Markus Haaranen, Janne Allonen

KAMERAVALVONNASSA KÄYTETTÄVÄN TEKO-ÄLYN HYÖDYNTÄMINEN SUOMESSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Haaranen, Markus & Allonen, Janne
Kameravalvonnassa käytettävän tekoälyn hyödyntäminen Suomessa
Jyväskylä: Jyväskylän yliopisto, 2020, 150 s.
Kyberturvallisuus, pro gradu-tutkielma
Ohjaaja(t): Lehto, Martti

Kameravalvonnan pääsääntöisenä tavoitteena on ollut tallentaa tapahtunut yksittäinen teko tai tapahtumasarja. Tehokkuuden sekä käytännöllisyyden takia siitä onkin useassa organisaatiossa muodostunut luontainen osa kokonaisturvallisuutta. Teknologisen kehityksen harppaukset ovat mahdollistaneet tekoälyohjelmistojen hyödyntämisen jopa kuluttajalaitteissa. Tekoälyllä varustettua kameravalvontaa voidaankin hyödyntää erilaisissa käyttötapauksissa usealla eri toimialalla. Kameravalvontaa hyödynnetään Suomessa niin yksityisellä, julkisella kuin viranomaissektorilla. Kameravalvontaan liittyy myös läheisesti tietosuoja sekä henkilötiedot ja niiden käsittely. Henkilötietojen käsittelyä säätelevät lait ovat hajallaan, eikä toimintaa ohjaavia ohjeita tai päätöksiä ole riittävästi saatavilla. Tämä vaikeuttaa toimijoiden lakisääteisesti ja eettisesti oikeiden ratkaisujen valintaa kameravalvonnassa. Tämän pro gradu-tutkielman tavoitteena on tutkia julkisen sektorin toimijan näkökulmasta kameravalvonnan ja tekoälyn luomien mahdollisuuksien suhdetta lainsäädäntöön. Kvalitatiivisen tutkimuksen aineisto kerättiin kirjallisuuskatsauksen ja asiantuntijahaastatteluiden avulla. Tutkimuksen tuloksista voidaan päätellä, että kameravalvonnassa käytettävän tekoälyn hyödyntäminen Suomessa perustuu eri toimijoilla eri lakeihin ja mahdollistaa tai rajoittaa ratkaisujen valintaa kameravalvonnassa. Lainsäädäntö edellyttää myös kyberturvallisuuden suhteen konkreettisia toimia rekisterinpitäjältä ja henkilötietojen käsittelijältä. Oikein toteutettuna tekoäly mahdollistaa merkittäviä hyötyjä kameravalvonnassa jo tälläkin hetkellä. Tekoälyn tehokkaampi hyödynnettävyys ja tulevaisuuden innovaatiot kameravalvonnassa vaatisivat regulaation lisäksi selkeitä ohjeita ja valvovan viranomaisen linjauksia. Näiden avulla eri sektorin toimijoiden ratkaisuja voitaisiin ohjata joustavasti, eikä tähän tarvittaisi hitaasti reagoivaa kameravalvontaan keskittynyttä uutta omaa lainsäädäntöä. Tämän tutkimuksen avulla julkisen sektorin toimija saa kattavasti tiedot siitä, mitä pitää ottaa huomioon harkittaessa kameravalvonnassa käytettävän tekoälyohjelmiston kehitystä tai käyttöönottoa.

Asiasanat: kameravalvonta, tekoäly, henkilötieto, tietosuoja, kyberturvallisuus

ABSTRACT

Haaranen, Markus & Allonen, Janne
Utilisation of Artificial Intelligence used in video surveillance in Finland
Jyväskylä: University of Jyväskylä, 2020, 150 pp.
Cyber Security, Master's Thesis
Supervisor(s): Lehto, Martti

The main aim of video surveillance has been to record a single happened act or a series of acts. For most parts it has become a natural part of security in many organizations for its efficiency and practicality. The leaps of technological development have enabled the utilization of Artificial Intelligence even in consumer equipment. Video surveillance equipped with Artificial Intelligence can be utilized in different kinds of use cases in different businesses. Video surveillance is utilized in private, public and authority sectors in Finland. Data protection, personal data and the handling of personal data is closely involved with video surveillance. The legislation which regulates the handling of personal data is widely spread and there is not enough guiding or judgments available. This complicates the operators legally and ethically correct choices of solutions in video surveillance. The aim of this Master's Thesis is to research the legal relationship of possibilities created by Artificial Intelligence and video surveillance from the eyes of a public sector organization. The material of this qualitative research was collected with the help of literature review and interviews from specialists. A conclusion can be drawn from the results of the research, that the utilization of Artificial Intelligence in video surveillance in Finland is based on different legislation with different actors and enables or limits the choice of solutions in video surveillance. The legislation requires also solid actions for cyber security from the controller and the handler of personal data. Correctly implemented Artificial Intelligence can enable significant benefits in video surveillance as we speak. A more effective utilization of Artificial Intelligence and future innovations in video surveillance would require in addition with regulation clear guidelines and policies by the supervising authority. With the help of these, the solutions of different actors could be flexibly guided instead of a new slowly reacting legislation focused solidly on camera surveillance. With the help of this research the public sector actor will get comprehensive information of what is to be taken in consideration when considering the development or implementation of an Artificial Intelligence based software in video surveillance.

Keywords: video surveillance, Artificial Intelligence, personal data, data protection, cyber security

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Ensimmäisen varsinainen valvontakäyttöön tarkoitettu kamera kehitettiin jo vuonna 1933 ja sen avulla saatiin kiinni kananmunavaras (Innovative Security, 2017). Kamerat ovatkin olleet hyvin pitkään lähinnä fyysisen turvallisuuden apuvälineitä ja vartijan nukahtavan silmän väsymätön jatke. Valvontakameroiden tarkoitus pelkästä videokuvan tuottamisesta on kuluvalla vuosituhannella siirtynyt uuteen, tekoälyn aikakauteen. Isoissa tiedusteluvaltioissa, kuten Kiinassa ja Yhdysvalloissa, videomateriaalista prosessoidaan irti kaikki mahdollinen data viranomaisten valtaviin palvelinkeskuksiin tai kaupallisten isojen yksityisten yritysten tarpeisiin.

Valvontakameroiden määrä jatkaa kasvuaan, eikä sille tunnu näkyvän loppua. Kasvua on edesauttanut niiden hintojen merkittävä lasku. Suomessa myytiin jo vuonna 2009 arviolta 30000 uutta valvontakameraa vuosittain. Pääosa myynnistä tapahtui turvallisuustoimijoiden toimesta yrityskäyttöön (Yle, 2009). Vuonna 2017 myytiin maailmanlaajuisesti videovalvontatuotteita noin 28 miljardilla dollarilla. Markkinoiden oletetaan kasvavan 87 miljardiin vuoteen 2025 mennessä (Allied Market Research, 2017). Ihmisen onkin liki mahdotonta liikkua kaupungeissa joutumatta valvontakameran kuvaamaksi.

Tietoverkkojen tiedonsiirron nopeutuessa ja kameratarpeen kasvattamisen vuoksi markkinat ovat siirtymässä pois analogisista kameroista. IP eli Internet Protocol kamerat valtaavat markkinoita niiden monien etujen vuoksi. Ne ovat esimerkiksi etäohjattavia ja mahdollistavat reaaliaikaisen katselun laajalle levittyneissä kameraverkoissa. Valvontakamerat ovat yksi datan lähde, jota älykaupungit hyödyntävät kehittäessään palveluita kansalaisilleen (Allied Market Research, 2017). Digitaalinen tiedonsiirto mahdollistaa myös kameroissa käytettävän tekoälyn hyödyntämisen paljon tehokkaammin. Data ja siitä analysoitu tieto on nykyajan öljyä, jonka vuoksi teknologian suuret yritykset kuten Facebook, Google ja Microsoft kohdentavat tekoälyn kehitykseen vuosittain miljardeja euroja (Marttinen, 2018, 158-159).

Regulaatio ei kuitenkaan tahdo pysyä teknologisen kehityksen mukana. Lisäksi ihmisille ominainen tuntemattoman pelko on merkittävä haaste etenkin puhuttaessa kameravalvonnasta. Euroopassa ja etenkin Suomessa luottamus

ihmisiin ja eri yhteiskunnan instituutioihin on kansainvälisestikin maailman kärkiluokkaa. Jotta kameravalvonnalla hankittu data ja sen analysointi tekoälyllä säilyttäisi ihmisten luottamuksen, tulisi se olla valvonnan kohteelle ymmärrettävää, läpinäkyvää ja säädöksiin perustuvaa. Kansalaisen tulee voida luottaa, että häneen kohdistettu tiedonkeruu, sen käsittely ja säilyttäminen täyttää lain edellyttämät vaatimukset (Valtiovarainministeriö, 2019, 1-4).

Suoranaisesti kameravalvontaa koskevaa lainsäädäntöä ei Suomessa juurikaan ole, vaikkakin sen käyttö on hyvin säädeltyä. Esimerkiksi julkisella paikalla kameravalvontaa suorittavan tahon on laadittava asiasta tietosuojaseloste. Tämä pohjautuu tietosuojavaltuutetun linjaukseen, jossa tallennettu kuva ja ääni, josta henkilö on tunnistettavissa, ovat henkilötietolain mukaisesti rinnastettavissa henkilötietoon (Tietosuojavaltuutettu, 2019a).

Kunnat ovat joutuneet säästökuurille, sillä noin kahdessa kolmasosassa Suomen kunnista tulos oli negatiivinen vuonna 2018. Negatiivisesta tuloksesta huolimatta kuntayhtymien menot jatkavat nousua. (Kuntalehti, 2019) Digitalisaatiosta haetaan helpotusta niin budjettivajeeseen kuin palveluiden ja turvallisuuden parantamiseksi. Erilaisia kannustimia kehitykseen on tullut myös valtion taholta. Esimerkiksi vuonna 2019 valtiovarainministeriö avasi 30 miljoonan kannustinjärjestelmän kuntien digitalisaation yhteishankkeisiin. Tuella on tarkoitus tehostaa muun muassa tietojohtamista ja tekoälyn sekä uusien teknologioiden hyödyntämistä (Valtionvarainministeriö, 2019).

Tarve kunnissa tekoälyn hyödyntämiseksi on suuri. Kameravalvonnan kautta saatava data ja sen hyödyntämisen mahdollisuudet ovat merkittävät. Tekoälyohjelmiston avulla voidaan esimerkiksi laskea ja analysoida ihmisten määrää yleisötilaisuuksissa tai yleisissä kokouksissa, vähentää ruuhkia ja ennalta estää rikoksia. Mahdollisuudet ovat periaatteessa rajattomat. Ongelmaksi kuitenkin nousee se, millä tavoin tekoälyä kameravalvonnassa voidaan hyödyntää siten, että se noudattaa sille luotuja lakiin perustuvia säädöksiä. Etenkin, kun säädökset ovat hyvin hajanaisia, puutteellisia ja pohjautuvat enemmänkin yksilön oikeuksiin varsinaisen toiminnanohjauksen sijasta.

1.1 Tutkimustehtävä ja -kysymykset

Tämän pro gradu -tutkielman tarkoituksena on tuottaa kaupungille analyysi niistä mahdollisuuksista, joilla se voisi hyödyntää kameravalvonnassa käytettävää tekoälyä parantaakseen kaupungin turvallisuutta ja tiedolla johtamista. Empiirisessä tarkastelussa ovat etenkin kameravalvontaan kohdistuva kansallinen ja kansainvälinen regulaatio. Koska suoranaista kansallista lakia kameravalvonnalle ei ole, arvioidaan sääntelyä niin yksilönoikeuksien kuin erilaisten tekoälyohjelmistojen ominaisuuksien kautta. Tutkimustehtävän avaamiseksi siihen vastataan kolmen alatutkimuskysymyksen avulla. Alatutkimuskysymykset ovat:

1) Mitä regulaatiota liittyy Suomessa tehtävään kameravalvontaan?

2) Millä tavoin tekoäly vaikuttaa kameravalvonnasta saatavaan informaatioon suhteessa yksilön henkilötietoihin?
3) Mitä tulisi huomioida kameravalvontaan liittyvissä tekoälyohjelmistojen hankinnassa ja käytössä?

Tutkimus on tehty itsenäisenä kokonaisuutena Tampereen kaupunkiseudun elinkeino- ja kehitysyhtiö Business Tampere Oy:n toimeksiannosta ja se toteutettiin laadullista eli kvalitatiivista tutkimusmenetelmää käyttäen. Tutkimuskysymystä lähestytään kirjallisuuskatsauksen avulla. Lähteinä käytetään aiheeseen liittyviä painettuja ja sähköisiä lähteitä. Pääpaino kirjallisuuskatsauksessa on kansallisessa ja kansainvälisessä lainsäädännössä, niihin liittyvissä lain esitöissä sekä eri viranomaisten tekemissä päätöksissä ja tuomioissa. Kirjallisuuskatsauksen jälkeen teoriaosuuden pääteemat kootaan yhteen ja niistä luotujen haastattelurunkojen avulla suoritetaan asiantuntijoiden teemahaastattelut. Haastateltaviksi valitaan laaja-alaisesti kameravalvontaan ja siihen kohdistuvaan regulaatioon sekä tekoälyteknologian käyttöön liittyviä erityisasiantuntijoita.

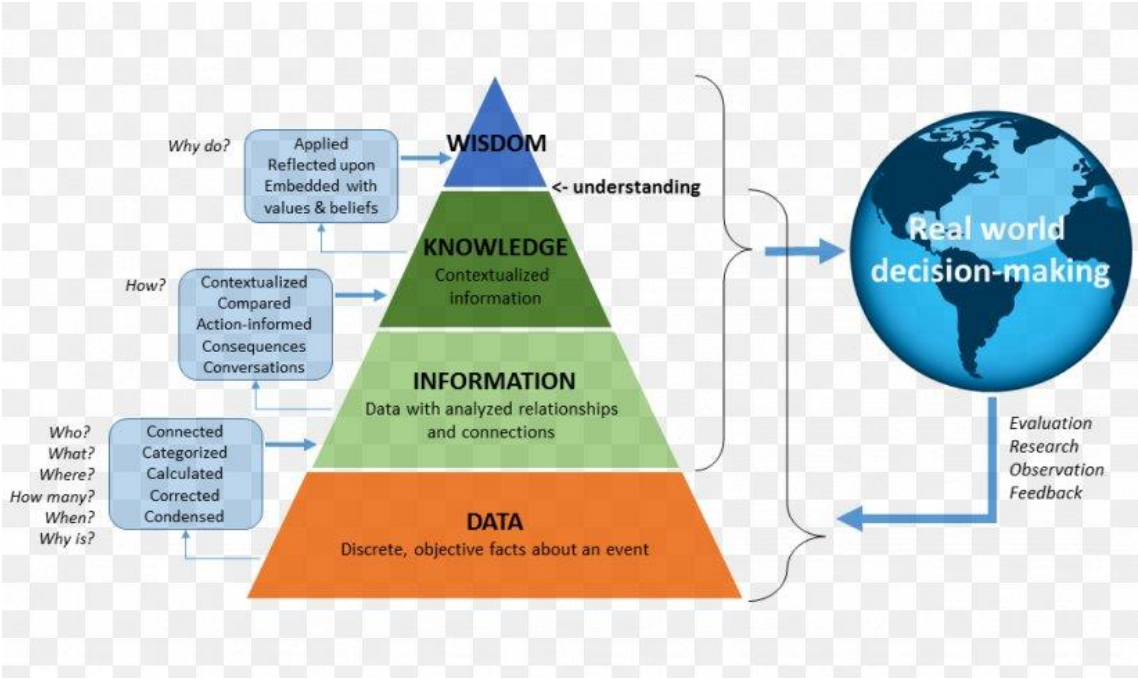
1.2 Perustelut tutkimukselle

Suomessa valvontakameroiden käyttö on sidottu useisiin eri lainsäädäntöihin ja muihin linjauksiin. Toimintaan vaikuttaa paljolti rikoslaki, jonka nojalla tuomioistuimet tekevät päätöksiä. Nämä osaltaan ohjaavat kameravalvonnan laitonta käyttöä, silloin kun kameravalvonnalla on rikottu henkilön yksityisyyttä tai kotirauhaa. Nämä päätökset ohjaavat kameranvalvonnan asentamista ja käyttämistä. Myös tietosuojavaltuutettu on kannanotoissaan linjannut milloin kameravalvonnassa syntyvä data muodostaa henkilötiedon ja käytöstä muodostuu henkilörekisteri (Tietosuojavaltuutettu, 2019b). Lisäksi Euroopan tietosuojaneuvosto EDPB on laatinut yleisen tietosuoja-asetuksen, joka tunnetaan paremmin nimestään General Data Protection Regulation ja lyhenteestään GDPR. Asetuksessa linjataan ohjeita, suosituksia ja parhaita käytäntöjä henkilötietojen käsittelylle. EDPB on myös heinäkuussa 2019 tarkentanut määritelmiä koskien henkilötietojen käsittelyä videolaitteilla (EDPB, 2019). Ohjaavat linjaukset ovat Euroopan unionin puolelta hyvinkin tuoreita, eikä niihin ole Suomessa otettu esimerkiksi tietosuojavaltuutetun puolelta kunnolla vielä kantaa.

Perustuslain (731/1999) 2§ määrittää, että julkisen vallan käyttö tulee perustua lakiin. Kameravalvontaa kuitenkin Suomessa toteuttaa niin yksityinen kuin julkinen taho. Sen lisäksi yksityistä tahoa hyödynnetään julkisen tahon puolelta niin kameravalvontajärjestelmien asennuksiin, käyttöön kuin valvontakameramateriaalin datan lähteenä. Suomessa myös useat kunnat tarjoavat kameravalvontapalveluita suoraan turvallisuusviranomaisten käyttöön, mikä mutkistaa entisestään valvonnan käyttötapauksia ja linjausten tulkintaa. Tietosuojavaltuutettu piti syyskuussa 2019 Oulun kaupungin ja poliisin valvonta-

kameroiden käyttöön liittyvää sopimusta ongelmallisena ja on pyytänyt saada asiaan ratkaisua eduskunnan oikeusasiamieheltä (Yle, 2019b).

Datan kerääminen ja siitä analysoimalla tuotettu informaatio helpottaa tietojohtoista toimintaa. Tekoälyä hyödyntämällä suurista tietomassoista saadaan suodatettua oleellista tietoa joko suoraan tai epäsuorasti analysoitavaksi. Tekoälyä voidaan hyödyntää myös strukturoimattoman datan strukturointiin, jolloin raakadatasta tehdään hakukelpoista (Physicsworld, 2019). Videovalvonnassa tämä tarkoittaa esimerkiksi kuvatun videon automaattista purkamista halutun tarpeen täyttämiseksi. Hyvin tyypillinen ja kaikkien ymmärtämä toiminto on automaattinen kasvojentunnistus, jossa videosta tunnistetaan ihmisen kasvot ja niille luodaan yksilöity matemaattinen ja hakukelpoinen malli (Norton, 2020). Kuvassa (kuvio 1) havainnollistetaan, miten datasta syntyy informaatiota ja miten se edelleen jalostuu tiedoksi ja viisaudeksi.



KUVIO 1 DIKW pyramidi (PNGwave, 2020)

Tekoälyn tuodessa uusia mahdollisuuksia kameravalvonnasta saadun datan käyttöön, laajenee toiminnasta saatu hyöty merkittävästi. Tämä tuo mukanaan kuitenkin monia tulkinnallisia kysymyksiä, joille ei löydy regulaatiosta täysin suoria vastauksia. Lisäksi käyttöä ohjaavat linjaukset ovat hyvin tuoreita, eikä niitä ole vielä kunnolla tulkittu etenkään Suomessa. Oletettavaa on myös, että tutkimuksen aikana Euroopan uniosta tulisi lisää aihetta sivuavaa ohjeistusta. Euroopan komissio on laatimassa ehdotusta tekoälyn hyödyntämisestä kameravalvonnassa. Komiteamietintö oletetaan julkaistavan 2020 alkuvuodesta. Kirjavan ohjeistuksen ja monisyisen lainsäädännön vuoksi Tampereen kaupungin Smart Urban Security and Event Resilence eli SURE-hanke haluaa teettää aiheesta tutkimuksen. Tutkimuksen avulla hanke voisi paremmin harkita erilais-

ten kameravalvontaa koskevien tekoälyohjelmistojen hyödyntämistä ja hankkimista, kehittäessään omaa kaupunkiturvallisuuttaan.

1.3 Kohdeorganisaatio

Tampereen kaupunkiin ja siihen kytkeytyviin lähiseutuihin on keräytynyt mittava määrä turvallisuusosaamista. Yhtenä Suomen isoimpana kaupunkina Tampere tuottaa myös paljon erilaisia suuria tapahtumia ympäri vuoden. Kaupunkiturvallisuuden kehittämiseksi Tampere sai rahoitusta EU:n Urban Innovative Actions -ohjelmasta. Tämän rahoituksin turvin käynnistettiin syyskuussa 2019 SURE -hanke, joka toimii tutkimuksen tilaajana. Hankkeen tarkoituksena on luoda kaupunkiturvallisuuden kokonaisratkaisu, jonka avulla ratkaisussa kehitettyjä toimintoja sekä teknologioita voitaisiin hyödyntää myös kansainvälisesti. (SmartTampere, 2019) Yhtenä vientiväylänä toimisi Tampereella vuosittain järjestettävä Smart City Week. Tampere kuuluu myös Open & Agile Smart Cities eli OASC -verkoston perustajajäseniin. Verkostossa on maailmanlaajuisesti yli 140 älykaupunkia. (OASC, 2020)

Kaupunkiturvallisuuteen linkittyy myös vahvasti sisäistä turvallisuutta ylläpitävä viranomainen eli poliisi. Kaupungin ja poliisin yhteistoimintaa on kehitetty myös kameravalvonnan osalta. Vuonna 2018 kaupunki laajensi kaupunkikameroiden määrää keskustan alueella yli kymmenellä kameralla ja jolloin kokonaismäärä kasvoi 32 kappaleeseen. Tampereen osalta kaupunki hankkii ja asentaa kamerat, mutta kameran dataa käsittelee ja hyödyntää ainoastaan poliisi. (Aamulehti, 2018). Vuoden 2018 jälkeen kameraverkostoa on entisestään laajennettu.

Kohdeorganisaation eli SURE-hankkeen kanssa käydyssä vuoropuhelussa tuli esille, että tutkimuksessa haluttaisiin tarkemmin selvitettävän EU:n ja kansallisten säännösten rajoituksia liittyen valvontakameradatan automaattiseen käsittelyyn. Painopisteinä olisi konenäköpohjaisen henkilölaskennan käyttö, hahmontunnistus ja objektianalyysi sekä biometristen tunnisteiden rajanveto liittyen erilaiseen objektianalytiikkaan.

Tutkimuksen aikataulun määrittelee kohdeorganisaation tarve. Tutkimuksen teoriaosuutta on alustavasti suunniteltu ennen tutkimuksen varsinaista aloittamista, joka voidaan määrittää tammikuuhun 2020. Tutkimuksen tuloksia jaetaan SURE-hankkeen kesken tutkimuksen edetessä ja lopullinen raportti tuotetaan kesään 2020 mennessä.

1.4 Tutkimuksen keskeiset käsitteet ja rakenne

Tutkimus pyrkii kattamaan laajasti kameravalvontaan kohdistuvia mahdollisuuksia ja sitä ohjaavaa regulaatiota. Tutkimuksen pääteemana on kameravalvonnassa käytettävän tekoälyn hyödyntämisen mahdollisuudet Suomessa. Tut-

kimuksen keskeisiä käsitteitä pyritään kuitenkin kohdistamaan kameravalvonnassa käytettävään tekoälyyn, henkilötietoihin ja yksityisyyden suojaan, lainsäädäntöön ja muuhun regulaatioon koskien kameravalvontaa sekä datan käyttöön ja jakamiseen.

