Technology*, *1*(2), 27–47.

Russell, S. & Norvig, P. (2009). *Artificial Intelligence: A Modern Approach*. 3. painos, Pearson.

Schreurs, M.A. & Steuwer, S.D. (2016). Autonomous Driving–Political, Legal, Social and Sustainability Dimensions. Teoksessa M. Maurer, J.C. Gerdes, B. Lenz & H. Winner (toim.), *Autonomous Driving Technical, Legal and Social Aspects* (s. 149–171). Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48847-8_8

Shaout, A. & Jarrah, M.A. (1997). Cruise control technology review. *Computers & Electrical Engineering*, *23*(4), 259–271. https://doi.org/10.1016/S0045-7906(97)00013-X

Smith, B.W. (2020). Ethics of Artificial Intelligence in Transport. Teoksessa M Dubber, F Pasquale, S Das (toim.), *The Oxford Handbook of Ethics of Artificial Intelligence*. https://ssrn.com/abstract=3463827

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. 7. painos, Pearson.

Sweet, M. (2011). Does Traffic Congestion Slow the Economy*? Journal of Planning Literature*, *26*(4), 391–404. https://doi.org/10.1177/0885412211409754

Vellinga, N.E. (2019). Automated driving and its challenges to international traffic law: which way to go?. *Law, Innovation and Technology*, *11*(2), 257–278. https://doi.org/10.1080/17579961.2019.1665798

Wagner, P. (2016). Traffic Control and Traffic Management in a Transportation System with Autonomous Vehicles. Teoksessa M. Maurer, J.C. Gerdes, B. Lenz & H. Winner (toim.), *Autonomous Driving Technical, Legal and Social Aspects* (s. 301–316). Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48847-8_15

Wang, C., Li, X., Zhou, X., Wang, A. & Nedjah, N. (2016). Soft computing in big data intelligent transportation systems. *Applied Soft Computing*, *38*, 1099–1108. https://doi.org/10.1016/j.asoc.2015.06.006

Wang, Q. & Sawhney, S. (2014). VeCure: A practical security framework to protect the CAN bus of vehicles. *2014 International Conference on the Internet of Things (IOT)*, Cambridge, MA, USA, 13–18. https://doi.org/10.1109/IOT.2014.7030108

Wolf, I. (2016). The Interaction Between Humans and Autonomous Agents. Teoksessa M. Maurer, J.C. Gerdes, B. Lenz & H. Winner (toim.), *Autonomous Driving Technical, Legal and Social Aspects* (s. 103–124). Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48847-8_6

World Health Organization. (2020). *Leading causes of death and disability 2000–2019: A visual summary*. Haettu 10.3.2023 osoitteesta Leading causes of death and disability 2000-2019: A visual summary (who.int)

Yagdereli, E., Gemci, C. & Aktas, A.Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, *12*(4), 369–381. https://doi.org/10.1177/1548512915575803

Yen, C.-C., Ghosal, D., Zhang, M. & Chuah, C.-N. (2021). Security Vulnerabilities and Protection Algorithms for Backpressure-Based Traffic Signal Control at an Isolated Intersection. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 6406–6417. https://doi.org/10.1109/TITS.2021.3056658

Zhang, W., Wu, C., You, X., Kust, L., Chen, Y. & Shi, J. (2022). Communication Between Automated Vehicles and Drivers in Manual Driving Vehicles: Using a Mechanical Arm to Produce Gestures. *International Journal of Human-Computer Interaction*. https://doi.org/10.1080/10447318.2022.2082022

Zhou, Z.-H. (2021). *Machine Learning* (kääntäjä S. Liu). Springer Singapore. https://doi.org/10.1007/978-981-15-1967-3