Pro gradu -tutkielma on rakenteeltaan jaettu niin, että luvuissa 2-4 käsitellään tutkimuksen teoreettista viitekehystä. Luvussa kaksi keskitytään kameravalvontaan kohdistuvaan regulaatioon Suomessa ja Euroopassa. Luvussa kolme käsitellään kyberturvallisuutta ja tietojen käsittelyä sekä säilyttämistä kameravalvontajärjestelmän näkökulmasta. Luvussa neljä pureudutaan tekoälyn määritelmään ja hyödyntämisen mahdollisuuksiin kameravalvonnassa. Luvussa viisi tutkimuksen teoriaosuus nivotaan yhteen ja tarkastellaan tutkimuksen teoriaosuuden tärkeimpiä osa-alueita.

Teoriaosuuden jälkeen luvussa kuusi avataan tutkimuksessa käytettyä toteutustapa, tutkimusstrategia sekä analyysimenetelmä. Luvussa käsitellään myös aineistokeruun tapa ja metodologia sekä teemahaastattelut. Seitsemännessä luvussa kootaan yhteen tutkimuksen tulokset, johtopäätökset ja pohdinta. Viimeisessä kahdeksannessa luvussa avataan tutkimuksen johtopäätöksiä ja pohdintaa kuten mahdollisia jatkotutkimusaiheita.

Tutkimuksessa molemmat tutkijat ovat osallistuneet jokaisen osa-alueen toteutukseen. Tutkijoiden oman alaa koskevan asiantuntemuksen puolelta osa-alueita on painotettu siten, että Haaranen on pohjustanut lainsäädännöllistä ja Allonen tietoturvan puolta. Tutkijat ovat käyneet jatkuvaa vuoropuhelua aihealueiden käsittelyn osalta ja yhdessä päivittäneet sekä lisänneet kohtia jokaiseen lukuun. Haastattelut olivat myös jaettu puoliksi siten, että Haaranen suoritti haastattelut 1-5 ja Allonen 6-10.

2 LAINSÄÄDÄNTÖ JA MUUT OHJAAVAT SÄÄDÖKSET

Luvussa käsitellään kameravalvontaan liittyvää regulaatiota niin viranomaisten kuin yksityisenkin sektorin puolelta. Valvontakameroita asennetaan ja ylläpidetään paljon enemmän yksityisten tahojen toimesta. Kameroiden loppukäyttäjä ja henkilötietojen vastaanottaja on kuitenkin hyvin monesti viranomainen, joka vastaa esimerkiksi kauppakeskuksessa tapahtuneen rikoksen esitutkinnasta. Kameroista saavat lisäarvoa molemmat tahot, mutta niiden tuottaman tiedon yhteiskäyttöön on Suomessa asetettu merkittäviä rajoitteita johtuen rekisterinpitäjän velvoitteista ja vastuista.

Vielä vuonna 2008 Suomessa oli toisiksi eniten valvontakameroita Euroopassa (Suomen Kuvalehti, 2008). Turvallisuusilmapiirin muutoksen takia Keski-Euroopan maat ovat kuitenkin kasvattaneet kamerakattavuutta merkittävästi ja Suomea ei enää löydy tilastojen kärkisijoilta (Aithority, 2019). Huomioitavaa on myös se, että monista muista Euroopan maissa, kuten Ruotsissa ja Tanskassa löytyy erillinen lainsäädäntö kameravalvonnalle. Suomessa tällaista ei kuitenkaan ole, vaan toimintaa ohjaa muut kansalliset ja kansainväliset lait sekä säädökset.

Suomessa viranomaisilla toimintaa ohjaa perustuslaillinen toimivalta ja siihen sidotut omat lait, esimerkiksi poliisilaki (872/2011) ja laki henkilötietojen käsittelystä poliisitoimessa (616/2019). Näistä jälkimmäinen koki muutoksia viime vuonna, jolloin siihen sisällytettiin Euroopan unionin tietosuoja-asetuksen eli GDPR:n mukanaan tuomia uudistuksia. Lisäksi kesäkuussa 2019 poliisin ja tullin mahdollisuuksia hyödyntää biometrisia tietoja rikosten ennalta estämiseksi ja tutkimiseksi osittain tehostettiin, vastaamaan rajavartiolaitoksen vastaavia säädöksiä.

Yksityistä sektoria ei taasen rajoita toimivaltaperusteet, sillä toimintaa säädellään tarkoitusperusteen mukaisesti. Tällöin ratkaisevaa on se missä ja minkä vuoksi kameravalvontaa suoritetaan ja henkilötietoja joudutaan käsittelemään. GDPR toi myös tähän paljon muutoksia, koska kameravalvonnan tuottama data luetaan pääsääntöisesti henkilötiedoksi. Henkilötiedon käsittelijälle

tämä aiheuttaa vaatimuksia ja rekisteröidylle se mahdollistaa pääsyn omien tietojen tarkasteluun (Hanninen, Laine, Rantala, Rusi & Varhela, 2017, s. 56)

2.1 Henkilötiedot

Euroopan unionin tietosuoja-asetuksen (2016/679) eli GDPR:n 4 artiklan 1 momentin mukaan henkilötietoja ovat kaikki tiedot, jotka ovat sidottavissa tunnistettuun henkilöön tai tiedot, joilla henkilö pyritään tunnistamaan. Kameravalvontaan suhteutettuna kuva ja ääni, joista henkilö on tunnistettavissa täyttävät henkilötiedon määritteen. Samoin myös muut tiedot kuten auton rekisterinumero, paikannustiedot tai mitkä tahansa tiedot, joilla voidaan yksilöivästi tunnistaa henkilöä ovat henkilötietoja. Mikäli kamerat ovat kiinteästi ylhäältä kuvaavia, niin ettei järjestelmän avulla voida tunnistaa edes henkilön hahmoa, eikä muita tietoja yhdistelemällä voida selvittää henkilöllisyyttä, kyseessä ei ole henkilötieto. Lähtökohtaisesti uusien asennettujen valvontakameroiden tallentama data on henkilötietojen keräämistä, koska kameroiden kuvanlaatu on niin hyvä, että kameran kuva-alaan joutunut kohde voidaan siitä tunnistaa. Kameravalvontaa käytetään myös yleisesti etenkin viranomaisen puolelta henkilön tunnistamiseksi, jolloin yhdistelemällä kameradataan muita tietoja, tallenteella ollut henkilö voidaan tunnistaa. Mikäli reaaliaikaisesta videovirrasta tallennetaan ainoastaan ns. ei yksilöiviä tietoja, kuten ihmisten lukumäärä tai varsinaista videovirtaa ei tallenneta lainkaan, toiminteesta ei muodostu henkilötietorekisteriä, eikä tietosuojalakia (1050/2018) sovelleta.

GDPR:n 4 artiklan 2 momentin mukaan henkilötietojen käsittelyä on kaikki henkilötietoihin kohdistuva manuaalinen tai automaattinen käsittely, lähtien niiden keräämisestä ja tallentamisesta. Näin valvontakameran takautuvasta kuvasta tekoälyn avulla tehty tiedon indeksointi tai muu toiminta on käsittelyä, vaikka se ei tuottaisi mitään tuotosta. Vaikka käsittelyä tehtäisiin siten, että siitä muodostuisi täysin henkilötietoon kohdentamatonta tietoa, alkuperäisen materiaalin käsittelyn takia tieto perisi henkilötiedon vaateet.

GDPR:n 4 artiklan 5 momentin mukaan henkilötietojen pseudonymisoinnilla alkuperäinen henkilötieto käsitellään niin, ettei se ole enää yhdistettävissä tiettyyn rekisteröityyn. Lisäksi syntynyt aineisto on säilytettävä erillään ja hyödynnettävä sellaisia teknisiä keinoja, ettei tietoa enää voida yhdistää rekisteröityyn. Tästä huolimatta pseudonymisoidut tiedot ovat henkilötietoja, jolloin niitä käsiteltäessä on sovellettava tietosuojasäännöksiä.

Vasta anonymisoimalla tiedot, niitä ei käsitellä enää henkilötietoina. Anonymisoinnilla yhteys henkilötietoihin tulee muuttaa tunnistamattomaksi kuten tilastoksi. Rekisterinpitäjän tulee olla varma, ettei tietoa voida enää muuntaa missään vaiheessa henkilötietoihin yhdistettäväksi. Esimerkiksi kerättäessä kameravalvonnassa käytettävän tekoälyn avulla tietyn alueen ihmismäärää, tulee kerätty tilastotieto siirtää pois kameravalvontajärjestelmästä. Lisäksi tilastotiedon avulla ei saa pystyä palaamaan tiettyyn yksittäiseen tapahtumaan, joka voidaan sitoa yksittäiseen henkilötietoon. Esimerkiksi kovin tarkan tilastotie-

don avulla, mikä on sidottu tiettyyn tapahtumapaikkaan, voidaan takautuvasti selvittää yksittäisen henkilön sijaintitieto. Rekisterin pitäjän tuleekin pystyä kohtuudella ennakoimaan ja sulkemaan ne keinot pois, jotta tietoja voidaan muuttaa takaisin tunnistettavaksi myös tulevan teknisen kehityksen myötä (Tietosuojavaltuutettu, 2020).

2.1.1 Erityiset henkilötiedot

Lähtökohtaisesti erityisten henkilötietoryhmien käsittely on kiellettyä. Myös tietojen luonteen vuoksi, tietoja tulee turvata erityisen huolellisesti. GDPR:n 9 artiklan mukaan erityisiä henkilötietoja ovat:

- Henkilön rotu tai etninen alkuperä
- Yksilön poliittiset mielipiteet
- Uskonnollinen tai filosofinen suuntaus
- Ammattiliiton jäsenyys
- Geneettiset tai biometriset tiedot
- Terveyttä koskevat tiedot
- Seksuaalista suuntautumista tai käyttäytymistä koskevat tiedot

EU:n yleisen tietosuoja-asetuksen, unionin oikeuden tai erillisen kansallisen lainsäädännön nojalla erityisiä henkilötietoja voidaan käsitellä ja tallentaa. Lähtökohtaisesti kameravalvontaan liittyvien erityisten henkilötietojen käyttö pohjautuu yksityisellä ja kunnallisella puolella lähes täysin GDPR:n artikla 9a kohtaan eli henkilö on antanut siihen nimenomaisen suostumuksen. Suostumuksen perusteella erityisiä henkilötietoja voidaan käyttää vain siihen käyttötarkoitukseen, johon suostumus on annettu. GDPR:n artikla 7 mukainen suostumus on kuitenkin hyvin haasteellinen, koska se asettaa rekisterinpitäjälle paljon vaatimuksia. Käsittelijän tulee todistaa, että suostumus on annettu kirjallisesti ja siten, että suostumuksen antaja on sen oikeasti ymmärtänyt. Suostumus voidaan peruuttaa milloin tahansa ja se on oltava yhtä helppoa kuin suostumuksen antaminen. Lisäksi rekisterinpitäjän on mahdollistettava vaihtoehtoinen käytäntö, ettei biometrisia tietoja tarvitse luovuttaa, jos näin ei halua toimia. Esimerkiksi jos biometristä tietoa eli henkilön kasvokuvaa käytettäisiin konsertin sisäänpääsyn yhteydessä. Henkilö voisi luovuttaa oman kasvokuvansa järjestäjän henkilörekisteriin, jolloin hän pääsisi alueelle ilman tunnistautumista portilla. Portille asetetut kasvojentunnistukseen soveltuvat valvontakamerat päästäisivät lipun haltijat kasvojentunnistusta hyödyntäen konserttialueelle. Tapahtumanjärjestäjän tulisi kuitenkin antaa mahdollisuus henkilölle päästä konserttiin ilman kasvokuvan luovuttamista. Henkilöllisyys ja lippu tarkastettaisiin manuaalisesti toisaalla. Rekisteröity voisi missä tahansa vaiheessa pyytää kasvokuvansa poistamista järjestelmästä ja tunnistautua ilman kasvokuvaa. Järjestäjän tulisi myös varmistaa kasvojentunnistukseen kykenevä kameravalvonta alueella siten, ettei kasvokuvatunnistuksen yhteydessä käsiteltäisi sellaisia henkilöitä, jotka eivät olisi suostumusta antaneet. Toiminta ei olisi sallittua, mikäli kame-

ran avulla tallennettaisiin sellaisen henkilön biometrinen tieto, joka ei olisi suostumusta antanut ja vaikka tallennus kestäisi ainoastaan vertailun ajan (EDPB 3/2019, s. 16-17).

GDPR:n artikla 9i kohdan mukaan erityisiä henkilötietoja voisi käsitellä myös kansanterveyteen liittyvän yleisen edun vuoksi. Tällöin esimerkiksi rajat ylittävän vakavan terveysuhan torjumiseksi voitaisiin käyttää kasvojentunnistusta. Lisäksi eri viranomaisilla Suomessa on omat erityislainsäädännöt biometristen tietojen hyödyntämisestä.

2.1.2 Henkilötietojen käsittelyä koskevat periaatteet

GDPR:n viidennen artiklan mukaa käsiteltäessä henkilötietoja tulee noudattaa tiettyjä vaatimuksia.

- Käsittely on lainmukaista ja rekisteröidylle läpinäkyvää
- Keräys ja käsittely pohjautuu ainoastaan lailliseen käyttötarpeeseen
- Kerätään ja käsitellään vain tehtävään nähden tarpeellinen määrä henkilötietoja
- Tietovarannon on oltava ajantasainen
- Henkilötietoja säilötään tunnistettavassa muodossa vähimmäismäärä käyttötarpeen toteutumiseksi
- Tiedon käsittely on tietoturvallista ja luottamuksellista

Käsittelyn lainmukaisuus tarkoittaa, että ennen tiedon keräämistä eli käsittelyä tulee rekisterin perustajalla olla aina lainmukainen käsittelyperuste. Tätä perustetta ei voida kesken kaiken muuttaa tai vaihtaa toiseen, koska tällöin rekisteröidyn oikeudet eivät enää toteudu. Lakisääteiset perusteet henkilötietojen keräämiselle ovat (TSV käsittelyperusteet, 2020):

- Rekisteröidyn suostumus
- Sopimus
- Rekisterinpitäjän lakisääteinen velvoite
- Elintärkeiden etujen suojaaminen
- Yleistä etua koskeva tehtävä
- Julkinen ja valta
- Rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

Kaupungin kameravalvonnan osalta käsittelyperusteena toimii pääsääntöisesti rekisteripitäjän lakisääteinen velvoite tai yleistä etua koskeva tehtävä. Tällöin kameravalvontaa yleisesti käytetään kaupungin omaisuuden suojaamiseksi, rikosten ennalta estämiseksi ja selvittämiksi tai kaupungin henkilökunnan tai asukkaiden turvallisuuden varmistamiseksi.

Kameravalvonnassa olisi myös hyvä huomioida elintärkeiden etujen suojaaminen. Henkilötietojen käsittely olisi sallittua, jos kameravalvontajärjestelmän käsittelyperusteena olisi rekisteröidyn tai jonkin muun hengen tai tervey-

den suojaaminen. Hyvänä esimerkkinä toimii meneillään olevan koronavirusepidemian leviämisen seuranta. Myös muut terveydelle massiiviset tilanteet kuten laajan väkivallan teon toteuttaminen tai ennalta estäminen täyttäisi laillisen käsittelyperusteena. (TSV käsittelyperusteet, 2020) Tietosuojaselosteessa tulisikin tarkoin huomioida erilaiset käyttökohteet ja siihen soveltuvat henkilötietojen käsittelyperusteet. Viranomaistahon kuten poliisin tulee konsultoida tietosuojavaltuutettua, etenkin jos kameravalvonnassa hyödynnettäisiin tekoälyä yksittäisen henkilön seurantaan. Kunnallisen tahon käsittelyperuste tulee suoraan GDPR:n 6 artiklan 1 kohdan d alakohdasta, eikä näin ollen välttämättä vaatisi vanhan lain mukaista tietosuojavaltuutetun lupamenettelyä. (HE 9/2018)

Näiden lisäksi rekisterinpitäjältä edellytetään myös konkreettisia toimenpiteitä. Rekisterinpitäjän ja henkilötietojen käsittelijän henkilötietojen käsittelyyn liittyvän riskienarvion vaatimuksista säädetään GDPR:n 32 artiklassa. Artikla edellyttää, että rekisterinpitäjä ja henkilötietojen käsittelijä toteuttavat riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Artiklan velvoitteella varmistetaan myös, että henkilötietoja käsittelevät henkilöt käsittelevät niitä rekisterinpitäjän ohjeiden mukaisesti.

2.1.3 Rekisteröidyn oikeudet

GDPR:n 12 artiklassa määritetään rekisteröidyn oikeuksia omiin tietoihinsa. Nämä alla listatut oikeudet asettavat vaatimuksia rekisterinpitäjälle, jonka tulee tarjota kyseisen oikeuden käyttäminen helpoksi. Oikeudet eivät ole suoranaisia ja niitä saatetaan arvioida tapauskohtaisesti liittyen tiettyihin poikkeustilanteisiin. Lisäksi rekisteröidyn oikeuksien käyttö liittyy rekisterinpitäjän käsittelyperusteeseen, eikä niitä voi käyttää kaikissa tilanteissa. GDPR:n artiklan 12 mukaan rekisteröidyllä on oikeus:

- Saada yksinkertaisella kielellä tietoa henkilötietojensa käsittelystä
- Mahdollisuus nähdä ja oikaista sekä poistaa kerättyjä tietoja
- Tarvittaessa rajata tietojensa käsittelyä
- Halutessaan siirtää tiedot itselleen tai toiseen järjestelmään
- Vastustaa tietojensa käsittelyä
- Olla joutumatta automaattisen päätöksen tai profiloinnin kohteeksi

Kameravalvonnan osalta julkiset tietosuojaselosteet antavat kattavat tiedot henkilötietojen käsittelystä. GDPR:n 12 artiklassa korostetaan tietojen läpinäkyvyyttä ja tekstin selkeyttä eli ne tulisi olla kirjoitettu ns. kansan kielellä. Henkilölle tulee tarjota mahdollisuus saada itseään koskevia tietoja, kuten esimerkiksi kuvia kameravalvontajärjestelmästä. Huomioitavaa on kuitenkin se, että rekisterin pitäjän tulee varmistua, ettei kuvassa tai videossa ole näkyvillä tunnistettavasti muiden rekisteröityjen henkilötietoja (EDPB 3/2019, s. 19). Rekisterinpitäjän tulee vastata pyyntöön kuukauden sisällä sen vastaanottamisesta. Pyynnöstä huolimatta tietoja voidaan olla luovuttamatta, mikäli pyyntö on ilmeisen

perusteeton tai sen toteuttaminen on kohtuuton. Esimerkiksi valvontakameramateriaalin pyytäminen koko kerätyn tietovarannon ajalta ilman, että pyyntöä on rajattu tiettyyn aikaan ja paikkaan voi toimia perusteena. Rekisterinpitäjän kirjallisesta päätöksestä voi valittaa tietosuojavaltuutetulle, joka käsittelee asian. Rekisteröidylle omien tietojen tarkastaminen, poistaminen, oikaisu ja siirtäminen on lähtökohtaisesti maksutonta (2016/679).

2.1.4 Valokuva oikeudellisena kysymyksenä

Tietosuojavaltuutettu on ottanut päätöksessään (423/452/2016) kantaa valokuvan oikeudelliseen asemaan, kun puhutaan valokuvan suhteesta henkilötietoihin. Tietosuojavaltuutetun toimivalta on valokuvan suhteen siis kohtuullisen pieni, koska valokuvaa voidaan hyödyntää ja tarkastella monen muun oikeudellisen kysymyksen kautta. Henkilön henkilötietona pidetään kaikkea luonnollista henkilöä kuvaavaa asiaa, jotka voidaan liittää henkilöön tai hänen kanssaan samassa taloudessa asuvaan tahoon. Näin ollen pelkästään kuva henkilöstä ei ole ainoa henkilötieto vaan kaikki tiedot liittyen henkilön omaisuuteen tai kotiinsa, jotka voidaan yhdistää henkilöön. Kuvat esimerkiksi henkilön autosta ja sen rekisterikilvestä tai kodista ovat henkilöön liittyviä henkilötietoja. Valokuva on siis henkilötieto, mikäli henkilö on siitä tunnistettavissa. Kuva auton rekisterikilvestä on henkilöön liitettävä henkilötieto, jos samassa kuvassa on näkyvillä henkilön kasvot. Mikäli kuvassa on ainoastaan rekisterikilpi, eikä yhteyttä henkilöön, ei tieto suoraan ole sen omistajaan liitettävä henkilötieto. Tietosuojalautakunnan päätöksessä (10/2016) kuitenkin määritetään, että myös rekisterikilpi on yksittäisenäkin tietona henkilötieto. Mikäli kyseessä on kymmeniä vuosia vanha kuva, johon ei ole linkitetty henkilön nimitietoa, ei siihen sovelleta henkilötietolakia. Päätös on myös nykyisen henkilötietolain korvanneen tietosuojalain mukainen

Kaikkiin henkilötietoihin sovelletaan Suomessa kansallista tietosuojalakia, kun niitä käsitellään. Henkilötietojen käsittely vaatii henkilörekisterin laatimisen ja näin ollen tietosuojaselosteen. Tietosuojavaltuutettu ei ole toimivaltainen määrittelemään missä saa kuvata. (GDPR:n kautta kuin myös EDPB:n tulkinnoissa linjataan kameravalvontaan liittyviä kuvauskieltoja. Eduskunnan oikeusasiamies on myös joissain tapauksissa ottanut kantaa kuvaamiskieltoa koskeviin kanteluihin. Henkilöstä otettua kuvaa käsiteltäessä tulee huomioida oikeusjärjestelmän koko kokonaisuus. Kuvaan liittyy niin rikosoikeudellisia merkityksiä, kuin henkilön yksilönoikeuksiin sekä itsemääräämisoikeuksiin liittyviä juonteita. Tärkeää onkin huomioida, että Suomessa henkilötietoihin liittyviä säännöksiä on yli 600 erityislaissa (Tietosuojavaltuutettu, 2016).

2.1.5 Tietosuojavaltuutettu ja vaikutustenarviointi

Tietosuojalainsäädännön toteutumista Suomessa valvoo tietosuojavaltuutettu, jonka tarkoituksena on tehdä selvityksiä ja linjata ihmisten oikeuksien ja vapauksien toteutumista henkilötietoja käsiteltäessä. GDPR (2016/679) 35 artiklan

mukaisesti rekisterinpitäjän tulisi tehdä kirjallinen vaikutustenarviointi, jos tarkoituksena on käsitellä erityisiä henkilötietoja tai rikostuomioihin tai rikkomuksiin liittyviä henkilötietoja. Lisäksi GDPR:n 35 artiklan 3 kohdan c alakohdassa erikseen ohjeistetaan, että vaikutustenarviointi tulisi tehdä, kun henkilötietoja käsitellään uusien teknologioiden avulla tai yleisiä alueita valvotaan järjestelmällisesti ja laajamittaisesti.

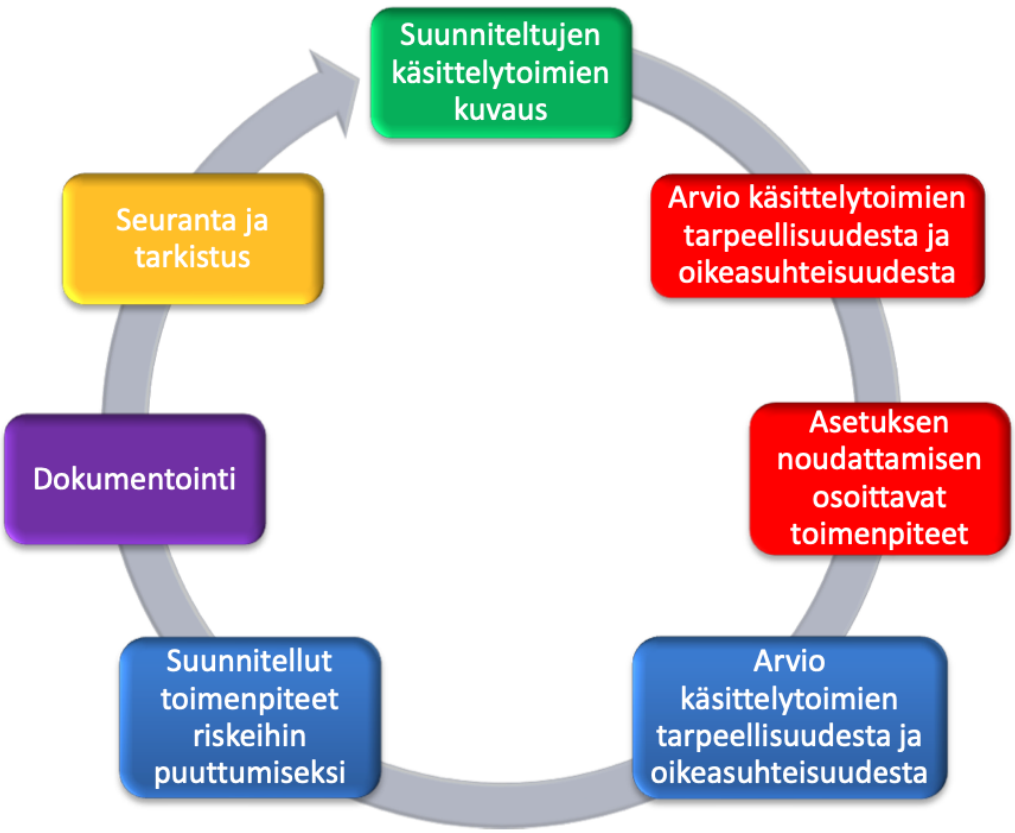
Euroopan tietosuojaneuvoston tietosuojaryhmä WP29 on riippumaton EU:n työryhmä. Tietosuojaryhmän tulkinnan mukaan, uuden tekniikan hyödyntäminen ja innovatiivisten ratkaisujen käyttö voi johtaa helposti siihen, että kerätystä datasta saadaankin luotua uutta tietoa. Lisäksi se voi luoda uusia henkilötietojen käyttötapoja. Tämä johtaa helposti henkilöiden oikeuksiin ja vapauksiin kohdistuviin korkeisiin riskeihin. Esimerkiksi kameravalvontajärjestelmän videomateriaalista tekoälyllä tehtävä tiedon indeksointi, luo normaaliin tunnistettavaan kuvaan lisää hakuparametreja. Näin yksittäiseen kuvaan, josta henkilö on tunnistettava, syntyy lisää henkilöön liittyviä tietoja. Vaikutustenarvioinnin avulla rekisterinpitäjä voi ymmärtää ja käsitellä teknologian käytöstä syntyviä uusia riskejä. (17/FI, 2017, s. 12)

Tietosuojaryhmän WP29 tulkinnan mukaan yleisellä alueella tarkoitetaan paikkaa, jossa henkilön on vaikea tietää kuka heitä koskevia tietoja kerää. Lisäksi henkilön on vaikea julkisella paikalla välttää joutumatta valvotulle alueelle. Esimerkkeinä tällaisista julkisista paikoista ovat, aukiot, torit ostoskeskukset tai jotkin muut julkiset tilat kuten kirjasto. Kysymys siitä mitä laajamittainen henkilötietojen käsittely on, ei ole tarkkaan määritelty. Toiminnassa kuitenkin otetaan huomioon kasautuvien henkilötietojen ja eri rekisteröityjen määrä, käsittelytoimen kesto sekä maantieteellinen ulottuvuus. Tärkeää on myös huomioida, että erilaisten tietoaineistojen yhdistäminen jo kahdesta eri tarkoituksiin tarkoitetusta lähteestä voi vaatia vaikutustenarvioinnin. Etenkin silloin kun rekisteröity ei välttämättä miellä, että hänestä kasattuja tietoja voitaisiin yhdistää (17/FI, 2017, s. 10-12). Tällainen tietojen yhdistäminen voisi esimerkiksi tapahtua kun, henkilöllä käytössä olevan kaupungin julkisen liikenteen sovelluksen sijaintitietoja sovitettaisiin kaupungin kameravalvontajärjestelmän dataan. Perussääntönä voidaankin pitää, että mikäli kaupungilla on käytössä kameravalvontajärjestelmiä, niistä tulisi nykylainsäädännön mukaisesti laatia vaikutustenarviointi.

Tietosuojatyöryhmän ohjeistuksessa (17/FI, 2017) kunnalliset tahot voivat kuitenkin tehdä yhden yhteisen arvioinnin, mikäli esimerkiksi kunnan alueella eri viranomaisten tarpeisiin kerätään valvontakameroiden avulla samanlaisia henkilötietoja. Näin esimerkiksi Tampereen kaupunki voisi kerätä ja käsitellä yhden videohallintajärjestelmän avulla eri tahojen tarpeisiin materiaalia tai käyttää useita eri järjestelmiä hajautetusti. Kamerajärjestelmien sulauttamista ja hallinnointia ei rajata alueellisesti. Mikäli rekisterinpitäjällä on tarve hyödyntää kameravalvontajärjestelmää esimerkiksi kuntayhtymään kuuluvissa kaupungeissa, se voidaan hoitaa yhden vaikutustenarvioinnin kautta. Samassa järjestelmässä voi olla myös sidottuna muita tahoja yhteisrekisterinpitäjiksi, esimerkiksi poliisi. Mitä laajempi ja hajanaisempi järjestelmä sekä sen käyttäjäkunta on,

sitä tarkemmin on vaikutustenarvioinnissa määritettävä rekisteriinpitoon osallistuvien tahojen velvollisuudet ja tehtävät. Tietosuojavaltuutetulle tulisi kirjallisesti selvittää eri osapuolien erilaiset riskit koskien henkilötietojen käsittelyä ja kuvata järjestelmään kerättyjen rekisteröityjen oikeuksien toteutuminen. On myös tärkeää perustella, miksi järjestelmiä hyödynnetään yhdessä ja niistä tehdään yksi koottu vaikutustenarviointi (17/FI, 2017, s. 8-10).

Vaikutustenarviointia ei tarvitse tehdä, mikäli vastaavanlaisesta toiminteesta asia on jo valvontaviranomaisen puolelta tutkittu (17/FI, 2017, s. 8-11). Rekisterinpitäjän pitää kuitenkin laatia uusi vaikutustenarviointi, mikäli henkilötietojen käyttötarkoitus muuttuu esimerkiksi uuden teknologian tai haavoittuvuuden myötä. Tämän vuoksi rekisterinpitäjän on huolehdittava vaikutustenarvioinnin ajantasaisuudesta. Se ei siis ole yksittäinen prosessi, vaan vaikutustenarviointi on aloitettava jo ennen varsinaista henkilötietojen käsittelyä ja hyödynnettävä välineenä koko prosessin ajan (17/FI, 2017, s. 16). Kuviossa 2 on tarkemmin kuvattuna vaikutustenarvioinnin prosessi.



KUVIO 2 Tietosuojaryhmän WP29 suositus vaikutustenarviointiprosessista. (17/FI, 2017)

2.2 Rikoslaki

Suomessa kameravalvonnan suhde lakiin on lähinnä määrittelyä siitä, milloin toiminta muodostuu laittomaksi. Rikoslain (39/1889) 24 luvussa on säädetty kameravalvontaa rajaavia säädöksiä, jotka koskevat yksityiselämään loukkaavan tiedon levittämistä, salakatselua sekä salakuuntelua. 38 luvussa otetaan kantaa tieto- ja viestintärikoksista, joita voidaan soveltaa nykyajan kameravalvontajärjestelmiin. Laissa myös linjataan oikeudettoman sijainnin määreitä eli kotirauhan suojaamaa paikkaa sekä julkisrauhan lainsäädännöllistä piiriä. Tärkeää on myös huomioida rikoslain (39/1889) 38 luvun 9 §:n tietosuojarikos sekä 47 luvun 1§:n työturvallisuusrikos.

2.2.1 Salakatselu ja -kuuntelu sekä niiden valmistelu

Rikoslain (39/1889) 24 luvun 6§:n mukaan salakatseluun syyllistyy henkilö, joka oikeudettomasti katselee tai kuvaa toista henkilöä teknisellä laitteella. Kuvauksen tulee tapahtua kotirauhan suojaamassa paikassa, käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa. Tärkeää on huomioida teknisen laitteen määritelmä, jota on hallituksen esityksessä (HE 184/1999, s. 27) kuvattu kamerana, kiikarina ja videokamerana tai niihin rinnastettava laitteena. Kuvauksen tulee olla myös oikeudetonta siten, että se loukkaa kohteen yksityisyyttä. Yksityisyydensuoja ei kuitenkaan ulotu tahoon, jolla ei olisi muuten oikeutta olla valvotussa tilassa esimerkiksi tilanteessa, jossa henkilö murtautuu luvatta suljettuun tilaan.

Valvontakameran ei välttämättä tarvitse tallentaa varsinaista kuvaa vaan millä tahansa tekniikalla tuotettu informaatio lasketaan kuvaamiseksi, jos se myöhemmin voidaan saattaa kuvan muotoon. Kaupunkien käyttämät kamerat kuvaavat yleisesti julkisia paikkoja, kuten toreja ja katuja, jotka eivät sisälly yksityisyyden suojan piiriin. Tähän rinnastettavia paikkoja ovat myös muut julkiset paikat kuten kaupat tai pankit. Rangaistavuuden osalta tulisi kiinnittää huomiota kuvauksen kestoon sekä kuvattavan ja kuvaajan suhteeseen. Julkinen kameravalvonta, jonka alaisuuteen joutuu ohimenevästi, eikä se ole kohdistettu suoranaisesti kehenkään, ei yleisesti olisi pidettävä rangaistavana (HE 184/1999, s. 28).

Kaupunkikameroiden käyttö poliisin työkaluna tietyn rikoksen tai rikoksentekijän seuraamiseksi sekä tunnistamiseksi, rikosten ennalta estämiseksi tai paljastamiseksi olisi poliisilain 4 luvun 1§:n mukaisesti teknistä valvontaa. Valvonta ei saa kohdistua suunnitelmallisesti keneenkään, mutta jos henkilö itse päätyy paikkaan, jossa sijaitsee yleisvalvontaan tarkoitettuja valvontakameroita, voidaan niitä hyödyntää yksittäisen kohteen tarkkailuun sen ajan, kun henkilö on laitteiden toiminta-alueella (HE 57/1994, 28).

Rikoslain (39/1889) 24 luvun 5§:n mukaan salakuunteluun syyllistyy henkilö, joka oikeudettomasta kuuntelee tai tallentaa keskustelua, puhetta tai yksityiselämästä kantautuvaa ääntä. Ääni pitää tallentaa tai sen pitää syntyä koti-

rauhan suojaamasta paikasta. Paikka ei kuitenkaan pelkästään rajoitu kotirauhan suojan piiriin. Salakuunteluun voi syyllistyä myös silloin kun esimerkiksi puhetta ei ole tarkoitettu muun ulkopuolisen tietoon ja se on kuultu sellaisessa paikassa, jossa muiden ei oletettaisi sitä kuulevan (HE 184/1999, s. 25-26).

Rikoslain (39/1889) 24 luvun 7§:n mukaan salakuuntelun ja -katselun valmistelu on rangaistavaa. Rikoksen tunnusmerkistö täyttyy, kun katseluun tai kuunteluun käytetty tekninen laite on asennettuna toimintavalmiiksi. Teon on kuitenkin osoitettava rikollista tarkoitusta (HE 184/1999, 30).

Nykyiset valvontakamerat ovat monisensorisia omia tietokoneitaan, joissa voidaan itsenäisesti suorittaa paljon erilaisia toimia kuvamateriaalin tallentamisen lisäksi. Sen vuoksi onkin tärkeää huomioida, että kyseinen rikoslain pykälä ottaa huomioon myös salakuuntelun. Videokuvaukseen tarkoitettu kamera voidaan sijoittaa oikeaan paikkaan ilman, että se kuvaa kotirauhan suojaamaan paikkaan. Myöhemmin kameran muita ominaisuuksia otettaessa käyttöön voi datan sekaan kuitenkin päätyä laitonta materiaalia. Tällainen esimerkki kaupunkikamerasuunnittelussa voisi tulla kyseeseen, kun asuinrakennuksen seinään kiinnitetään kamera kuvaamaan toria. Myöhemmin kameran mikrofonia hyödynnettäisiin esimerkiksi tekoälyllä tehtävään aseen laukauksen tunnistamiseen. Kamera läheisyydessä olevalta parvekkeelta kuitenkin kantautuisi kameran mikrofoniin keskustelua asunnon sisältä. Valmistelupykälä täyttyisi jo pelkästään tällaisen monisensorisen kameran asennuksen yhteydessä, toki rikoksesta epäillyn motiivia ja teon rikollista tarkoitusta punnittaisiin tarkasti.

2.2.2 Yksityiselämää loukkaavan tiedon levittäminen

Tarkasteltaessa kameravalvontaa rikoslain (39/1889) 24 luvun 8§:ssä säädetyn yksityiselämää loukkaavan tiedon levittämisen kautta, tulee se kyseeseen lähinnä silloin, kun valvonnasta saatu tallenne tai kuva jaetaan eteenpäin. Sosiaalinen median aikakaudella hyvin tyypillinen tapa onkin julkaista kuva internetissä tai hyödyntää jotain suoratoistopalvelua kuvavirran jakamiseksi muille. Teko täyttyy, kun yksityiselämää koskeva tieto on saatettu lukuisten ihmisten saataville esimerkiksi tietoverkkoon. (HE 184/1999, s. 31) Julkisilla paikoilla tapahtuva kuvaus, jonka kohteeksi henkilö joutuu satunnaisesti, ei kuitenkaan pidetä yksityisyyttä loukkaavana. Uutisissa voi esimerkiksi näyttää julkisilla paikoilla kuvattua materiaalia ilman henkilön omaa suostumusta. Tapauksissa, joissa henkilön toiminta on poikkeavaa tai liittyy hänen erityispiirteeseensä, tulisi kuvauksen kohteelta pyytää suostumus (Nuutila & Majanen, 2009, s. 654).

Verkossa on paljon palveluita, joiden kautta pystyy tarkastelemaan huonosti suojattuja tai jopa täysin julkista valvontakameroiden reaaliaikaista kuvaa. Tällaisen materiaalin toimittaminen on jo laajalti muiden nähtävissä verkossa, mikä sinänsä täyttää rikoksen tunnusmerkistön, jos materiaalissa olisi yksityiselämää loukkaavaa materiaalia. Helsingin hovioikeuden päätöksessä (R 18/2685) on kuitenkin linjattu, että yksityiselämää loukkaavan tiedon levittämistä koskeva rikos on vain tahallisena rangaistava. Viranomaiskäytössä olevan valvontakameran tietoturvan noudattamatta jättäminen toki voisi poikia muita

sanktioita, kuten moitteita tietosuojavaltuutetulta tai jopa täyttää tietosuojarikoksen tunnusmerkistön.

2.2.3 Salassapitorikos ja -rikkomus

Rikoslain (39/1889) 38 luvun 1§:ssä säädetty salassapitorikos ja sen lievempi muoto 2§:ssä salassapitorikkomus voi tulla kysymykseen, kun kameravalvontajärjestelmän rekisterinpitäjä tai tiedon käsittelijä paljastaa tai käyttää tietoa omaksi tai toisen hyödyksi salassapitovelvollisuuden vastaisesti. Tiedon käsittelyyn liittyvät velvollisuudet on otettava huomioon järjestelmää suunniteltaessa ja sovittava kirjallisesti tapauskohtaisesti, mikäli käsittelijä on esimerkiksi palveluntarjoaja tai organisaation ulkopuolinen taho (39/1889) Vuosikellomainen lokitietojen tarkastelu on yksi mahdollisuus kontrollille organisaation sisällä suoritettavaksi ns. insider-riskin välttämiseksi.

2.2.4 Viestintäsalaisuuden loukkaus ja törkeä viestintäsalaisuuden loukkaus

Kameravalvontajärjestelmän osalta viestintäsalaisuuden loukkaus, josta säädetään rikoslain (39/1889) 38 luvun 3§:ssä ja 4§:ssä sen törkeästä tekomuodosta, voi tulla kysymykseen esimerkiksi tietomurtojen tai -vuotojen yhteydessä. Rikoslaki määrittelee, että jos oikeudettomasti hankkii tiedon tietojärjestelmässä välitettävänä olevan puhelun-, sähkeen-, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta. Rikoksen törkeä tekomuoto edellyttää luottamusaseman hyväksikäyttöä, teknisiä erikoislaitteita tai tietojenkäsittelyohjelmaa, viestin sisällön erityistä luottamuksellisuutta ja rikos on oltava kokonaisuudeltaan arvostellen törkeä toteutuakseen. Rikoksen yritys on määritelty rangaistavaksi molemmissa tekomuodoissa. (39/1889)

2.2.5 Tietoliikenteen häirintä ja törkeä tietoliikenteen häirintä

Kameravalvontajärjestelmien tietoliikenteen häirinnästä ja sen törkeästä tekomuodosta säädetään rikoslain (39/1889) 38 luvun 5§:ssä ja 6§:ssä. Kameravalvontajärjestelmät voivat olla erityisen alttiita häirinnälle, ellei niiden tietoturvallisuuteen kiinnitetä riittävästi huomiota jo suunnitteluvaiheessa. Erilaiset palvelunestohyökkäykset ovat nykypäivänä osa digitalisaation arkea ja haavoittuvia järjestelmiä etsitään eri toimijoiden toimesta. Järjestelmät koostuvat monesti usean toimittajan laitteista tai osista, joka tekee niiden turvallisuuden hallinnasta monesti hankalaa. Törkeän tekomuodon täyttyminen vaatii erityisen luottamusaseman hyväksi käyttämistä, ihmishengen turvaavan hätä-, tele- tai radioviestinnän häirintää, rikoksen tekemistä erityisellä laitteella tai ohjelmakäskyjen sarjana, osallistumista järjestäytyneen rikollisryhmän toimintaan, aiheutetaan erityisten tuntuvaa haittaa tai taloudellista vahinkoa tai kohteena on yhteiskun-

nan tärkeän toiminnon kuten energianhuollon, terveydenhuollon ja oikeudenhoidon tai muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon. Lisäksi häirintä on oltava kokonaisuutena arvostellen törkeätä. (39/1889)

2.2.6 Tietojärjestelmän häirintä ja törkeä tietojärjestelmän häirintä

Joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla näihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, voidaan rikoslain (39/1889) 38 luvun 7a§:n ja 7b§:n mukaan tuomita tietojärjestelmän häirinnästä tai sen törkeästä tekomuodosta. Osana digitalisaation arkea ovat tulleet myös useat erityyppiset haittaohjelmat, joita pyritään etua tavoittelevien toimesta saada asennettua haavoittuviin tietojärjestelmiin. Kiristyshaittaohjelmat ovat globaali ilmiö, joista on vaarallisia esimerkkejä useilta eri aloilta. Yhtenä ehkä tunnetuimpana haittaohjelmana voidaan pitää vuonna 2010 löydettyä Stuxnetiä, jonka avulla sabotoitiin onnistuneesti Iranin ydinohjelmaa. (Tivi, 2019)

2.2.7 Tietomurto ja törkeä tietomurto

Rikoslain (39/1889) 38 luvun 8§ ja 8a§ määrittelevät tietomurron ja törkeän tietomurron tunnusmerkistön seuraavasti: joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka muutoin oikeudettomasti tunkeutuu tietojärjestelmään tai sellaisen osaan, jossa käsitellään sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, tuomitaan tietomurrosta. Rikoksen törkeä tekomuoto edellyttää, että teko tehdään osana järjestäytyneen rikollisryhmän toimintaa tai se tehdään erityisen suunnitelmallisesti ja lisäksi sen pitää olla kokonaisuutena arvostellen törkeä. Yhä useamman digitaalisen rikoksen taustalla on tietomurto, tietojenkalastelu tai osia niistä yhdistettynä muihin keinoihin. Rikollisilla keinoilla saavutettuja hyötyjä ja erityisesti dataa sen eri muodoissaan voidaan hyödyntää myöhemmin rikollisen toiminnan eduiksi. (39/1889)

2.2.8 Tietosuojarikos

Aiemmassa lainsäädännössä ollut henkilötietorekisteririkos on rikoslain (39/1889) 9 §:n mukaan korvautunut tietosuojarikoksella. Tietosuojarikoksen tunnusmerkistön täyttävässä teossa pitää käsitellä tahallaan tai törkeästä huolimattomuudesta henkilötietoja vastoin eri henkilötietolaissa tarkemmin kuvattuja käyttötarkoitussidonnaisuuksia. Henkilötietoja saa siis käsitellä vain sen käyttöoikeusperusteen mukaisesti mihin niitä on lakisääteisesti hankittu. Henkilötietojen käsitteleminen on niiden hankkimista ja vastaanottamista, luovuttamista tai siirtämistä. Teon on myös loukattava rekisteröidyn yksityisyyden suojaa tai aiheutettava hänelle vahinkoa. Tärkeää on myös huomioida, että ri-

kokseen voi syyllistyä, mikäli tahallaan tai törkeästi huolimattomuudesta jättää huolehtimatta henkilötietojen käsittelyn turvallisuudesta.

Kameravalvonnan osalta tietosuojarikokseen voi syyllistyä rekisterinpitäjän roolissa keräämällä sellaisia tietoja, joihin ei ole käyttöperustetta. Esimerkiksi tekoälyn avulla luotaisiin uusia erityiseksi henkilötiedoiksi rinnastettavia tietoja henkilön fyysisistä ominaisuuksista. Tällöin kameravalvonnan dataan voitaisiin tehdä hakuja järjestelmästä hankitun yksilöivän kuvan perusteella. Tekoälyalgoritmin perusteena kuvahaussa toimisi henkilön biometrisia tietoja kuten kasvokuva. Kyseessä voisi olla myös muita hahmon kautta saatavia henkilön yksilöiviä tietoja kuten kävelytyyli. Vaikka takautuvasti esimerkiksi poliisilla voisi olla rikoksen tutkimiseksi oikeus käsitellä biometrisia tietoja, niiden taltioimishetkellä kyseistä perustetta ei olisi ollut. (HE 9/2018)

Rangaistavaa olisi myös tietojen urkinta. Esimerkiksi henkilöllä, jolla olisi pääsyoikeus rekisterin pitämiin henkilötietoihin tarkastelisi sellaisia tietoja, joihin hänellä ei olisi tehtävään sidottua käyttöoikeusperustetta. (HE 9/2018). Mediassa on useasti ollut tapauksia, joissa poliisi tai terveydenhoitohenkilökunta on katsonut julkisuuden henkilöön liittyviä tietoja, vaikka he eivät ole olleet tapaukseen millään tavalla kytköksissä ja tätä kautta saaneet perustetta käsitellä kyseisiä henkilötietoja. Kameravalvonnan osalta tärkeää olisi eriyttää henkilöiden järjestelmän käyttöoikeudet siten, että ne ovat sopusoinnussa käsittelyperusteen kanssa. Järjestelmän käytön valvontaa helpottaisi myös käsittelyperusteiden kirjaaminen suoraan järjestelmään tapahtumahetkellä, jotta käyttöperuste jäisi talteen järjestelmän lokeihin. Toiminta lisäisi niin käyttäjän kuin rekisterinpitäjän oikeusturvaa.

2.2.9 Työturvallisuusrikos ja -rikkomus

Työturvallisuuden osalta rangaistavaan toimintaan voi syyllistyä niin rikoslain 47 luvun 1 §:n työturvallisuusrikoksen kuin työturvallisuuslain (738/2002) 8 luvun 63 §:n työturvallisuusrikkomuksen kautta. Kameravalvonnan osalta työturvallisuusrikos tulisi lähinnä kyseeseen silloin kun työpaikalla olisi kohonnut väkivallan riski. Tällöin työnantajan pitäisi huomioida työturvallisuuden erillisiä turvajärjestelyitä, joissa valvontakamerat ovat osaltaan merkittävässä roolissa niin tilanteiden ennalta estämiseksi kuin niiden selvittämiseksi. Käytössä oleva kameravalvontajärjestelmä pitäisi olla toimiva ja tarkistettu sekä sen käyttö ohjeistettua sekä vastata tarvetta. (HE 59/2002) Työturvallisuuden näkökulmasta järjestelmän osaavia käyttäjiä olisi hyvä olla riittävästi. Lisäksi niin reaaliaikaisen kuin takautuvan materiaalin tarkastelu työturvallisuusrikosten ennalta estämiseksi ja selvittämiseksi olisi tärkeää. Toimintaa voitaisiin entisestään tehostaa tekoälysovelluksin, jolloin materiaalin käsittely nopeutuisi. Rekisterinpitäjän, joka pääsääntöisesti on työnatajanataho, vastuulla olisi myös se, että videomateriaalia säilytettäisiin tarpeellisen ajan. Työnantajaa sitova työturvallisuuslaki voikin toimia osittain perusteena sille, miksi materiaalia olisi tarpeellista säilyttää pidempään kuin muutama päivä tai sen läpikäymistä voitaisi helpottaa tekoälysovelluksin.

2.3 Euroopan unionin jäsenvaltioihin liittyvä regulaatio

Euroopan unioni ja sen jäsenmaat toteuttavat annetun toimivallan periaatetta, jossa tietyiltä osin jäsenvaltiot ovat luovuttaneet päätöksentekovaltaansa unionille. EU:sta voidaan ohjata osittain kansallista lainsäädäntöä kolmiportaisesti. Asetustasolla kuten GDPR, jäsenmaat soveltavat asetusta sellaisenaan, kun taas direktiivit ovat kansallista lainsäädäntöä tukevia ohjeistuksia. Lisäksi regulaatiota täydentää EU tuomioistuimen päätökset, joilla on sitova velvoite niille, joihin päätökset kohdistuvat. Lisäksi nämä päätökset linjaavat Euroopan unionissa toteuttavaa lainsäädäntöä (Ulkoministeriö, 2020).

Euroopan tietosuojaneuvosto eli EDPB pyrkii varmistamaan EU:n alueella tietosuojasääntöjen yhdenmukaisesta soveltamisesta niin yksityisten toimijoiden kuin viranomaisten puolella. EDPB koostuu kansallisten tietosuojaviranomaisten kuin Euroopan tietosuojavaltuutetun EDPS edustajista. EDPB tuottaa tietosuojalainsäädäntöä koskevia yleisiä ohjeistuksia jäsenmaille, mutta myös neuvoo Euroopan komissiota henkilötietojen suojaukseen liittyvässä lainsäädännössä. EDPB on tehnyt myös suoraan kameravalvontaan koskevia ohjeistuksia (EDPB, 2020).

2.3.1 EDPB:n ohjeistus koskien kameravalvontaan

EDPB on julkaissut tammikuussa 2020 ohjeistuksen, jossa annetaan suuntaviivoja videovalvonnassa prosessoitavien henkilötietojen käsittelystä (EDPB 3/2019). Kameravalvonnan laajentuminen ja siinä hyödynnettävä tekoälyn kehittyminen ovat tuoneet uudenlaisia riskejä, joiden vuoksi EU-tasolta pyritään yhdenmukaistamaan hajanaisia käytäntöjä. Ohjeistus on kuitenkin vain suuntaa antava ja pyrkii tuomaan esille rekisterinpitäjille riskienarvioinnin ja tietosuojakäytäntöjen tärkeyttä. Henkilötietoja keräävien ja käsittelevien tahojen tulisi paremmin arvioida ja kuvata omia prosessejaan, jotta turhalta ja ylimääräiseltä tietojenkäsittelyltä vältyttäisiin.

Ennen kameravalvonnan käyttöönottoa rekisterinpitäjän tulisi arvioida onko kameravalvonnan käyttö tarpeellista ja voitaisiinko siitä saatu hyöty toteuttaa jollain muulla keinoin ilman, ettei henkilötietoja tarvitsisi kerätä. Lisäksi tulisi yksilöidä kameroiden käyttötapaukset yksittäisen kameran tai samankaltaisten kameraryhmien osalta. Esimerkiksi samaan järjestelmään liitetyt ulkoalueelle kuvaavat julkisten paikkojen yleisvalvontaan tarkoitetut kamerat, sisälle kuvaavat kamerat ja liikuteltavat dronet olisi eroteltava. Lisäksi näiden käsittelyperuste tulisi dokumentoida. Käsittelyperusteen tulisi kuvata juuri kyseisen kameran tarpeellisuus oikean elämän ongelman ratkaisemiseksi. Tämä tarve pitäisi pohjautua faktoihin. Esimerkiksi alueen rikos- tai häiriötilastoihin (EDPB 3/2019, s. 7-10).

Kerättäessä henkilötietoja pohjautuen henkilön suostumukseen, tulisi rekisterinpitäjän huolehtia siitä, että valvonta kohdistuu ainoastaan niihin tahoihin, jotka ovat suostumuksensa antaneet. Esimerkiksi käytettäessä biometrista

tunnistautumista sisäänkäynnin yhteydessä, tulisi tapahtumanjärjestäjän ilmoittaa asiasta etukäteisesti. Lisäksi pitäisi varata niille henkilöille, jotka eivät ole antaneet suostumusta ko. toiminnalle, mahdollisuus päästä sisälle tiloihin toista reittiä pitkin. Suostumuksen käyttöä henkilötietojen keräämisen kannalta tulisi muutenkin arvioida hyvin tarkasti, jotta henkilöllä on oikea vapaaehtoisuus toiminnan kannalta ja lisäksi henkilö voi päättää suostumuksensa, milloin tahansa (EDPB 3/2019, s. 14).

Videojärjestelmät keräävät isoja määriä henkilötietoja ja niiden avulla voidaan kohdistaa valvontaa, sekä luoda yksittäisestä henkilöstä hyvinkin yksilöiviä tietoja. Tällaisia voivat olla henkilön liikkeet, asuinpaikka ja ulkonäkö. Tämä ei kuitenkaan tarkoita sitä, että videomateriaali luokiteltaisiin pääsääntönä GDPR:n artikla 9 mukaan erityiseksi henkilötietoluokaksi. Henkilöä yksilöivät piirteet kuten vaatetus tai henkilön liikkumiskyvyn rajoitteet, eivät ole erityisiä henkilötietoja. Mikäli videomateriaali sisältää henkilöiden poliittisia mielipiteitä, esimerkiksi mielenosoituksiin osallistumisen, voi materiaali olla luokiteltavissa erityiseksi henkilötiedoksi. GDPR:n artikla 9:ssä erityisiä henkilötietoja voi käsitellä, mikäli henkilö on itse ne julkaissut. Julkiselle paikalle asennetun ja siitä ilmoitetun kameran kuvausalueelle saapumista, ei kuitenkaan voida suoraan pitää poliittisen mielipiteen julkaisemisena (EDPB 3/2019, s. 17).

Biometrinen tieto ja etenkin kasvontunnistus luo korotetun riskin kohdistuen henkilöön ja hänen oikeuksiinsa. Käytettäessä kyseisiä ohjelmistoja tulisi tarkkaan harkita niiden käytön tarpeellisuus ja datan käytön minimointi. Raaka videomateriaali ei ole biometristä tietoa. Materiaalista muodostuu biometrinen tieto, kun henkilön fysiologisista piirteistä tai käyttäytymisestä luodaan laskennallinen malli, jonka avulla henkilö voidaan yksilöidä. Henkilön piirteet kuten ikä, sukupuoli tai muut hahmoon liittyvät tiedot eivät ole erityisiä henkilötietoja, mikäli niiden avulla ei voida uniikisti yksilöidä tiettyä henkilöä. Biometrisia tietoja ei voi ilman laillista perustetta käsitellä ja vertailla. Pääosin julkisella puolella vertailua voi tehdä henkilön suostumuksella, mutta järjestelmän ylläpitäjän tulee varmistua siitä, että kasvontunnistuskameran kuva-alaan ei saa joutua yhtään sellaista henkilöä, joka ei ole suostumusta tähän antanut. Jo pelkkä vertailu tallennettuihin suostumuksella saatuihin biometrisiin tietoihin on GDPR:n mukaan laitonta, mikäli sitä toteutetaan sellaisten ihmisten osalta, joilta suostumusta ei ole saatu (EDPB 3/2019, s. 18-20). Suomessa vain tietyt viranomaiset voivat erityislainsäädännöllisin perustein ja hyvin rajatuissa käyttötapauksissa käsitellä biometrisia tunnisteita ilman rekisteröidyn suostumusta.

Biometrisen tiedon tallentaminen vaatii erityisiä toimia. Ensinnäkin kerättävän datan määrä pitää minimoida, jotta raakakuvasta taltioidaan vain ne tiedot, joita käytetään biometrisen mallinteen luomiseksi. Tallennettuun tietoon tulee olla rajattu ja valvottu pääsy sekä palvelintilan tulee olla suojattu. Mikäli rekisteröidyllä itsellään tarvitsee säilyttää vertailukuvaa, se tulee säilyttää ainoastaan hänen omassa fyysisessä laitteessansa ja vain poikkeustilanteissa se voidaan tallentaa palvelimelle. Palvelimille tallennetut biometriset tiedot tulee jakaa säilytettäviin ja siirrettäviin, raaka kuvamateriaali ja biometrinen vertailukuva tulee tallentaa erillisiin tietokantoihin mieluusti kryptattuna. Lisäksi tieto-

ja pitää murtosuojata ja varmistaa ettei tietoihin ole ulkopuolista pääsyä. Tietoihin olisi hyvä liittää myös uniikki yksilöivä tieto, jotta hävinneiden tietojen löytyessä niiden alkuperäinen sijainti olisi tiedossa. Biometrisen raakadatan kuten kuvien tai äänen osalta riski tietomurrolle on vielä biometrista vertailutietoa suurempi, koska raakadatasta voidaan luoda uusia biometrisia tietoja. Vertailutiedot ovat taas yleensä vain tietyn ohjelman ja algoritmin avulla hyödynnettävissä. Raakadataan kannattaisi kohdentaa tiedoston vesileimausta (EDPB 3/2019, s. 21).

Kameravalvonnasta tulisi ilmoittaa ennen kuin henkilö joutuu kuvattavalle alueelle. Ilmoittaminen olisi suotavaa tapahtua kahdessa vaiheessa, jossa ensimmäisessä vaiheessa henkilölle ilmoitettaisiin kyltein, että alueella suoritetaan valvontaa. Kyltissä olisi myös hyvä olla tieto kuka valvonnasta vastaa ja mistä henkilö voisi hakea asiasta lisätietoa. Toisessa vaiheessa henkilöllä olisi mahdollisuus saada fyysinen lappu suoritettavasta valvonnasta. Tätä lappua voitaisi jakaa esimerkiksi jonkun keskitetyn sijainnin kuten infopisteen kautta. Tiedot olisi hyvä olla myös digitaalisesti saatavilla (EDPB 3/2019, s. 22-24).

Tiedon tallentamisen osalta dataa ei saisi säilyttää kuin sen aikaa mikä on tarpeellista käyttöperusteen täyttymiseksi. Normaaleissa tilanteissa kameravalvontamateriaali olisi syytä kyetä käymään läpi 72 tunnin sisällä tapahtuneesta. Mikäli dataa säilötään enemmän kuin muutaman päivän ajan, tulisi se olla erillisesti perusteltua ja sidottu tallentamisen laillisuusperusteeseen. Myös tallentamisen osalta käyttöoikeuksien sitomien tiettyihin osiin tallenteita tulisi perustella ja arvioida käyttöoikeuksittain (EDPB 3/2019, s. 24). Mikäli tallenteita olisi, esimerkiksi rikosten selvittämisen osalta, säilytettävä selkeästi pidemmän aikaa, tulisi tieto säilöä ns. mustaan laatikkoon. Menetelmän avulla tietyn ajan päästä tallennuksesta, tietoon ei pääsisi käsiksi kuin vasta siinä vaiheessa, kun peruste asialle ilmenisi (EDPB 3/2019, s. 11).

2.3.2 Ruotsin tietosuojavaltuutetun päätös liittyen kasvontunnistukseen

Ruotsin tietosuojavaltuutettu SDPA määräsi Anderstorpin yläasteen sakkoihin GDPR:n (2016/679) vastaisesta toiminnasta 20.8.2019. Kouluun oli hankittu kasvojentunnistusohjelma helpottamaan seurantaa siitä, ovatko oppilaat läsnä opetuksessa. Toiminta oli jatkunut testauksen muodossa kolmen viikon ajan ja valvonta oli kohdistunut 22 oppilaaseen. Kasvojentunnistuksen järjestämiseksi koulun oppilaista oli huoltajan suostumuksella rekisteröity järjestelmään kasvojen vertailukuva ja profiiliin oli lisätty henkilön etu- ja sukunimi. Oppilaita kuvattiin valvontakameroilla heidän saapuessaan luokkaan. Kasvontunnistustietokonetta säilytettiin lukitussa kaapissa, ilman internet-yhteyttä. Oppilaitoksen perusteena biometristen tietojen hyödyntämiseksi oli ajansäästö. Joka tunnin alusta meni n. 10 minuuttia paikallaolevien selvittämiseen ja kirjaamiseen. Teknologian avulla arvioitu aikasäästö olisi ollut vuosittain 17280 tuntia (SDPA, 2019, s. 2-3).

Päätöksessä todettiin, että jo järjestelmän testausvaihe edellyttää rekisterinpitäjää samalla tavoin kuin järjestelmää käytettäisiin tuotannossakin. Bio-

metristen tietojen käsittelyperuste pohjautui oppilaiden ja huoltajien suostumukseen. Koska oppilaiden asema koettiin olevan riippuvainen julkisesta tahosta eli koulusta, suostumusta ei pidetty vapaaehtoisena. Koululla oli auktoriteettisuhde oppilaisiin, liittyen heidän koulumenestyksensä arviointiin sekä opintolainan puoltoon. Tämän vuoksi suostumusta ei voitu pitää täysin vapaaehtoisena. Myös koululla oli merkittävä rooli oppilaidensa tulevaisuuden kannalta. Lisäksi, vaikka koululla oli lakisääteinen velvollisuus valvoa oppilaiden osallistumista koulutukseen, erityisten henkilötietoryhmien hyödyntäminen tehtävän suorittamiseksi ei ollut sallittua. Biometristen tietojen käyttäminen johti suurempaan yksityisyyden loukkaamiseen (SDPA, 2019, s. 4-5).

Koulu käytti biometristen tietojen käsittelyn perusteena GDPR:n artikla 9 g kohdan mukaisesti yleistä etua koskevaa syytä. SDPA:n mukaan perusteen käyttö ei ollut sopiva siihen, että tunnille osallistumista valvotaan. Lisäksi lasten erityisten henkilötietojen kerääminen tätä tarvetta varten oli moitittavaa, koska valvontaa suoritettiin jo muutenkin. Kouluun asennetut valvontakamerat tallensivat jo henkilötietoja videodatana, mutta ohjelman avulla osasta koulun oppilaista kerättiin vielä erikseen erityisiä henkilötietoja. Tämä rikkoi niin henkilötietojen eheyttä kuin niiden minimoinnin periaatetta. Oppilaiden osallistumista tunnille olisi voitu suorittaa normaalin videovalvonnan turvin (SDPA, 2019, s. 6-9).

GDPR:n 35 artiklan mukaan henkilötietojen käsittelijän tulee arvioida henkilötietoihin kohdistuvat riskit. Riskienarvio oli tehty liittyen kameravalvonnassa kerättäviin henkilötietoihin sekä sieltä erikseen kerättävien erityisten henkilötietoluokkien suhteen. Riskienarvio ei kuitenkaan ollut tarpeeksi kattava, koska käsittely koski alaikäisten lasten henkilötietoja. Lisäksi kyseessä oli uusi tapa käsitellä henkilötietoja, jolloin asiasta olisi pitänyt konsultoida paikallista tietosuojavaltuutettua. Koska tätä ei ollut tehty SDPA katsoi, että koulu oli rikkonut tältäkin osalta määräyksiä. Kasvojentunnistukseen kykenevät kamerat olivat asennettu luokkahuoneisiin. SDPA:n mukaan tältä osin ei rikottu sääntelyä, koska luokkahuoneet katsottiin olevan ei julkisia tiloja, jolloin kameravalvonta ei tarvitse erillistä lupaa (SDPA, 2019, s. 10).

SDPA määräsi koulun maksamaan noin 20 000 euron suuruisen sakon, koska henkilötietoihin kohdistuva loukkaus oli vakava. Koulu käytti kasvojentunnistusohjelmistoa ilman, että oli etukäteisesti toimittanut kirjallista selvitystä asiasta tietosuojaviranomaiselle. Lisäksi perusteet erityisten henkilötietoryhmien käsittelemiseksi eivät täyttyneet ja suostumus edellä mainittujen henkilötietojen käsittelyyn oli vajavainen. Koulun toiminta rikkoi etenkin Euroopan tietosuoja-asetuksen artikloja 5 ja 9.1 (SDPA, 2019, s. 12).

2.3.3 Tapaus Lontoon metropolin poliisi

Metropolitan Police Service (MPS myöhemmin) on testannut automaattisen kasvojentunnistuksen teknologiaa aikavälillä elokuu 2016 – helmikuu 2019 kymmenessä tapahtumassa eri sijainneissa Lontoon alueella. Operatiivisen kokeen tarkoituksena oli arvioida teknologian arvoa, toteuttamiskelpoisuutta ja

sen luomia mahdollisia haasteita. Haasteita arvioitiin niin teknologisesta, laillisesta, eettisestä kuin hallinnollisesta näkökulmasta. Tapauksesta on laadittu raportti poliisin toimesta (Metropolitan Police Service, 2020, s. 3).

Testitapahtumista laadittiin myös tutkimus, joka on rahoitettu osana Economic Social Research Council:n (ESRC myöhemmin) Human Rights, Big Data & Technology -projektia. Tutkijat pääsivät poliisin mukaan seuraamaan testitapahtumia, haastattelemaan poliiseja ja arvioimaan laadittuja dokumentteja. Tutkimuksen tarkoituksena oli tuottaa itsenäinen akateeminen raportti poliisin automaattisen kasvojentunnistusteknologian käytön prosessista (ESRC, 2019, s. 5).

MPS on sitoutunut tutkimaan uusien teknologioiden vaikutusta rikostentorjuntaan yhä kasvavassa vaikeassa ympäristössä. Reaaliaikainen kasvojentunnistus on yksi keino poliisille yrittää ottaa kiinni muun muassa etsintäkuulutettuja, jotka ovat jo rekisteröity poliisin tietokantaan. Yleisen järjestyksen ja turvallisuuden takaamiseksi MPS pyrkii vähentämään etsintäkuulutettujen henkilöiden määrää nykyteknologialla. Käytössä olevilla metodeilla etsintäkuulutettujen henkilöiden paikantaminen voi olla aikaa vievää, henkilösidonnaista ja kallista (Metropolitan Police Service, 2020, s. 6). ESRC:n laatima tutkimusraportti ei suoraan ota kantaa automaattisen kasvojentunnistuksen teknologian käyttöön viranomaisten toimesta, vaikka se nostaakin esiin muutamia elementtejä, joista voi tulevaisuudessa muodostua keskustelua (ESRC, 2019, s. 5).

MPS:n raportin mukaan testien päämäärät olivat luoda todistusaineistopohjainen tietokanta kasvojentunnistusteknologialle osana poliisitaktiikkaa, varmistaa lainsäädännöllinen vaatimustenmukaisuus, rakentaa luottamusta kansalaisiin, varmistaa sosiaaliset ja eettiset näkökulmat, omaksua vahva, sopusuhtainen ja tekoälyyn pohjautuva henkilöiden lähestyminen sekä suorittaa arviointia ja näyttää objektiivisesti toteen kasvojentunnistusteknologian tehokkuus (Metropolitan Police Service, 2020, s. 6). ESRC:n tutkimusraportin mukaan testitapahtumien prosessikuvaukset olivat pääsääntöisesti vain teknisestä näkökulmasta, eivätkä ne ottaneet riittävästi kantaa ei-teknisiin päämääriin. Näillä tarkoitetaan sitä, ettei valvontaa suorittanut taho avannut tarpeeksi selvästi niitä yksittäisiä käyttötapauksia mihin kasvojentunnistusta hyödynnettäisiin. GDPR:n myötä selkeiden käyttötapausten avulla voidaan paremmin arvioida sitä, onko erityisten henkilötietojen hyödyntäminen tarpeellista ja suhteessa yksilön oikeuksiin (EPPB 3/2019, s. 15) Suoranaisen kansallisen lainsäädännön puuttuminen ja mandaatin antaminen reaaliaikaisen kasvojentunnistuksen käyttöön nähtiin myös ongelmallisena ihmisoikeuslain näkökulmasta. Biometristen tietojen hyödyntäminen pohjautui kansalliseen lakiin, joka oli vanha ja otettu käyttöön ennen Euroopan tietosuoja-asetusta. Teknologian hyödyntämisestä ei myöskään ole julkisesti saatavilla tarpeeksi tietoa, jotta riittävä läpinäkyvyys saavutettaisiin. Teknologian käyttämisen laillisuudesta voisi koitua ongelmia, mikäli asia vietäisiin oikeuden punnittavaksi. Tarpeellisuus teknologian käytöstä ja sen vaikutukset ihmisoikeuksiin sekä niiden määrittäminen riskienarvioinnin perusteella nähtiin puutteellisena. Näkemystä tuki myös kansallisen tietosuojavaltuutetun ohjeistus (ESRC, 2019, s. 6-9).

MPS:n raportin mukaan lainsäädäntö kuitenkin huomioitiin hyvissä ajoin ennen tapahtumien aloittamista. MPS huomioi erilaisia käyttötapauksia, datan käytöstä, säilyttämistä, käsittelystä ja poistamisesta sekä eettisistä kysymyksistä teknologian suhteen. Lisäksi MPS konsultoi kansallista kamera-, biometriikka- ja tietosuojavaltuutetun toimistoja prosessin lainsäädännön ja tietosuojan täyttämiseksi. Ennen ensimmäistä tapahtumaa MPS myös suoritti itsearvioinnin omasta toiminnastaan sekä kyselyn, jossa kansalaisryhmien mielipidettä kysyttiin teknologian käyttämisestä (Metropolitan Police Service, 2020, s. 7).

Tutkimuksessa huomioitiin myös mahdollisuus teknologian kattavampaan käyttöön, kuin mitä testitapahtumissa käytettiin. Teknologia voitaisiin laajentaa käyttöön esimerkiksi poliisien vartalokameroihin tai kaupunkikameroiden 24/7 toimintoihin, jonka seurauksena voisi muodostua tietokanta yksilön liikkeistä kaupungin alueella. Tietokantaa voitaisiin sen jälkeen hyödyntää muihin analyyseihin, kuten henkilöiden epätyypillisiin liikeratoihin, osallistumista tiettyihin tilaisuuksiin tai tapaamisiin tiettyjen henkilöiden kanssa. Teknologian vääristymät ja syrjintäepäilyt aiheuttivat myös huolia tutkimuksessa. Teknologialla voidaan saada erilaisia tuloksia riippuen tunnistettavan henkilön sukupuolesta, rodusta tai ihonväristä. Suoritettujen testien mukaan kasvojentunnistuksen tarkkuus laskee, kun käytetään staattisia kuvia vanhentuvista kasvoista. Samankaltaisten testien mukaan sukupuolen luokittelussa, ns. väärä positiivinen eli tarkastuksen jälkeen vääräksi todettu tunnistus, tulokset miehille laskevat. Algoritmit suoriutuivat paremmin vaaleilla yksilöillä ja heikoimmin tummaihoisilla naisilla. Suostumuksen varmistamista ja mahdollisuutta valita toisin testien osalta pidettiin myös ongelmallisena (ESRC, 2019, s. 20-24).

MPS piti suoritettuja testitapahtumia kuitenkin onnistuneena ja osoituksena automaattisen kasvojentunnistusteknologian tehokkuudesta. Tuloksena oli keskimääräinen 70 %:n arvo aitoja positiivisia tunnistuksia. Väärien tunnistusten suhde oli yksi henkilö tuhannesta. Poliisin resurssien vertailussa pidätysten määrän suhteen tulos oli 30 % positiivinen kasvojentunnistusteknologian avulla saatujen hälytysten myötä. Teknologian vaikuttavuusarvioinnissa otettiin huomioon myös rodulliset vääristymät, joita media on nostanut esille. Väärä positiivinen ja oikea positiivinen tuloksia vertailtiin etnisyyksien kesken, mutta tilastollisesti niillä ei ollut suuria eroja. Naisilla todettiin alhaisempi väärä positiivinen ja oikea positiivinen arvo kuin miehillä. Lopulta kyse on kuitenkin algoritmista, joka reagoi annettuun dataan ja luotuihin tunnisteisiin. Lopullisen päätöksen tunnistamisesta tekee kuitenkin poliisi, joka käyttää teknologiaa päätöksenteon tukena (Metropolitan Police Service, 2020, s. 28).

2.3.4 Tapaus Etelä-Walesin poliisi

Sekä ESRC:n tutkimuksessa, että MPS:n raportissa viitataan Etelä-Walesin poliisin tapaukseen, joka ESRC:n tutkimuksen aikana oli vielä avoinna mutta MPS:n raportin jälkeen tapaus oli jo käsitelty oikeusasteessa. Tapahtumat liittyvät poliisin kasvojentunnistusteknologian laillisuuden arviointiin. Asiasta saatiin Cardiffin korkeimman oikeuden päätös syyskuussa 2019. Päätös on ensimmäi-

nen kasvojentunnistusteknologian käyttöön kantaa ottanut oikeusaste koko maailmassa (BBC, 2019).

Tapahtumien taustalla on loukatun osapuolen kyseenalaistaminen poliisin kasvojentunnistusteknologian laillisuudesta yleisesti kolmessa erillisessä tapahtumassa. Poliisin osalta kaikki kolme tapahtumaa liittyivät kasvojentunnistusteknologian testitapahtumiin. Ensimmäinen tapahtuma oli Uefa Champions liigan finaalin aikaan Principality stadionilla Cardiffissa kesäkuussa vuonna 2017, jolloin poliisi kuvasi ja käytti kasvojentunnistusteknologiaa stadionin sisääntuloporteilla. Toisen tunnistustapahtuman paikkana oli Cardiffin keskusta joulukuussa vuonna 2017, jolloin loukattu oli jouluostoksilla. Teknologia oli käytössä julkisella paikalla poliisin pakettiautossa. Kolmas tunnistustapahtuma liittyi turvallisuusmessuihin, jotka pidettiin Motorpoint Arenalla vuonna maaliskuussa 2018. Loukattu osallistui protestiin areenan ulkopuolella. Kasvojentunnistusteknologiaa käytettiin valvonnassa, joka suunnattiin areenan sisäänkäynneille. Kahden viimeisimmän tapahtuman aikana loukattu ei nähnyt merkkejä tai varoituksia automaattisen kasvojentunnistusteknologian käytöstä, eikä hän huomannut, että poliisit olisivat antaneet sen käytöstä alueella mitään tietoa. Loukattu katsoi, että hänen perusoikeuksiaan loukattiin näissä tapahtumissa muun muassa ihmisoikeus-, tietosuoja- ja tasa-arvolakien perusteella. Hän kuitenkin nosti syytteet vain kahdesta viimeisimmästä loukkauksesta. Lisäksi hän katsoi, että poliisilla ei ole kasvojentunnistusteknologian käytölle laillisia perusteita (UK High Court of Justice, 2019).

Poliisi oli eri mieltä loukatun oikeuksien loukkaamisesta sekä teknologian käytön laillisista perusteista. Todisteita loukatun läsnäolosta ei ollut, vaikka pragmaattisista syistä poliisi hyväksyikin läsnäolon. Biometrisen tiedon tallentumisesta ei myöskään ollut mahdollista enää saada todisteita, koska tiedot on hävitetty joko välittömästi tai viimeistään 30 päivän sisällä tunnistuksesta. Lisäksi henkilö ei voi olettaa, ettei hän joutuisi poliisin kameravalvonnan kuvaamaksi, kun hän tulee julkiselle paikalle. Poliisi käyttää rikostentorjunnassa kameravalvontaa laajasti julkisilla paikoilla. Viimeisenä poliisi perusteli näkemyksiään sillä, että kasvojentunnistusteknologian käyttö on äkillinen prosessi, eikä henkilöiden biometrinen data koskaan päädy poliisin käsiteltäväksi. Poliisi piti kiinni myös näkemyksestään, että tilanteissa toimittiin voimassa olevan lainsäädännön mukaisesti, jonka lisäksi tietosuoja, tietoturva ja eettiset näkökulmat täyttyivät. Näin ollen katsottiin, että poliisi ei ole rikkonut henkilöiden oikeuksia tai lakia käyttäessään automaattista kasvojentunnistusteknologiaa tilanteissa katsoi, että poliisi oli toiminut ihmisoikeuslain mukaisesti ja sen toimenpiteet täyttivät riittävät lainsäädännölliset kontrollit. Ensisijainen lainsäädäntö mahdollistaa myös kasvojentunnistusteknologian käytön viranomaisilla. Edellytyksenä on, että henkilötietojen kaikki käsittely turvataan asianmukaisesti, niitä käytetään vain käyttötarveperusteisesti ja säilytetään sen aikaa kuin on tarpeellista. Lisäksi edellytetään, että data on tarkkaa ja ajantasaista sekä käyttöperusteiden pitää olla tarkkaan kuvattu, täsmällisiä ja lakiin perustuvia. Oikeuden mukaan poliisin toiminta täytti myös toissijaiset lainsäädännölliset vaatimukset, jotka koostuvat kahdestatoista ohjeesta kansallisesta valvontakame-

raoppaasta. Poliisin omat politiikat tukivat myös teknologian käytön läpinäkyvyyttä ja käyttöperusteita. Käyttöperusteiden kuvaukset olivat laadukkaat ja lakiin perustuvia, joilla pyrittiin estämään aikaisemmin tunnistettujen häiriköiden vaikutukset tilaisuuksissa. Käytössä olleet listat haettavista henkilöistä eivät koskeneet loukattua osapuolta, jolloin hänestä ei otettu lainkaan dataa. Lopuksi poliisi on itse arvioinut kasvojentunnistusteknologian käyttöä, eikä sitä voida pitää automaattisena toimenpiteenä poliisitoiminnassa sen useiden haasteiden vuoksi. Näillä perusteluilla oikeus katsoi, että loukatun syytteet hylätään kaikkien tapahtumien osalta. Poliisi on toiminut tilanteissa ihmisoikeus- ja tietosuoja- sekä tietoturvalainsäädännön mukaisesti (UK High Court of Justice, 2019).

Oikeus katsoi myös, että perusteet täyttyvät tietyille käyttötapauksille, joissa automaattista kasvojentunnistusteknologiaa voitaisiin käyttää. Etelä-Walesin poliisi on käyttänyt kasvojentunnistusteknologiaa noin 50 kertaa aikavälillä toukokuu 2017 – huhtikuu 2019 (UK High Court of Justice, 2019). Oikeuden mukaan automaattisen kasvojentunnistusteknologian hyväksytyt käyttöperusteet ovat:

- Etsintäkuulutettujen henkilöiden etsintä
- Pidätystä karttavien henkilöiden etsintä
- Rikoksesta epäiltyjen henkilöiden etsintä
- Suojelua tarvitsevien henkilöiden etsintä, esimerkiksi kadonneet
- Tapahtumaturvallisuus, vaarallisten henkilöiden etsintä
- Poliisia kiinnostavien henkilöiden etsintä, esimerkiksi tiedustelu
- Haavoittuvien henkilöiden etsintä

2.4 Yhteistoiminta poliisin kanssa

Kaupungit ja kunnat tuottavat erilaisia turvallisuuspalveluja myös täysin itsenäisesti. Tästä huolimatta poliisi on Suomen sisäisen turvallisuuden päävastuuviranomainen. Kameravalvonnan puolella kaupungit ovat toimittaneet julkisten paikkojen yleisvalvontajärjestelmiä myös poliisin saataville. Yhteistä käytäntöä näille ei kuitenkaan ole olemassa. Joissain kaupungeissa kameroiden rekisterinpito on kaupungin vastuulla, kuten Oulussa (Oulu, 2019). Osassa se on siirretty täysin poliisille kuten Helsingissä, jolloin kaupungilla ei ole ylläpitämiinsä kaupunkikameroihin edes käyttöoikeutta (Helsinki, 2019). Tampereella rekisterinpito on jaettu kaupungin ja poliisin yhteiseksi (Tampere, 2018). Tärkeää on kuitenkin huomioida, että kaupungeilla on paljon muitakin kameravalvontajärjestelmiä, mutta edellä mainituissa esimerkeissä kyse on nimenomaisesti poliisin suorakäyttöoikeudellisista valvontakameroista.

Useasti yleisvalvontakameroiden rekisteriselosteiden mukaan käyttötarkoitus kaupungin puolella on omaisuuden suojaaminen, rikosten ennalta ehkäisy ja selvittäminen, henkilökunnan ja asiakkaiden turvallisuuden varmista-

minen. Poliisin toimivalta rekisteriselosteissa perustuu poliisilain (872/2011) 4 luvun 1§:n 2 momenttiin, jonka mukaan ennalta ilmoitetuissa paikoissa poliisi saa suorittaa teknistä valvontaa muun muassa rikosten ennalta estämiseksi ja selvittämiseksi. Uuden tietosuojalainsäädännön myötä kesällä 2019 toimivalta-perusteet sidottiin lakiin henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) ja lakiin henkilötietojen käsittelystä poliisitoimessa (616/2019). Uudistuneen lainsäädännön myötä kaupunkien ja poliisin yhteiskameravalvonnan rekisteripitoa ollaan siirtämässä keskitetysti Poliisihallituksen ja kaupunkien välille. Sopimustilanne on kuitenkin vielä kesken, koska tietosuojavaltuutettu piti Oulun kaupungin ja poliisin kamerasopimusta ongelmallisena. Tietosuojavaltuutetun kannanoton vuoksi Poliisihallituksessa ollaan valmistelemassa vaikutustenarviointia, johon liittyy kaupunkien teknisen valvonnan hyödyntäminen poliisin toimesta. Tietosuojavaltuutettu ei kuitenkaan ota kantaa poliisin toimivaltaan asiassa, jonka vuoksi asia on vireillä vielä toistaiseksi eduskunnan oikeusasiamiehellä.

2.4.1 Tapaus Oulun kaupunki

Vuonna 2018 oli julkisuudessa esillä, että Oulun kaupungin rekisterinpidossa olevista kaupungin valvontakameroista oli rakennettu suorakäyttöyhteys Oulun poliisilaitoksen johtokeskukseen. Oulun kaupungin kameravalvontaa ei ollut poliisin käytön osalta rajattu julkisia paikkoja kuvaaviin kameroihin, vaan järjestelmän kautta poliisi pääsi tarkastelemaan esimerkiksi koulujen sisätiloja ja terveysasemien odotusauloja. Muiden kuin yleisvalvontakameroiden osalta poliisille oli luotu kuitenkin oma erillinen supertunnus, jota käytettäisiin ainoastaan silloin kun kyseessä on yksittäinen lakiin perustuva virkatehtävä. Tällöin käytöstä ilmoitettaisiin erikseen rekisterin pitäjälle, sekä tapahtumasta jäisi erillinen lokimerkintä (TSS 6610/182/18, 2019, s. 1-3).

Tietosuojavaltuutettu piti Oulun kaupungin ja Oulun poliisilaitoksen sopimusta ongelmallisena, koska sopimuksen avulla poliisilaitos oli ulkoistanut sille säädettyä toimivaltaa teknisen tarkkailun osalta. Järjestelmä oli täysin Oulun kaupungin rekisteripidossa ja poliisi pääsi katsomaan suoraan tietoja ilman tiedon luovuttamisen menettelyä. Tietosuojavaltuutetun mukaan kyseessä olisi uuden tietosuojalainsäädännön mukaisesti ennemmin yhteisrekisterin vaativa tietovaranto. Etenkin kun osapuolet ovat yhdessä sopineet ja määrittäneet henkilötietojen käsittelyyn ja keräykseen liittyvät toimet (TSS 6610/182/18, 2019, s. 5).

Rikosasioiden tietosuojalain (1054/2018) 20§:n 1 momentin mukaan henkilötietoja keräävän tahon eli rekisterinpitäjän tulee ennen käyttöä arvioida miten henkilötietojen käyttö järjestelmän avulla vaikuttaa yksilön tietojen suojaan. Jos suunniteltu tietojen käsittely voi aiheuttaa selvän riskin tulee sitä arvioida kirjallisesti suorittamalla vaikutustenarviointi. Oulun tapauksessa poliisi käytti kaupungin kamerajärjestelmää suoraan omaan tarkoitukseen, jolloin käyttötapaus ja siitä muodostettu sopimus oli uudenlainen. Tietosuojavaltuutetun mu-

kaan toiminta olisi velvoittanut rekisterinpitäjän suorittamaan vaikutustenarvioinnin (TSS 6610/182/18, 2019, s. 4).

Poliisi hyödyntää teknisen yhteyden kautta suoraan 42 kaupungin ja kunnan kamerajärjestelmää (Yle, 2020a). Tietosuojavaltuutetun kannanoton mukaan jo perinteisen kameravalvonnan osalta rekisterinpidollista problematiikkaa on syntynyt. Tekoälyn hyödyntäminen kamerajärjestelmissä luo jälleen uuden tavan käsitellä ja hyödyntää henkilötietoja kameroiden keräämän ja käsittelemän datan kautta. Tärkeää on myös huomioida, että jo pelkkä algoritmeilla tehty laskenta on käsittelyä, joka kohdistuu tunnistettavaan kuvaan eli henkilötietoon. Näin ollen, vaikka tekoälyn tuottama materiaali ei olisi yksittäisenä henkilötietoa, se muodostuisi henkilötiedon käsittelyn kautta ja näin vaatisi rikosasiantietosuojalain mukaisesti vaikutustenarvioinnin. Lain henkilötietojen käsittelystä rikosasioissa (1054/2018) mukaan vaikutustenarvioinnin tulee sisältää yleinen kuvaus siitä, miten järjestelmää käytetään ja henkilötietoja käsitellään, riskiarvion siitä millaisia riskejä käsittelystä voi muodostua ja mitä toimia riskien toteutumisen vähentämiseksi on toteutettu ja voitu varmistaa henkilötietojen suojaaminen. Lain 21§:n mukaan asiasta on haettava tietosuojavaltuutetun kannanotto, jos käsittely aiheuttaa merkittävän riskin rekisteröidyn oikeuksilla tai tietoja käsitellään uusilla tekniikoilla tai menettelytavoin. Tietosuojavaltuutetun pitää toimittaa vastaus lähtökohtaisesti kuuden viikon sisällä.

2.4.2 Laki henkilötietojen käsittelystä poliisitoimessa

Poliisin henkilötietolaki (616/2019) uudistui GDPR:n myötä 1.6.2019. Isoimpana muutoksena lehdistön mukaan pidetiin sitä, että poliisi olisi saanut oikeuden automaattiseen kasvojentunnistukseen. Kasvojentunnistusta voitaisi käyttää rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi kuin myös etsintäkuulutettujen tavoittamiseksi (Yle, 2019a). Helsingin sanomissa (2020) poliisitarkastaja Pekka Sallinen kuitenkin kaventaa median tuomaa tulkintaa käyttöoikeuksia siihen, että tällä hetkellä poliisi käyttää automaattista kasvojentunnistusta vain passin- ja henkilökorttien hakuprosessissa henkilöllisyyden varmistamiseen. Samassa artikkelissa apulaistietosuojavaltuutettu Jari Råman jatkaa, että kasvojentunnistuksen käyttö poliisilla on hyvin rajallista ja uusien käyttötapausten laajentaminen vaatisi uutta lainsäädäntöä. Biometristen tietojen käyttö ei kuitenkaan ole uusi asia poliisille, vaan esimerkiksi sormenjälkiä on tallennettu ja vertailua tehty jo hyvin kauan.

Uuden lainsäädännön myötä kasvokuvia voidaan verrata sormenjälkien tapaan tehtäväkohtaisesti silloin, kun se on välttämätöntä rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi. Huomiona on kuitenkin, että kerätyt biometriset tiedot, kuten sormenjälki, DNA tai biometrisesti haettavaan muotoon muunnettu kasvokuva, saadaan tallentaa poliisin rekisteriin vain silloin, kun ne on pakkokeinolain tai ulkomaalaislain nojalla kerätty rikostorjuntaa varten. Tämä siis mahdollistaa sen, että rikospaikalta taltioitu valvontakameran videolla olevaa rikoksentekijän kuva voidaan muokata biometriseen muotoon ja vertailla poliisin rekistereihin. Ulkomaalaislain nojalla kerättyihin

kasvokuviin kohdistuu vielä tiukemmat kriteerit kuin rikosperusteella kerättyihin kasvokuviin. Lähtökohtaisesti ulkomaalaislain perusteella kerättyyn tietokantaan saa kohdistaa hakuja vain vakavien, kuten terroristisen rikosten perusteella. Vertaamista varten luodut biometriset tiedot tulee hävittää välittömästi toimenpiteen jälkeen (HaVM 39/2018).

Sisäministeriön poliisiosaston ylijohtajan Risto Lammin mukaan kameravalvontaan tai muuhun tekniseen valvontaan liittyen uudistettu poliisin henkilötietolaki ei tuonut muutoksia (Intermin, 2019). Poliisilain (872/2011) 4 luvun 1§:n mukaan poliisilla on oikeus suorittaa teknistä valvontaa ajoneuvoihin ja kuljettajiin, jalankulkijoihin tai yleisöön kohdistuvaa teknisellä laitteella tapahtuvaa katselua sekä kuvan automaattista tallentamista. Teknisen valvonnan alue tulee olla ennalta ilmoitettu. Poliisilain 4 luvun 2§:n mukaan poliisi voi päällystön kuuluvan poliisimiehen pyynnöstä saada viranomaiselta maksutta tehtävänsä suorittamiseksi tarpeelliset tiedot. Poliisin henkilötietolain (616/2019) 35§:n mukaan rikosten ennalta estämiseksi ja paljastamiseksi teknisellä valvonnalla kerätyt tiedot tulee poistaa viimeistään kuuden kuukauden kuluttua.

2.5 Pelastustoimi

Pelastuslaitokset ovat omassa toiminnassaan myös alkaneet hyödyntämään yhä enemmän tekoälyä erityisesti IoT-laitteiden kanssa. Kameravalvonnan laajempi hyödyntäminen pelastustoiminnassa voisi vielä avata uusia mahdollisuuksia tulevaisuudessa, kunhan tietosuojasta ja tietoturvasta huolehditaan riittävästi. Pelastuslaitokset toimivat poliisin tavoin viranomaisroolissa, mutta henkilötietojen käsittely perustuu eri säätelyyn kuin poliisilla. Pelastuslaitokset noudattavat EU:n yleistä tietosuoja-asetusta ja omaa erityislainsäädäntöään pelastuslakia (379/2011), joka määrittelee pelastusviranomaisen käyttö- ja toimivaltaperusteet sekä tarkemmin myös henkilötietojen käsittelyä.

Pelastustoimen lainsäädäntö on kehittynyt viimeisien vuosikymmenien muutamaan kertaan. Vuonna 1958 annettu väestönsuojelulaki (438/1958) korvattiin vuonna 1975 lailla palo- ja pelastustoimesta (559/1975). Laki palo- ja pelastustoimesta taas korvattiin vuonna 1999 voimaan tulleella pelastustoimilailla (561/1999). Vuonna 2003 säädettiin uusi pelastuslaki (468/2003), koska pelastustoimen alueellistaminen edellytti muutoksia. Viimeisin ja toistaiseksi voimassa oleva pelastuslaki säädettiin vuonna 2011 (Pelastustoimi 2014, 69-74). Nykyistä pelastuslakia on esitetty uudistettavaksi HE 18/2018 mukaisesti. Lainsäädännön tarkoituksena on ollut edistää kuntien yhteistoimintaa muun muassa poistamalla mahdollisimman pitkälti kuntien yhteistyön esteet pelastustoimen tehtävien hoitamisessa (HE 257/2010).

Pelastuslain (379/2011) 42§ mukaisesti kunnat vastaavat pelastustoimen tehtävistä yhteistyössä alueen pelastustoimen kanssa. Pelastuslaitokset tuottavat heille oman alansa turvallisuuspalveluita sopimusperusteisesti. Tarkemmin tehtävistä säädetään pelastuslain 1. luvun 2§:ssä, jonka mukaan pelastuslaitok-

sen velvollisuus on ehkäistä tulipaloja ja muita onnettomuuksia sekä rajoittaa niiden seurauksia. He ovat myös velvollisia varautumaan ja toimimaan niiden uhatessa tai sattuessa. Pelastuslaki edellyttää pelastuslaitoksia osallistumaan myös pelastustoiminnan tehtäviin ja väestönsuojelukoulutukseen sekä rakentamaan ja ylläpitämään väestönsuojia. Pelastuslain 89§:ssä linjataan, että myös 42§:ssä tarkoitettuja tietoja voidaan saada rajapinnan kautta tai muuten sähköisesti. Lisäksi 89§ mukaan pelastusviranomaisella on sille säädettyjen tehtävien suorittamiseksi salassapitosäännösten estämättä tiedonsaantioikeus pelastustoimintaa ja valvontatehtäviä varten. Erityisten riskikohteiden kuten päihdeongelmaisten tukiasuntojen osalta tiedot tulee olla sillä tavoin yksilöityjä, ettei tietojen perusteella voida tunnistaa yksittäistä luonnollista henkilöä (Pelastustoimi, 2020). Pelastuslain 88§ nojalla pelastusviranomaisella ja onnettomuuden tutkintaan määrätyllä tutkintalautakunnan jäsenellä tai asiantuntijalla on tiedonsaantioikeus välttämättömien tietojen saamiseksi onnettomuuskohteesta. HE 257/2010 mukaan tiedoilla tarkoitetaan kaikkia viranomaisten hallussa olevia tutkinnan kannalta välttämättömiä tietoja.

Hallituksen esityksen (HE 18/2018) mukaan pelastustoimen olemassa olevien yhteistoimintarakenteiden ja -prosessien hyödyntäminen jää vajavaiseksi. Tämä voi muodostua toiminnan kannalta kriittiseksi esimerkiksi pitkäkestoisessa torjuntaoperaatiossa kuten öljy- ja kemikaalivahingot. Alueellista ja paikallista yhteistoimintaa tukisivat myös yhtenäiset laadukkaat, kattavat ja ajantasaiset toimintaohjeet. Tietynkaltaisissa vahingontorjunta tilanteissa kaupunkien kameravalvontajärjestelmän hyödyntäminen olisi myös perusteltua pelastuslaitoksille.

Kameravalvontajärjestelmän hyödyntämistä pelastuslaitoksen tarpeisiin erilaisten hälytysten, analysoinnin tai suunnittelun muodossa tulisi perusteellisesti pohtia järjestelmän suunnitteluvaiheessa. Tekoälyteknologian hyödyntämisen avulla on mahdollista tarjota pelastusviranomaiselle mahdollisuuksia parantaa toimintavalmiuttaan ja ennaltaehkäiseviä toimenpiteitään omalla toimialueellaan. Erityisesti kameravalvontamateriaalin jakaminen tai reaaliaikainen etäkäyttöyhteys tulisi määritellä käyttöperusteen mukaisesti ja tarkastella sen tarpeellisuutta toimijan tehtävien mukaisesti.

2.6 Yksityiset turvallisuuspalvelut

Kameravalvonnan osalta yksityiset turvallisuuspalvelut vastaavat pitkälti kameroiden päivittäisestä käytöstä ja tiedon luovuttamisesta viranomaiselle. Kaupungit myös tilaavat palveluita yksityisiltä tahoilta esimerkiksi kaupungissa järjestettävien isojen yleisötilaisuuksien ja kokousten turvaamiseksi. Valvontakameroiden käyttö on merkittävässä roolissa tapahtumaturvallisuuden osalta, jolloin etenkin tapahtuman tilannekeskuksesta tulisi olla järjestelmään käyttöoikeudet myös mm. järjestyksenvalvonnan puolelta. Laki yksityisistä turvallisuuspalveluista (1085/2015) määrittää vartioimisliiketoiminnaksi ansiotarkoituksen tai toimeksiantoon liittyvän perusvaatimuksen, jolloin tapahtumaan tai

kunnan palkkalistalle hankittu vartija suorittaa vartioimistehtävää. Lisäksi ko. lain 6§:n mukaan vartijoita sitoo se, ettei kenenkään oikeuksiin saa puutua kuin se on tehtävien suorittamiseksi välttämätöntä.

Hallituksen esityksen (HE 22/2014) mukaan yksityisten turvallisuuspalveluiden ja viranomaisten yhteistyön edistäminen palvelisi yleistä järjestystä ja turvallisuutta. Tietyillä alueilla, kuten julkisissa tapahtumissa toimivien järjestyksenvalvojien apu edistäisi molempien toimijoiden yhteistyötä ja lisäisi turvallisuutta. Vartioimisalue tulisi kuitenkin olla rajattu toimeksiantosopimuksessa vastaamaan tapahtuma-aluetta ja siitä kumpuavaa laillisuusperustetta. Laajemman kameravalvontajärjestelmän osalta, johon olisi liitetty myös muita kuin tapahtuma-alueeseen liittymättömiä kameroita, kamerakohtaisia näkyvyyksiä tulisi vartijalle rajata tapahtuma-alueen mukaisesti. Vartiointialueena voisi kuitenkin toimia niin yleinen kuin yksityinen paikka. Hallituksen esityksessä (HE 22/2014) kuitenkin erikseen todetaan, että henkilön koskemattomuuden suojaaminen tai rikosten paljastaminen voitaisiin tehdä erikseen määritetyn vartiointialueen ulkopuolella, jos siihen liittyy tehtävä. Tällainen tehtävä voisi esimerkiksi olla dronella suoritettava aluevalvonta, jonka yhteydessä rikoksen tekijä poistuu valvottavalta alueelta, mutta henkilön tarkkailua voitaisiin jatkaa yli määritetyn tapahtuma-alueen rajojen.

Kameravalvontamateriaalin jakaminen tai reaaliaikainen etäkäyttöyhteys tulisi pystyä toteuttamaan tilannekeskuksesta myös paikalla oleville vartijoille, järjestyksenvalvojille tai poliisille, mikäli se olisi tehtäväkohtaisesti tarpeellista. Tätä puoltaa tehtävän asianmukainen hoitaminen, jolloin rikoksen paljastamiseksi liittyvän henkilön lyhytaikainen tarkkailu olisi sallittua (HE 22/2014). Lisäksi sitä tukisi myös työnantajan työturvallisuusvelvoitteet, koska yleisesti edellä mainitut henkilöt joutuvat puuttumaan tapahtumien yhteydessä väkivaltatilanteisiin, jolloin riski myös työturvallisuuden järjestämisestä kasvaa (HE 59/2002).

Vartioimistehtävään kuuluu oleellisesti myös rikosten paljastaminen (1085/2015), jolloin pääsy takautuvaan valvontakameramateriaaliin olisi tehtävän kannalta välttämätöntä. Erilaisten tekoälysovellusten hyödyntäminen tehostaisi vartijan tehtävien suorittamista, kunhan vartijalla olisi oikeus tehtävien osalta käsitellä valvontakamerajärjestelmän dataa ja siellä olevia henkilötietoja. Tietosuojaselosteessa tulisi tuoda esille myös vartioinnin osalta tarpeelliset käyttötapaukset ja arvioida henkilötietojen osalta syntyvät riskit ja varotoimenpiteet. Lain (1085/2015) 34§:n mukaan turvallisuusalan elinkeinolupa edellyttää myös vartijaa ja järjestyksen valvojaa noudattamaan salassapitovelvollisuutta.

3 Kyberturvallisuus

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on julkaissut Tietoturvan vuosi 2019 vuosikatsauksensa, jossa käydään läpi viime vuoden tapahtumia kyberturvallisuuden näkökulmasta. Katsauksessa muistetaan viime vuosi erityisesti uusien haavoittuvuuksien nopeasta hyödyntämisestä, laajavaikutteisista kiristyshaittaohjelmista ja uudesta normaalista eli käänteestä, jolloin näistä tuli osa arkeamme (Kyberturvallisuuskeskus, 2020).

Suurimmat Suomea koskevat uhat ovat vastavalitun Suomen kyberturvallisuusjohtaja Rauli Paanasen mukaan huijauskampanjat, palvelunestohyökkäykset ja yritysvakoilu. Yhtenä erityisenä riskinä Paananen nostaa esineiden internetin, jolta on syytä suojautua entistä paremmin. Verkossa kiinni olevien jääkaappien ja ilmalämpöpumppujen tietoturvallisuudesta täytyy huolehtia kuten puhelimen tai tietokoneen tietoturvasta. Paanasen mukaan tietoturvallisuus tulisi olla tuotteissa sisäänrakennettuna ja ohjelmiston päivitykset automatisoitu tuotteen koko elinkaaren ajaksi (Yle, 2020b).

Ruotsalaisen Axis Communications AB:n, joka on erikoistunut valmistamaan videovalvontakameroita ja -järjestelmiä, mukaan kyberturvallisuus on noussut yhdeksi kasvavaksi huoleksi kuluttajien ja yritysten toimitusketjussa. Kamerat ovat ottaneet askeleita omassa kehityksessään digitaalisessa maailmassa. Samalla ovet uudelle rikollisuudelle ovat avautuneet, kun kameroiden datan avulla hyödynnettäviä tietoja on varastettu ja myyty murtautumalla valvontakameroihin kytkettyihin verkkoihin. Yksikään järjestelmä, uusi tai vanha, ei ole 100 % turvallinen. Verkon ja tiedon suojaaminen ei vaadi sotilastason ympäristöä tai kryptaamista. Axis:n mukaan ensimmäisinä askeleina tulisi ymmärtää esineiden internetin periaate, tunnistaa oman järjestelmän haavoittuvuudet ja toteuttaa parhaiden käytäntöjen periaatteet tietojen suojaamiseksi (Axis, 2019).

Suomessa kansallinen tiedusteluviranomainen Suojelupoliisi ja Ruotsissa vastaava Säkerhetspolisen ovat molemmat nostaneet vuosittaisissa kansallisen turvallisuustilanteen kertomuksissaan esille yhteiskuntaa vaarantavia uhkia. Viranomaiset kokevat, että turvallisuuspoliittinen tilanne on muuttunut globalisaation ja digitalisaation myötä. Voimakkaiden talous- ja rahapoliittisten ris-

tikkäissidonnaisuuksien lisäksi molemmat nostavat kyberturvallisuuden yhtenä riskinä vakaville seurauksille yhteiskunnan toimivuuden kannalta. Digitalisaatio on mahdollistanut paljon mutta sen myötä myös verkon yli tapahtuvien laittomien toimintojen uhka on kasvanut. Toimijoiden ei välttämättä tarvitse edes astua valtion maaperälle toteuttaakseen mahdollisia haitanteko-, sabotaasi- tai tiedustelutehtäviä. Suojelupoliisi nostaa uutena ilmiönä ulkoistettuihin alihankinta- tai palveluntuottajaketjuihin kohdistuvat hyökkäykset, joiden kautta voi olla pääsy varsinaisen kohteen järjestelmiin ja tietoihin (Suojelupoliisi, 2020, s. 19; Säkerhetspolisen, 2020, s. 18).

3.1 Suunnitteluvaihe

Lähes kaikki kameravalvontajärjestelmät keräävät tai tallentavat tietoja. Tallennettu kuva tai ääni rinnastetaan henkilötietolaissa tarkoitettuun henkilötietoon, jos siitä on henkilö tunnistettavissa. Tallenteiden säilytysajalla ei ole vaikutusta henkilötietolain sovellettavuuteen. Ratkaisevaa on se, että tallentuuko tietoa vai ei (Finanssiala, 2010a). Tietosuojavaltuutetun toimisto on myös yksiselitteisesti todennut, että tallennettu kuva ja ääni ovat henkilötietoja (Tietosuojavaltuutettu, 2019).

Suunniteltaessa kameravalvontajärjestelmää ja sen tietojen säilyttämistä on hyvä ottaa huomioon järjestelmän ja tietojen käytettävyys, turvallisuus ja eheys. Tallennettuja tietoja tulee säilyttää niiden käyttötarkoituksen mukaisesti. Hallintaverkon suojaus, järjestelmän toimivuus, tunnistettavuus, kuvanlaatu, yhteysvirheiden aikainen tallennus, turvallinen ympäristö, fyysinen sijainti ja etähallinta ovat avainsanoja, kun pohditaan, säilytetäänkö tietoja esimerkiksi keskitetyssä pilvipalvelussa vai omassa infrastruktuurissa.

Erinomaisena taustana voidaan käyttää Finanssialan laatimaa kameravalvonnan K-menetelmä suunnitteluohjetta, vaikkakin se on laadittu jo vuonna 2010. Tietyt lainalaisuudet ja toteutukset pätevät kuitenkin edelleen nykyäänkin. Ohje pitää sisällään mm. suunnitteluun, järjestelmään, hankintaan ja ylläpitoon sekä tietyntyyppisiin tiloihin olevia ohjeita. Ohjeen tarkoitus on lisätä turvallisuutta ja ehkäistä vahinkoja (Finanssiala, 2010b).

Lisäksi hyvinä taustoina järjestelmän suunnittelun tukena toimivat eurooppalaiset standardit EN 62676-1-1 ja EN 62676-1-2, jotka ovat myös vahvistettu suomalaisiksi kansallisiksi standardeiksi. Standardit ovat vahvistettu vuonna 2014. Mainitut standardit ottavat kantaa kameravalvontajärjestelmän yleisiin vaatimuksiin, videonsiirtoa koskeviin suorituskykyvaatimuksiin ja turvasovelluksissa käytettävien kameravalvontajärjestelmien järjestelmävaatimuksiin. Standardit pyrkivät tukemaan monenlaisia käyttötapauksia, kuten suojaus, turvallisuus, liikenne ja niin edelleen, jonka vuoksi standardit monesti kattavatkin vain vähimmäisvaatimukset. Standardit eivät myöskään ota kantaa minkälaista teknologiaa kameravalvontaan käytetään. Lisävaatimuksia voidaan määritellä standardien liitteissä.

Yleiset vaatimukset standardissa EN 62676-1-1 ottavat kantaa järjestelmäturvallisuuteen, joka pitää sisällään järjestelmän ja datan eheyden. Järjestelmän eheydellä tarkoitetaan järjestelmän komponenttien fyysistä turvallisuutta sekä fyysisen että loogisen pääsynhallinnan erittelyä. Datan eheydellä tarkoitetaan loogista pääsyä dataan ja datan suojaamista häviämiseltä tai manipuloinnilta. Standardissa todetaan myös, että kameravalvontajärjestelmät sijaitsevat nykyään turvallisuusverkoissa, jotka käyttävät IT-infrastruktuuria, -laitteita ja -yhteyksiä suojatun alueen sisällä. Standardi myös luokittelee kameravalvontajärjestelmät tarvittavan turvallisuustason takaamiseksi. Luokittelu perustuu riskitasoon, jonka avulla arvioidaan (alhainen / suuri ja vähäinen / vakava) järjestelmän käyttötarpeen tapausten todennäköisyydet ja niiden aiheuttamien vahinkojen määrä. Luokkia on neljä, vähäinen riski (luokka 1), vähäisestä kohtalaiseen riskiin (luokka 2), kohtalaisesta suureen riskiin (luokka 3) ja suuri riski (luokka 4).

Standardi EN 62676-1-2 ottaa kantaa yleisiin videonsiirtoa koskeviin suorituskykyvaatimuksiin. Standardi määrittelee turvallisuusarkkitehtuurin videonsiirtolaitteelle, jolla pyritään mahdollistamaan vertaisolioiden, datan alkuperän ja verkkolaitteen todentaminen ja datan luottamuksellisuus ja eheys. Standardi määrittelee myös datan siirtämisen osalta, että kaikki suojattujen tilojen ulkopuolella tapahtuva viestintä tulee olla salattua turvallisuusluokittelusta riippumatta. Salaukseen on käytettävä TLS-protokollia RFC-standardien mukaisesti. Mikäli viestintä tapahtuu suojattujen tilojen ulkopuolella, tulee salauksen tarjota symmetristä 128-bittistä AES salausta ja käytettävä 1024-bittistä RSA avainta. Standardi pitää sisällään myös turvasovelluksissa käytettäviä laitteita koskevat vaatimukset. Standardi määrittelee tiedonsiirron toiminnallisuuksia ja teknisiä vaatimuksia niiden hallintaan mutta ei kuvaile vaatimuksia sen syvällisemmin.

Standardien ja sertifikaattien lisäksi tietoturvallisuuden ja tiedonhallinnan varmistamiseksi on säädetty tuore (906/2019) laki julkisen hallinnon tiedonhallinnasta, joka velvoittaa mm. valtion virastot ja laitokset, tuomioistuimet, eduskunnan virastot, valtion liikelaitokset, kunnat, kuntayhtymät, itsenäiset julkisoikeudelliset laitokset ja ylipistolaissa tarkoitetut yliopistot ja ammattikorkeakoulut huolehtimaan tiedonhallinnasta. Käytännössä tämä laki velvoittaa huolehtimaan, että kohteella on:

- Määritelty tiedonhallinnan toteuttamisen vastuut
- Laadittu ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta
- Tarjolla koulutusta varmistamaan henkilöstön ja tiedonhallintayksikön riittävän tuntemuksen voimassa olevista tiedonhallintaa, tietojenkäsittelyä, sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista

- Hankittu asianmukaiset työvälineet tiedonhallintaa koskevien velvollisuuksien toteuttamiseksi
- Järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta

Valtiovarainministeriö on lisäksi julkaissut julkisen hallinnon pilvipalvelulinjaukset, joilla on tarkoitus tukea valtion, maakuntien ja kuntien päätöksentekoa niiden suunnitellessa ja hankkiessa uusia ICT-palveluita. Julkaisussa otetaan kantaa erilaisiin palvelu- ja toteutusmalleihin, joiden avulla kuvaillaan mahdollisia etuja tai haasteita. Eduiksi julkaisun mukaan voidaan lukea muun muassa kustannustehokkuus, skaalautumiskyky, tietoturva, energiatehokkuus, joustavuus ja innovatiivisuus. Haasteina nähdään hankintaa ja käyttöä suunniteltaessa esimerkiksi ei-julkisten tietojen käsittely, toiminnan jatkuvuuteen liittyvät riskit, tietoturvan toteutuminen tiedon sijainnista ja hallinnasta riippuen, tietosuoja toteutuminen tiedon sijainnista ja hallinnasta riippuen, riskienhallinnan moniulotteisuus ja yksipuoliset sopimusehdot (Valtioneuvosto, 2019). Linjaukset koostuvat seuraavista seitsemästä kohdasta:

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta
2. Pilvipalveluissa on kiinnitettävä erityistä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen
3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset
4. Mikäli pilvipalvelu tai pilvipalveluteknologia tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita
5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti sekä oleellisten sopimusehtojen muuttuessa
6. Julkisen tiedon käsittelyä ei rajoiteta
7. Ei-julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva ja tietosuoja on asianmukaisesti toteutettu ja todennettu

3.2 Tiedon käsittely

GDPR:n (2016/679) mukaan tietojen käsittelyllä tarkoitetaan kaikkea keräämistä, siirtämistä, tallentamista, organisointia, jäsentelyä, säilyttämistä, muutoin saataville asettamista aina tiedon hävittämiseen asti. Käsittely voi olla automatisoitua tai manuaalista. Tietosuojavaltuutetun mukaan kaikki henkilötietoihin kohdistuvat toimenpiteet käsittelyn suunnittelusta poistamiseen ovat henkilötietojen käsittelyä. Henkilötiedoilla käsitetään kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön (Tietosuojavaltuutettu, 2019).

Kameravalvontajärjestelmässä käsiteltävät tiedot vaihtelevat järjestelmän tietosuojaselosteen käyttöperusteen mukaisesti julkisesta tiedosta henkilötietoi-

hin. Henkilötietojen lisäksi käsitellyt tiedot voidaan luokitella salassa pidettäviksi erityisiksi henkilötiedoiksi, muuksi salassa pidettäväksi tiedoksi tai jopa turvaluokitelluksi tiedoksi riippuen järjestelmän käyttötarpeesta. Käyttötarpeiden tunnistaminen järjestelmässä ja sen sovelluksissa on äärimmäisen tärkeätä heti järjestelmän suunnittelun alkuvaiheessa.

Salassa pidettävän tiedon käsittelyn ja säilyttämisen osalta edellytetään lainsäädännön mukaan turvallisuustoimenpiteitä. Tiedonhallintayksikön edellytetään seuraavan toimintaympäristönsä tietoturvallisuutta ja varmistettava tietojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Toimenpiteet on mitoitettava riskienarvioinnin mukaisesti. Kameravalvontajärjestelmän tiedon käsittelyn ja säilyttämisen vähimmäisvaatimusten osalta niitä käsitellään alaluvussa 3.5.

3.3 Tiedon säilyttäminen

Asetukset ja lait viime kädessä määrittelevät niin tiedon käsittelyn kuin säilyttämisenkin osalta julkisen ja yksityisen sektorin toimijoiden kriteerit tietoturvallisuuden suhteen. Asetusten ja lakien pohjalta on luotu kriteeristöjä, jotka on tarkoitettu parantamaan tietoturvallisuutta erilaisissa käyttötapauksissa. Kriteeristöihin on lisäksi kerätty parhaita oppeja aikaisemmista käytännöistä. Kriteeristöt itsessään eivät aseta ehdottomia vaateita. Kriteeristöjen vaatimukset kuitenkin pohjautuvat voimassa olevaan lainsäädäntöön. Alla on kuvattu kaksi erinomaista kriteeristöä, joiden vaatimukset täyttämällä tietoturvallisuuden tasoa nostetaan ja tiedon käsittely ja säilyttäminen kohdeorganisaatiossa pyritään varmistamaan. Kriteeristöt kattavat turvallisuuden hallintaa hallinnollisen, fyysisen ja teknisen tietoturvallisuuden saralla. Kriteeristöt soveltuvat erinomaisesti esimerkiksi tietojärjestelmien turvallisuuden arviointiin.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on julkaissut pilviturvallisuuden arviointikriteeristön (PiTuKri), jonka tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. Kriteeristö ottaa kantaa sekä viranomaisen turvallisuusluokiteltuihin IV-luokan salassa pidettäviin tietoihin, että muihin kuin turvallisuusluokiteltuihin salassa pidettäviin tietoihin ja henkilötietojen säilyttämiseen. PiTuKri:a voidaan esimerkiksi käyttää työkaluna tapauksissa, joissa viranomaisen määräämisvallassa olevan tai hankittavaksi suunniteltavan pilvipalvelupohjaisen tietojärjestelmän tietoturvallisuutta arvioidaan (Kyberturvallisuuskeskus, 2019).

Katakri on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Katakri keskittyy enemmän turvaluokitellun tiedon käsittelyn ja säilyttämisen vaatimuksiin. Sitä voidaan käyttää myös apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä. Katakriin kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin tietoturvallisuusvelvoitteisiin kuten PiTuKri:kin. Katakrin vaatimukset on jaet-

tu kolmeen osa-alueeseen. Turvallisuusjohtamista koskevassa osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on riittävät turvallisuusjohtamisen valmiudet sekä kyvykkyys. Fyysistä turvallisuutta koskevassa osa-alueessa kuvataan salassa pidettävien tietojen fyysistä käyttöympäristöä koskevat vaatimukset. Teknistä tietoturvallisuutta koskevassa osa-alueessa kuvataan puolestaan tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset (Puolustusministeriö, 2015).

3.4 Tietojärjestelmien arviointi ja hyväksyntä

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen NCSA-toiminnon tehtävänä on tarjota arviointi- ja hyväksyntäpalveluita. Näitä palveluita tarjotaan kansainvälisistä tietoturvallisuusvelvoitteista, turvallisuusselvityksistä sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettujen lakien mukaisesti. Toiminnon tehtävänä on viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden edistäminen ja varmistaminen (Kyberturvallisuuskeskus, 2019).

Tietojärjestelmien hyväksyntäpalvelua tarjotaan sellaisille valtionhallinnon organisaation tietojärjestelmille, jotka käsittelevät tai säilyttävät esimerkiksi kansallista, EU- tai NATO-luokiteltua salassa pidettävää tietoa ja mikäli laki kansainvälisistä tietoturvallisuusvelvoitteista tai laki turvallisuusselvityksistä edellyttää hyväksyntää kansalliselta tietoturvaviranomaiselta. Tietojärjestelmien arviointipalvelua voidaan tarjota viranomaisen määräämisvallassa oleville tai hankittavaksi suunnittelemille tietojärjestelmille, joissa käsitellään tai säilytetään salassa pidettäviä tietoja. Kohdeorganisaation on tehtävä tästä arvioinnista erillinen pyyntö NCSA-toiminnolle. Arviointipalvelua tarjotaan myös Valtiovarainministeriön pyynnöstä tehtäviin selvityksiin valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta (Kyberturvallisuuskeskus, 2019).

Arviointi- tai hyväksyntäprosessi koostuu vähintään kuudesta keskeisestä prosessista, sekä näitä täydentävien osaprosessien mukaan onko kyseessä arviointi vai hyväksyntä. Prosessin vaiheita ovat:

1. Arviointipyyntö
2. Pyynnön tarkastus ja Traficomin vastaus
3. Esipalaveri toimeksiantajan kanssa
4. Arvioinnin tai hyväksynnän valmistelevat toimet
5. Arviointi
6. Arvioinnin jatkamisen perusteet, arvioinnin päättäminen
7. (Hyväksyntä, todistus vaatimustenmukaisuudesta)

Arviointi- tai hyväksyntäpyyntö suositellaan lähetettäväksi vasta, kun tilaajaorganisaatio arvioi itse täyttävänsä käytettyjen arviointikriteeristöjen, Katakri 2015 tai PiTuKri, vaatimukset. Arviointi koostuu yleensä hallinnollisesta ja tek-

nisestä turvallisuuden osuudesta mutta arviointiin voi sisältyä myös fyysisen turvallisuuden osuus. Arviointi- tai hyväksyntäpyyntö voidaan myös keskeyttää tilanteissa, joissa prosessia ei pystytä aloittamaan, jos arvioinnissa todettujen poikkeamien korjauksesta ei saada näyttöä 6 kuukauden aikana tai tilaajaorganisaatio pyytää arvioinnin keskeyttämistä (Kyberturvallisuuskeskus, 2019).

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arvioinnista mukaan viranomaiset saavat käyttää tietoturvallisuuden arvioinnissa myös Traficomin hyväksymiä tietoturvallisuuden arviointilaitoksia. Hyväksyntä tietoturvallisuuden arviointilaitokseksi edellyttää erillistä menettelyä tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaisesti.

Tiedon säilyttämisen osalta käsiteltävien tietojen luokittelu määrittelee järjestelmän vaatimukset. Tapauksissa, joissa kaupunki ja viranomainen ovat kameravalvontajärjestelmän yhteisrekisterinpitäjiä voivat arviointi- tai hyväksyntävelvollisuudet kohdistua molempiin organisaatioihin. Kameravalvontajärjestelmässä tiedot luokitellaan yleisesti henkilötiedoiksi. Kameravalvontajärjestelmän tietosuojaselosteen käyttöperusteen mukaan tietojen luokittelu voi kuitenkin vaihdella. Kameravalvonnan näkökulmasta esimerkiksi biometriset tai geneettiset tiedot luokitellaan erityisiin henkilötietoryhmiin kuuluviksi tiedoiksi. Erityiset henkilötietoryhmät ovat julkisuuslain (621/1999) mukaan salassa pidettäviä tietoja. Kansallista tai kansainvälistä salassa pidettävää tietoa lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arvioinnista (1406/2011) mukaan Liikenne- ja viestintävirasto Traficom voi myöntää vaatimukset täyttävälle salassa pidettäviä tietoja käsittelevälle järjestelmälle hyväksynnän.

3.5 Kameravalvontajärjestelmän tietoturvan vähimmäisvaatimukset

Tiedon käsittelyyn ja tiedonhallintaan laadittiin tiedonhallintalaki (906/2019). Lain avulla selkiytetään julkishallinnossa tietoon ja sen hallintaan liittyviä seikkoja. Lisäksi lain avulla täsmennetään ja yhdenmukaistetaan datan hallintaa, sen käsittelyä sekä luovuttamista. Valtionvarainministeriö on valmistellut erinäisiä suosituksia, jotka toimivat ohjenuorana eri tahojen tiedonhallinnasta vastaaville henkilöille, heidän laatiessaan yrityksensä tai muun tahon toimia ja ohjeita (Valtiovarainministeriö, 2019).

Poliisi on ottanut käyttöön oman pilvipalvelun nimeltä Pouta. Järjestelmän avulla kansalaiset voivat toimittaa poliisille rikoksiin tai muuhun poliisitutkintaan liittyviä videota ja kuvamateriaalia. Palvelu toimii väliaikaisena yhdyskäytävänä poliisille ja vastaanotettu aineisto käsitellään tietosuojavelvoitteiden mukaisesti. Käytännössä poliisi suorittaa toimitetulle materiaalin esiselvityksen, jonka jälkeen se siirretään pilvipalvelusta turvallisuusverkon sisälle liitettäväksi tietyn tutkinnan todistusaineistoksi. Vasta materiaalin päätyessä

turvallisuusverkon sisään aineisto luokitellaan tapauskohtaisesti (Pouta, 2020). Samaa logiikkaa voi soveltaa kaupunkien kameravalvontajärjestelmien osalta. Julkisille paikoille kuvaavat kamerat eivät sisällä pääsääntöisesti salassa pidettävää aineistoa. Mikäli poliisi suoraan omilla käyttöoikeuksilla tai muun tahon kautta hankkii materiaalia liitettäväksi poliisin tutkintaan, järjestelmästä tuotu materiaali liitetään vain siltä osin mukaan asiaan. Vasta käsitelty ja liitetty materiaali perii poliisiasian salassapitosäännökset sekä elinkaaren.

Tarkasteltaessa kaupungin tai kunnan valvontakamerajärjestelmiä olisi syytä noudattaa tietoturvallisuuden osalta julkisen hallinnon tiedonhallintalain 12-18§:ssä esiintuotuja seikkoja, jolloin ne täyttäisivät lain vähimmäisvaatimukset. Alaotsikoissa kukin vaatimus tuodaan esille kytkettynä kaupunkikamerajärjestelmänkontekstiin.

3.5.1 Kameravalvontaan liittyvät erityistä luotettavuutta vaativat tehtävät ja käyttöoikeudet

Kameravalvontajärjestelmät tilataan yleisesti niitä toimittavilta yrityksiltä. Kaupunkien hankintoja koskee niin kilpailutuslainsäädäntö, kuin hankinnasta luotava sopimus. Sopimuksessa on tärkeä huomioida, että laitteilla tullaan käsittelemään henkilötietoja ja niitä asentavilta tahoilta edellytetään erityistä luotettavuutta. Monesti järjestelmän asentanut taho toimii myös sen ylläpitäjä, jolloin huolto- ja korjauspalvelut on hankittu samojen kilpailutusten kautta. Ylläpitäjä tällöin suorittaa myös järjestelmän päivityksen sekä lisää tai poistaa laitteita järjestelmästä.

Asennuksen jälkeen järjestelmän pääkäyttäjät vastaavat järjestelmän toimivuudesta ja tietosisällöstä sekä käyttöoikeuksista ja niiden hallinnasta sekä ajantasaisuudesta. Käyttäjien rooleja olisi myös hyvä jakaa niihin, ketkä voivat käsitellä reaaliaikaista videokuvaa ja niihin, jotka pääsevät lisäksi hakemaan takautuvasti materiaalia. Tallenteisiin pääsevät käyttäjät myös yleisesti jakavat materiaalia sitä tietosuojaselosteessa määritetyille tahoille, kuten poliisille. Materiaalin säilyvyydelle voi luoda eri tasoja, jolloin käyttöoikeusluokkia voi olla enemmän. Huomioitava on se, että mitä pidempään materiaalia säilötään, sitä suurempaan henkilötietomassaan käsittelijällä on pääsy. Käyttöoikeuksia rajaamalla järjestelmän käyttöä voidaan itseasiassa laajentaa, kunhan kunkin käyttöoikeuden omaavan tahon käyttöoikeusperuste on selvästi tuotu esille ja perusteltu. Käyttöoikeuksien osalta on kuitenkin noudatettava vähimpien oikeuksien periaatetta, jolloin vain niille käyttäjille on oikeudet tietojärjestelmään, jotka ovat työn suorittamiseksi välttämättömiä (HE 284/2019).

Tiedonhallinnasta vastaavan tahon on määritettävä ne tehtävät, jotka vaativat henkilöiltä turvallisuusselvityslaissa (726/2014) määritetyn turvallisuusselvityksen tai muun henkilöarvioinnin liittyen yksityisyyden suojaan työelämässä liittyvän lain (759/2004) mukaisesti.

3.5.2 Kameravalvontajärjestelmän lokitietojen kerääminen

Tietojärjestelmästä vastaavan tahon on käsiteltävä lokitietoja suunnitelmallisesti ja perusteellisesti. Lokitietojen avulla voidaan valvoa järjestelmän käyttöä, väärinkäytöksiä ja tietoturva- sekä järjestelmähäiriötä. Valvontakamerajärjestelmän osalta käyttöoikeudet tulisi olla henkilökohtaiset. Näin käytön hallintaa voidaan määrittää paremmin ja esimerkiksi järjestelmästä muualle siirretty aineisto voidaan takautuvasti selvittää. Lokitietojen hallinta tulee siis kattaa koko elinkaaren ajan eli tietojen keräämisen, käsittelyn, säilyttämisen, luovuttamisen ja poistamisen. Lokitiedosta tulee ilmetä kirjautumisten lisäksi, käyttäjän tekemät toimet järjestelmässä sekä tapahtuma ja sen aikaleima eli päivämäärä ja kellonaika. Yleisesti viranomaistoimintaan liittyvien järjestelmien lokitietojen säilytetään viisi vuotta, mikä perustuu rikoksen vanhenemisaikaan (HE 284/2018).

Lokitietoja tulisi myös seurata säännöllisesti, jota varten olisi oma prosessinsa. Erilaisten automaattisten hälytysten käyttö helpottaa tietojen seurantaa ja analyysia. Esimerkiksi yhtäaikaisten eri päätelaitteilta tapahtuvien samojen käyttäjätunnusten kirjautumisyritykset voisivat tuottaa hälytyksen järjestelmän pääkäyttäjille. Näin reaaliaikainen puuttuminen ja reagoiminen häiriöihin olisi mahdollista. Samoin järjestelmään liitettyjen laitteiden toimintahäiriöt, kuten verkosta häviäminen tuottaisi hälytyksen.

Lokitietoja voidaan luovuttaa esimerkiksi viranomaisille tietoturvapoikkeamia ja rikostutkintaa varten. Järjestelmän omistajalla tulee olla prosessi ja toimintamalli lokipyyntöjen tarkastuspyynnöille. Lokit ovat osa järjestelmän tietoaineistoa, joten niitä tulee käsitellä yhtä tietoturvallisesti kuin muitakin järjestelmän osia. Lokit tulevat olla kirjoitussuojattuja ja niiden sijainti suositellaan olevan erillisessä lohkossa tai jopa toisessa tietokannassa (Viestintävirasto, 2016, s. 2-3).

3.5.3 Kameravalvontajärjestelmän tietojen elinkaari

Tiedon elinkaari koostuu tiedon kaikista vaiheista aina sen syntymisestä poistumiseen. Tiedon käsittelyn vaiheet ovat siis jaettu tiedon luomiseen tai vastaanottoon, säilytykseen, käyttöön, jakamiseen sekä arkistointiin tai tuhoamiseen. Valvontakamerat taltioivat ja joskus jopa säilövät sekä käsittelevät väliaikaisesti dataa. Tietoverkkojen dataa siirretään paikallisiin tallentimiin, jos sitä voidaan siirtää tai noutaa verkkoon liitettyjen päätelaitteiden avulla. Järjestelmän hallintaa organisoidaan hallintapalvelimen kautta, josta käyttäjien pyynnöt ja järjestelmän liikenne hyväksytään. Kameravalvontajärjestelmässä tietoa käsitellään siis useassa eri sijainnissa ja laitteessa. Tärkeää onkin huomioida, että järjestelmän tuottaman tiedon elinkaari on itse järjestelmän elinkaarta pidempi (HE 284/2018).

Tiedon luonnin vaiheessa on tunnistettava ja selvitettävä ne perusteet minkä vuoksi tietoa kerätään ja mihin käyttötarkoitukseen sitä hyödynnetään. Lisäksi tärkeänä seikkana tulee tunnistaa kerätyn tiedon erityisvaatimukset. Kaupunkikameravalvontajärjestelmän avulla on pääsääntöisesti tarkoitus kerä-

tä yleisiltä paikoilta videomateriaalia, joka sisältää henkilötietoja. Mikäli järjestelmän avulla kerättyä dataa jatkojalostetaan tekoälyä hyödyntäen siten, että tiedon luokka muuttaa muotoaan, tulee asian käyttötarkoitus ja peruste olla selkeästi avattuna tietosuojaselosteessa. Käsittelyn perustetta ei voi vaihtaa, mikäli järjestelmän käyttöperuste on aluksi sidottu toiseen tarkoitukseen (906/2019).

Tiedon säilytyksessä on huomioitu säilytettävän tiedon vaatimukset ja niistä syntyvät riskit. Riskejä olisi hyvä tunnistaa ja arvioida sekä huomioida toteutuneen riskin haittavaikutuksia ja keinoja hallita riskejä. Tiedon saatavuus ja säilyminen on turvattava (906/2019). Kameravalvontajärjestelmien tekoälyohjelmistot ovat varsin uusi ilmiö ja markkinoissa tapahtuu paljon muutoksia. Mikäli tekoälyä hyödynnetään kameravalvonnassa, olisi kriittistä suojata kameran taltioima raaka videomateriaali erikseen. Näin materiaaliin olisi pääsy, vaikka tekoälyohjelmisto ja sen tuottama data eivät olisikaan enää käytössä.

Tiedon käytössä on tärkeää huomioida se, kuka pääsee näkemään ja käsittelemään tietoa. Mitä enemmän valvontakamerajärjestelmällä on käyttäjiä ja käyttötarkoituksia sitä tärkeämpää on avata ja perustella käyttäjien käyttötarpeet ja sitoa ne käyttöperusteeseen (906/2019). Kameravalvonnan tekoälysovelluksissa tietoa voidaan käsitellä esimerkiksi tapahtumakohtaisesti. Näin tietyistä kameroista haetaan materiaali, jotta esimerkiksi tapahtunutta rikosta voidaan selvittää. Sovelluksessa itsessään tulisi myös olla käyttäjiä rajaavia ominaisuuksia, jotka perivät kameravalvontajärjestelmästä käyttöoikeushierarkian. Näin tietoon on pääsy niillä henkilöillä, joilla siihen on käyttöperusteen myötä käyttöoikeus. Tietojen käyttöä tulee valvoa, jotta tunnistettuja riskejä voidaan havaita sekä ryhtyä tarvittaviin toimenpiteisiin.

Tiedon jakamisesta tulee niin ikään mainita tietosuojaselosteessa. Jakaminen voi olla myös tiedon siirtämistä tai luovuttamista. Kaupungin kameravalvontajärjestelmissä yleinen tiedonjakokumppani on poliisi, jolle materiaali siirretään rikoksen tutkimiseksi. Jakamisessa tulee huomioida materiaalin suojaustasot, jolloin esimerkiksi salaamattoman sähköpostin käyttäminen ei ole sallittua. Myös tiedon vastaanottaja tulee olla varmistettu, jotta voidaan varmistua siitä, että materiaali päätyy sellaisella taholle, jolla on oikeus materiaali käsitellä (906/2019). Poliisilla on monen kaupungin kanssa rakennettu tekninen rajapinta siten, että polisi pääsee suoraan hakemaan materiaalia oman toimivaltansa perusteella. Tällöin tietojen luovutuksesta ei kirjata erillistä toimenpidettä, jolloin valvonnan ja lokien tallentamisen rooli korostuu entisestään. Tiedonsiirron teknisen rajapinnan osalta pitää varmistaa asianmukainen salaus, mutta myös se, että vastaanottajalla on tehtäväkohtainen peruste aineiston käsittelyyn. (906/2019)

Tiedon arkistoinnilla määritetään kerätyn tiedon säilyttämistä. Arkistoinnin tarkoituksena on rajata tallennetun datan elinkaari siten, että se on suhteessa käyttöperusteeseen. Arkistoinnin avulla voidaan myös määrittää tahoja, joilla on oikeus mihinkin osuuteen datasta. Tärkeänä seikkana on myös huomioida missä dataa fyysisesti säilötään ja millä tavoin (906/2019). Pilvipalveluiden yleistyessä datan fyysisen sijainnin merkitys korostuu entisestään, etenkin toi-

mittaessa viranomaisten kanssa. Pilvipalveluiden käyttö määrittää oma arviointikriteeristö PiTuKri, mikä on Kyberturvallisuuskeskuksen työkalu pilvipalveluiden turvallisuuden arviointiin. Viranomaisella on myös mahdollisuus julkaista tietoa avoimeksi dataksi. Julkaistaessa avointa dataa pitää tiedon luovuttajan anonymisoida tieto siten, ettei siitä ole julkaisuhetkellä tai teknisen kehityksen myötä tulevaisuudessa mahdollista muodostaa yksilöivää tietoa 906/2019). Viranomaisella on myös mahdollista rajatuissa tilanteissa julkaista myös erityisiä henkilötietoja, kun rikoksen estämiseksi tai rikollisen kiinnisaamiseksi tai tunnistamiseksi on välttämätöntä jakaa esimerkiksi kuvan rikoksen tekijästä (Poliisi 2020, 24). Kaupunkikamerajärjestelmästä voi siis päätyä julkisuuteen tietoja niin poliisin niitä julkaisemalla, mutta myös esitutkinta-aineiston kautta. Esimerkiksi rikoksen esitutkintapöytäkirjaan liitetty video pahoinpitelystä voi päätyä julkiseksi, ellei sitä ole erityisestä syytä määritetty salassa pidettäväksi. Vaikka esitutkintamateriaali on tutkinnan ajan salassa pidettävää, tuomioistuiminen päätöksiä ohjaa julkisuusperiaate ja näin ne ovat lähtökohtaisesti julkisia asiakirjoja (370/2007).

Tiedon tuhoaminen tulee toteuttaa, kun tiedon säilytysaika ja käyttötarve päättyy. Tiedon tuhoaminen pitää myös huomioida, kun tiedon keruuseen tai sen säilömiseen käytettyä laitteistoa huolletaan tai poistetaan. Erityisesti sähköisesti tuotettua ja käsiteltyä materiaalia poistettaessa tulee huomioida, ettei tieto ole uudelleen palautettavissa edes osittain (906/2019). Kiintolevyjen elinkaaren hallinnasta on laadittu oma ohjeistus Kyberturvallisuuskeskuksen toimesta. Ohjeesta löytyy seikkaperäisemmin tekniset keinot kiintolevyjen ylikirjoittamiseen ja uusikäyttöön (Viestintävirasto, 2016).

3.5.4 Kameravalvontajärjestelmän riskienhallinta

Riskienhallinnan avulla tietovarantoja ja järjestelmiä voidaan turvata sekä määrittää haluttua tietoturvan tasoa. Arvioimalla riskejä tuodaan esille käyttäjien tarpeiden ja vaatimusten, kustannusten sekä tietoturvallisuuden raja-arvoja. Näistä tunnistettujen riskien avulla voidaan tietojärjestelmän toimia mitata ja arvioida. Riskien toteumaa ja niiden aiheuttamia vaikutuksia voidaan myös ennalta arvioida ja suunnitella suojaavia toimia, niin ettei riskejä pääse toteutumaan tai niiden realisoituessa vahingot voidaan minimoida. Riskiarvio on jatkuvaa ja siihen tulee liittää toiminnan tavoitteet, määrittää vastuut sekä tuoda esille menettelytavat. Riskejä analysoimalla voidaan myös kehittää prosesseja, jotta toiminta on tietoturvallisempaa. Järjestelmän koko ja siihen liittyvät henkilöt sekä tahot vaikuttavat riskien koordinoitiin. Tärkeää on kuitenkin, että riskiarviointi ja sen seuranta on valtuutettu vähintään yhdelle taholle (HE 284/2018). Kaupunkikamerajärjestelmän näkökulmasta rekisterinpidossa määritettyjen järjestelmän käyttäjien puolelta olisi järkevää tarkastella riskejä kukin omasta tahostaan. Yhteistoiminnalla ja vastuunjakamisella tehostetaan riskien tunnistamista ja niiden arviointia sekä voidaan paremmin rakentaa prosessit riskien torjumiseksi ja vaikutusten vähentämiseksi. Kameravalvonnan käyttö ja etenkin siinä hyödynnettävä tekoälyn käyttö on hyvin kiinnostava aihe nyky-

medioiden näkökulmasta. Jotta vältytään tarpeettomalta huomiolta, järjestelmän läpinäkyvyys ja riskien tunnistaminen korostuu. Lisäksi havaittuihin tietoturvapoikkeamiin voidaan reagoida nopeasti.

Riskienhallinnan osalta on tärkeää myös dokumentoida koko prosessi. Riskiarvioissa on hyvä näkyä arvioidut riskit, niiden todennäköisyys, toimet riskien minimoimiseksi sekä jäännösriski. On myös hyvä tuoda ilmi mitä toteutuneesta riskistä seuraa. Korkeimpien riskien osalta olisi hyvä myös erikseen vielä avata prosessit ja vastuut riskien toteutuessa. Riskiarvion on osa jatkuvuussuunnittelua ja vaikuttaa merkittävästi myös järjestelmään liittyvään ohjeistukseen ja koulutukseen. Riskienhallintaa toteutetaan säännöllisesti koko tietoaineiston elinkaaren ajan. Seurantaa ja hallintatoimenpiteiden toteutumista tulisi toteuttaa vähintään neljä kertaa vuodessa ja ohessa olisi tarkastella myös onko aiemmin arvioidut tietoriskit vielä relevantteja vaiko vaativatko ne päivittämistä (VM 22/2017, s. 28).

3.5.5 Kerätty data ja sen luovuttaminen teknisen rajapinnan avulla

Tiedonhallintalain (906/2019) mukaan viranomaiset voivat rakentaa järjestelmien välille teknisen rajapinnan, mikäli vastaanottavalla taholla on kerättyihin tietoihin laissa säädetty tiedonsaantioikeus. Tapauskohtaisesti on kuitenkin pysyttävä varmistamaan, että tietoja vastaanottavalla taholla on siihen työtehtäviensä puolesta tarve, jos tiedot ovat henkilötietoja tai muita salassa pidettäviä tietoja. Mikäli kameravalvontajärjestelmä on ainoastaan kunnan vastuulla, eikä järjestelmää ole yhteirekisterinpidossa, tulee tietojen luovutus kirjata tapauskohtaisesti ylös. Tiedonhallinlain 23§:n mukaan avattaessa toiselle viranomaiselle tekninen katseluyhteys, on sitä rajattava vain tarpeellisiin tietoihin sekä tietojen hakemisen yhteydessä selvitettävä tietojen käyttötarkoitus. Lisäksi poikkeavat tietohaut tulee tunnistaa automaattisesti.

Teknisten rajapintojen kautta ei voida luovuttaa mitä tahansa tietoa, vaan sen tulisi olla määrämuotoista ja käyttöperusteeseen sidottu. Kameravalvontajärjestelmän osalta se olisi videomateriaalia tai siitä tekoälyllä prosessoitua dataa, johon luovutettavalla olisi tehtävään kuuluva käyttötarve. Mikäli tietoja luovuttavalla viranomaisella datan jakaminen olisi mahdollista kieltää, vedoten tiedon käyttötarpeeseen, teknistä rajapintaa tietojenluovutukselle ei saisi lakisääteisesti rakentaa (906/2019). Kaupunkikamerajärjestelmien osalta onki tärkeätä, että tekniset rajapinnat rakennetaan käsittelemään vain ja ainoastaan videomateriaaliin liittyvään aineistoon, eikä hallintapalvelimen kautta voitaisi hankkia muita tietoja, kuten järjestelmän lokitietoja. Yhteiskäyttöisten järjestelmien osalta toiminnallisen toteutustapa olisi kuitenkin aina yhteisrekisterinpito. Näin tekninen rajapinta ja tietojärjestelmän hallinta voitaisiin suunnitella sekä toteuttaa yhdessä ja molemmilla osapuolilla olisi omaa käyttöä varten tarpeelliset järjestelmäoikeudet.

Rakennettaessa teknisiä rajapintoja tiedonhallintalain (906/2019) 23§:n mukaan vastaanottava viranomainen määrittää ja vastaa niistä käyttöoikeuksista, joita se jakaa tarpeellisille henkilöille. Kyseisillä tahoilla tulee olla käsittely-

peruste järjestelmästä haettaville tiedoille ja tunnuksia hyödynnetään vain näiden työtehtävien hoitamiseksi. Taholla kenelle on luovutettu käyttöoikeudet järjestelmään, on ilmoitusvelvollisuus, jos käyttöoikeuksissa tulee muutoksia. Luovuttanut taho taas vastaa, että järjestelmän käyttöoikeudet ovat ajantasaisia ja oikeilla henkilöillä on pääsy järjestelmään (HE 284/2018).

Kameravalvontajärjestelmään kertyvän datan määrä on suuri ja sen sisältämien henkilötietojen lukumäärä mittava. Tämän vuoksi järjestelmästä ulos otettavan datan määrää tulee rajata käsittämään yksittäisiä pyyntöjä. Yksittäisen pyynnön avulla ei myöskään voida ladata isoa määrää tietoa kerralla, esimerkiksi yksittäisen kameran koko tallennuselinkaaren videomateriaalia. Katseluyhteyden osalta tiedonhakua voidaan rajoittaa antamalla käyttäjälle mahdollisuus kohdistaa tiedonhankintaa tiettyjen rajausten perusteella. Tietopyyntöön olisi hyvä liittää tiedonhaunperuste, josta kirjautuisi lokitiedon yhteyteen merkintä. Näin jokaisen tietohaun kohdalla käyttäjää vaaditaan arvioimaan kunkin tapahtuman käsittelyperuste (HE 284/2018). Yksittäisen käyttäjän useat ja laajat haut olisi syytä tunnistaa automaattisesti, jolloin poikkeavaan toimintaan voidaan puuttua nopeammin. Näin järjestelmän väärinkäytön riskiä voidaan madaltaa (VM 8/2017, s. 34-35). Kameravalvonnan osalta laajat haut tuottavat myös ison määrän dataa, koska nykyisten valvontakameroiden kuvanlaatu on teräväpiirtotasoa. Suurten videotiedostojen siirto vaikuttaa myös merkittävästi verkon kuormitukseen.

Kameravalvontajärjestelmien tietojen ollessa pääsääntöisesti salassa pidettäviä, teknisten rajapintojen kautta tapahtuva tiedonsiirto on toteutettava salattuna tai muuten suojattua tiedonsiirtoyhteyttä tai tapaa käyttämällä. Salaaminen tukee tiedon eheyttä, luottamuksellisuutta ja saatavuutta, mutta näiden takaamiseksi pitää teknisten ratkaisujen lisäksi huomioida hallinnolliset seikat. Mikäli reaaliaikaista kuvavirtaa siirretään julkisen verkon puolella, tietoliikenneyhteyden tulee olla suojattu esimerkiksi erilaisilla VPN-ratkaisuilla tai IPSec-salauksen turvin sekä käyttäen järjestelmässä palomuureja (HE 284/2019).

Henkilökohtaisten käyttäjätunnusten ja salasanojen avulla tiedonsiirron vastaanottoja voidaan tunnistaa. Näin voidaan myös varmistua siitä, että oikeat henkilöt pääsevät käsittelemään salassa pidettäviä henkilötietoja. Salasanalla tunnistamista voidaan vahvistaa monivaiheisen tunnistamisen avulla, jossa käyttäjätunnukseen liitettyyn laitteeseen tai tiliin lähetetään kertakäyttöinen erikseen hyväksyttävä vahvistusviesti. Käyttäjätunnuksen osalta on syytä myös huomioida kyseisen tunnuksen luku- ja kirjoitusoikeudet järjestelmässä. Näiden rajaaminen käyttövaltuuksien avulla parantaa tietoturvan kaikkia osa-alueita.

Fyysinen turvallisuus on myös merkittävässä roolissa, kun tietoaineistoja ja teknisiä rajapintoja toteutetaan. Järjestelmään liitettävät valvontakamerat ja niistä lähtevät tietoliikenneyhteydet tulee suojata niin fyysisiltä vahingoilta kuin osittain tunkeutumiseltakin. Esimerkiksi valvontakameran kautta on mahdollista päästä käsiksi tietoverkkoon, mikäli järjestelmään voidaan liittää siihen ulkopuolisia laitteita. Jokaisella laitteella on oma yksilöivä laitetunnus, jolloin asennusvaiheessa järjestelmä voidaan tietoteknisesti rajata sallimaan vai

kyseiset fyysiset laitteet. Lisäksi kameroissa ja kytkimissä sekä muissa verkkoon liitettävissä laitteissa olisi suositeltava käyttämään erilaisia murtosuojia (HE 284/2019).

Valvontakameramateriaalin käyttö sen vahvan todistusvoimaisuuden vuoksi, on yksi kaupunkikamerajärjestelmän parhaista osa-alueista. Tämän vuoksi tiedon muuttuminen ja eheys koko tiedon elinkaaren osalta on kriittistä. Näin oikeudessa käytettävää videoaineiston oikeellisuutta ei voida kiistää. Riskien arvioinnissa tulee huomioida ja määrittää riittävät toimet, jotta todistusvoimaisuus säilyy eikä tahalliset tai tahattomat virheet vaarantaisivat sitä (HE 284/2019). Esimerkiksi kameravalvonnan aikaleiman tulisi vastata sen hetkistä oikeaa aikaa. Tämän toteuttaminen mahdollisesti avoimesta verkosta suljetussa järjestelmässä vaatii toimenpiteitä tai ainakin käyttäjän pitää olla tietoinen vaadittavista toimista aikaleiman määrittämisessä.

3.6 Tietojenkäsittelyyn liittyvät sopimukset

Tekoälyn myötä valvontakamerajärjestelmien tuottama data tulee tulevaisuudessa saamaan monenlaisia erilaisia käyttötapauksia. Se ei enää ole pelkästään fyysisen turvallisuuden jatke. Tämä lisää entistään niin henkilötietojen käsittelyä kuin käsittelijöiden määrää. Tietosuoja-asetuksessa edellytetään, että kaikkien tahojen kanssa, jotka käsitelevät henkilötietoja rekisterinpitäjän lisäksi, tulee tehdä kirjallinen sopimus. Tietojenkäsittelysopimus ei kuitenkaan ole sama kuin tietojenluovutussopimus, jossa luovutettavien henkilötietojen koko määräysvalta siirretään toiselle taholle. Tietojenluovutuksesta puhutaan esimerkiksi silloin, kun valvontakameran dataa luovutetaan poliisille. Tällöin materiaali perii siihen liittyvän rikosilmoituksen elinkaaren ja poliisi vastaa täysin käsiteltävästä tiedostosta. Tietojenkäsittelysopimuksesta puhuttaisiin esimerkiksi, kun kaupunkisuunnittelu tekee videodatasta henkilölaskentaa jalkakäytävien uudistushankkeessa (Hanninen ym., 2017, s. 82).

EU-komissio on tehnyt tietojen käsittelyä ja siirtoa varten vakiolausekkeita, jotka löytyvät myös tietosuojavaltuutetuntoimiston sivuilta. Sopimuksessa voi myös olla itse laadittu, kunhan se sisältää seuraavat seikat:

- Henkilötietojen käsittelyn kohteet ja keston
- Käsittelyn tarkoituksen
- Mitä henkilötietoja käsitellään (esimerkiksi kuva, sukupuoli ja ikä)
- Rekisteröityjen ryhmät (esimerkiksi kaupungilla oleskelijat)
- Rekisterinpitäjän oikeudet ja velvollisuudet

Tietosuoja-asetuksessa on lisäksi erityisesti edellytettyjä sopimusehtoja. Henkilötietojenkäsittelijän tulee käsitellä henkilötietoja rekisterinpitäjän ohjeistuksen mukaisesti ja vain ainoastaan sovittua tarkoitusta varten. Rekisterinpitäjän tulee siis ohjeistaa käsittelijää ja käsittelijän tulee ohjeistus hyväksyä. Henkilötietoja

voidaan myös käsitellä EU-alueen ulkopuolella ja kielto tai puolto asiasta tulee mainita sopimuksessa. Henkilötietojen käsittelijän tulee varmistaa, että ne henkilöt, jotka lopulta käsittelevät henkilötietoja noudattavat salassapitovelvollisuutta. Käsittelijän tulee myös arvioida omasta toiminnastaan aiheutuvia riskejä henkilötietojen käsittelyssä. Esimerkiksi siten, että raakavideodatan sijasta henkilötietojen käsittelijälle toimitetaan vain anonymisoidut kuvat, josta lopullinen henkilölaskenta tehdään (Hanninen ym., 2017, s. 84-86).

Henkilötietojen käsittelijä ei saa käyttää tiedon käsittelyyn alihankkijaa, ellei se ole erikseen sopimuksessa sallittu. Rekisterinpitäjä voi vaatia, että aina kun uusia alihankkijoita tarvitsee vaihtaa tai lisätä ne tulee hyväksyttää rekisterinpitäjällä. Käsittelijällä on velvollisuus ilmoittaa, mikäli alihankinnoissa tapahtuu muutoksia. Tärkeää on myös huomioida, että mikäli rekisteröity haluaa tarkastaa omia tietojaan, tulee sopimuksessa sopia myös tarkastuksen toteuttamisesta henkilötietojen käsittelijän ylläpitämistä tiedoista. Lisäksi käsittelijällä on velvollisuus avustaa rekisterinpitäjää siinä, että rekisterinpitäjä toiminta täyttää tietosuoja-asetuksen vaateet. Avustusvelvollisuus koskee kuitenkin ainoastaan niiltä osin mitä tietoja käsittelijä käsittelee. Henkilötietojen käsittelijä on järjestettävä henkilötiedot siten, että ne ovat poistettavissa tai palautettavissa rekisterinpitäjälle tämän niitä pyytäessä. Käsittelijän tulee myös mahdollistaa rekisterinpitäjälle keinot auditointien tai muiden henkilötietoihin kohdistuvien tarkastusten suorittamiseksi, mikäli rekisterinpitäjä tällaisia päättää toteuttaa (Hanninen ym., 2017, s. 87-90).

Tietojenkäsittelysopimuksessa sovitaan myös vahingonkorvauksista ja vastuunrajoituksista. Vahingonkorvaukset voidaan myös rajata sopimuksen ulkopuolelle siten, että tahot vastaavat täysimääräisesti itse aiheutuneiden vahinkojen korvaamisesta. Tietosuoja-asetuksessa ei ole linjattu tietojenkäsittelysopimuksesta aiheutuvien kulujen maksullisuudesta ja siitä, miten ne jakautuvat. Tietosuoja-asetus on kuitenkin tuonut paljon enemmän vastuita ja velvollisuuksia henkilötietojenkäsittelyn suhteen, jotka nostavat kuluja. Järkevintä olisi kuitenkin liittää kulut pääsopimuksen hintaan. Kuluista sopiminen myös tehostaa seurannan ja valvonnan suorittamista. Yleisesti tarkastustoimenpiteet aiheuttavat ainakin työajallisia kuluja ja jos ne on sovittu jo pääsopimuksen sisälle, velvoitetaan niitä toteutettavaksi säännöllisin väliajoin (Hanninen ym., 2017, s. 91-92).

Henkilötietojen luovutuksesta tulisi olla myös tietosuojaselosteessa merkintä. Esimerkiksi kirjaamalla kenelle järjestelmän tietoja voidaan luovuttaa ja millä perusteella. Valvontakameroiden osalta tietojenluovutuksen yleisin kohde on poliisi, joka hyödyntää kameradataa rikosprosessissa. Mikäli tietojen luovutus perustuu lakiin, eikä niistä tarvitse tehdä erillistä sopimusta. Mikäli rekisterinpitäjä käsittelee itse tietoja toisessa yhteydessä kyseessä voi olla tietojen siirtämistä rekisterinpitäjältä käsittelijälle tai luovuttamista rekisterinpitäjältä toiselle rekisterinpitäjälle. Kaupunkikamerajärjestelmän osalta kannattaisi poliisin kanssa tehdä yhteisrekisterinpitosopimus, jossa sovittaisiin järjestelmän yhteiskäytöstä ja vastuista. Henkilötietojen luovuttaminen vaatii aina sen, että luovutettavalla taholla on laillisen peruste käsitellä kyseisiä henkilötietoja. Henkilö-

tietojen luovutuksesta tulisi laatia erillinen luovutus- tai yhteistyösopimus, johon olisi kirjattava ainakin seuraavat asiat:

- Mitä henkilötietoja luovutetaan ja millä perusteella
- Milloin ja miten tiedot luovutetaan
- Miten tietoturvasta huolehditaan
- Vastuu omien tietosuojaselosteiden päivityksestä, jotta rekisteröityjen oikeudet toteutuvat
- Tietoja vastaanottavan ilmoitusvelvollisuus rekisteröidyille uusien tietosuoja-asioiden päivityksestä
- Tietoja luovuttavan tahon vastuu luovutettavien tietojen ajantasaisuudesta ja rekisteröidyn tekemistä ilmoituksista
- Sopimuksen voimassaoloaika

Tietosuoja-asetuksessa luovutussopimusta ei kuitenkaan ole kuitenkaan erikseen säädetty, mutta sen laatiminen selkeyttää ja parantaa molempien osapuolten oikeusturvaa (Hanninen ym., 2017, s. 93-96).

3.7 Kyberrikollisuus ja siltä suojautuminen

Rikollisuutta esiintyy monessa muodossa ja yleisesti niiden taustalla on vanhojen käyttäjätunnusten ja salasanojen pareja tai osia niistä, jotka ovat vuotaneet erilaisten tunnistettujen tai tuntemattomien tapausten yhteydessä. Tietomurrot ovat erilaisten tahattomien tai tahallisten haavoittuvuuksien tai heikkojen toteutusten myötä yleistyneet viime vuosina rajusti, kuten tämän luvun alussa totesimme. Tietomurrolla tarkoitetaan luvatonta tietojärjestelmään, palveluun tai laitteeseen tunkeutumista, esimerkiksi sähköpostitilin luvatonta käyttöä haltuun saatujen tunnusten avulla. Tietomurto ja sen yritys on rikoslaissa määritelty rangaistava teko. Kohteen tai käytettyjen tietojen hyväksikäyttöä ei edes tarvita, pelkkä luvaton tunkeutuminen riittää täyttämään rikoksen tunnusmerkistön (Kyberturvallisuuskeskus, 2019).

Tietomurroilla pyritään saamaan taloudellista hyötyä. Murrettua kohdetta voidaan käyttää jakamaan haitallista materiaalia, käyttämällä sitä osana muita hyökkäyksiä tai murretun kohteen tiedot voidaan lamauttaa kiristyshaittaohjelmilla. Tietomurtoja voidaan tehdä myös ihan puhtaasti kiusantekona, jolloin esimerkiksi saatavilla olevat heikosti suojatut järjestelmät tehdään toimintakelvottomiksi tai tahtotilana on organisaation tavallisen asioinnin estäminen. Tietomurrot aiheuttavat organisaatiolle taloudellisia- ja mainehaittoja, jonka lisäksi organisaation toiminta voi keskeytyä pitkäksikin aikaa. Näitä tunnistettuja riskejä vastaan on syytä suojautua (Kyberturvallisuuskeskus, 2019).

Kyberturvallisuuskeskus suosittelee neljää toimintoa, kuinka suojautua tietomurroilta:

- Pidä ohjelmistot ja järjestelmät päivitettynä
- Käytä monivaiheista tunnistautumista
- Älä käytä samoja salasanoja useammassa eri palvelussa
- Muista varmuuskopiot

Erittäin tärkeää suojautumisen kannalta on pitää järjestelmien ja laitteiden päivityksen ajan tasalla. Ohjelmistopäivityksiä julkaistaan tasaisesti ja monet niistä sen vuoksi, että niillä korjataan haavoittuvuuksia tuotteesta. Haavoittuvat järjestelmät ovat suurempi riski tietomurron kohteeksi. Monivaiheisella tunnustautumisella tarkoitetaan käyttäjätunnuksen ja salasanan täydentävää menetelmää, kuten kertakäyttöinen koodi tai tekstiviesti, käyttäjän tunnistamiseksi. Internetissä on miljoonia käyttäjätunnus-salasana-pareja, jotka on vuodettu internetissä käytettyjen palveluiden suurien salasanavuotojen myötä. Käyttämällä pitkiä ja vahvoja eri salasanoja järjestelmissä vaikeutetaan sanakirjahyökkäyksiä tai vuotaneiden tunnusten hyväksikäyttöä. Tärkeimmät tiedot ja palvelut on hyvä varmuuskopioida kiristyshaittaohjelmien varalta. Järjestelmien ja tietojen kahdentaminen sekä niiden säilyttäminen erillään varmistaa, että tiedot ja tarvittavat asetukset voidaan palauttaa (Kyberturvallisuuskeskus, 2019).

Mikäli henkilö tai organisaatio joutuu tietomurron kohteeksi, tulisi toimia seuraavanlaisesti:

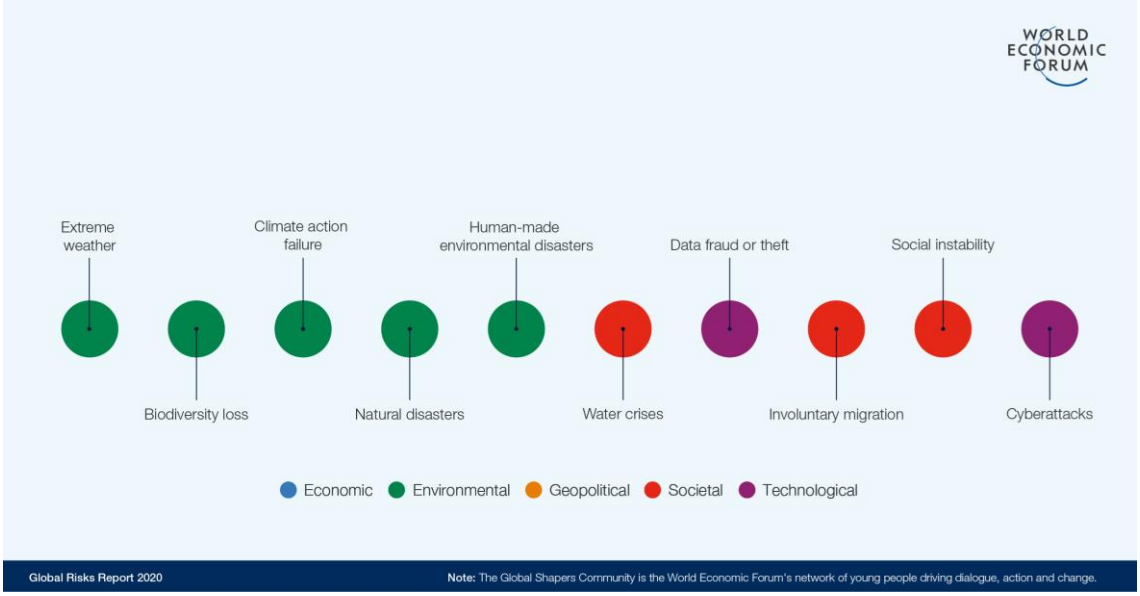
- Ilmoita
- Eristä murretut kohteet
- Vaihda salasanat / lukitse tunnukset
- Varmista lokit
- Palauta varmuuskopiot
- Muista viestintä

Tietomurrosta olisi syytä aina ilmoittaa Kyberturvallisuuskeskukseen ja tehdä rikosilmoitus poliisille. Ilmoitukset ovat tehtävissä sähköisesti lomakkeilla tai sähköpostilla viranomaisten internetsivujen kautta. Jos tietomurron seurauksena on saatu haltuun suojattavia tai salassa pidettäviä tietoja, on kyseessä tietovuoto. Mikäli epäilet, että murretut tai vuotaneet tiedot sisältävät henkilötietoja, on kyseessä tietosuojarikkomus, josta täytyy tehdä ilmoitus tietosuojavaltuutetulle (Kyberturvallisuuskeskus, 2019).

3.8 Toimitusketjuturvallisuus

World Economic Forumin vuoden 2020 riskiraportin mukaan maailma on siirtynyt taloudellisista riskeistä ympäristö- ja teknologisiin riskeihin viime vuosina (kuvio 3). Ilmastoriskien hallitessa viiden todennäköisimmän riskin titteliä vuonna 2020. Teknologiset riskit kuten datapetokset tai -varkaudet ja kyberhyökkäykset ovat menettäneet vuosien 2018 ja 2019 kärkisijoituksensa. Tämä

ei kuitenkaan tarkoita, että ne olisivat hävinneet, vaan ennemminkin korostaa ilmastoriskien vakavuutta. Yli 50 % maailman ihmisistä ovat verkossa. Digitaalinen teknologia tarjoaa valtavia hyötyjä mutta luo samalla merkittävän riskin. Informaatioinfrastruktuurin romahtaminen nähdään vaikutuksiltaan kuudenneksi suurimpana riskinä (World Economic Forum, 2020, s. 7).



KUVIO 3 Pitkäaikaisen riskin näkymät (World Economic Forum, 2020)

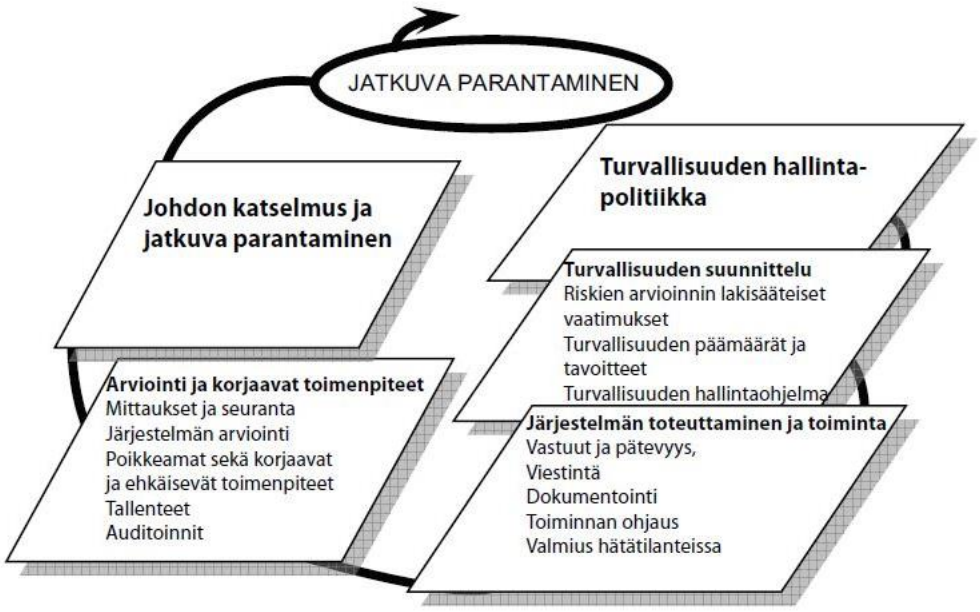
Riskien hallitsemiseksi on olemassa erinomaisia hallintajärjestelmiä, joista ehkä tunnetuin on ISO 28000 standardi. Standardit pitävät sisällään monesti erinomaisia elementtejä halutun toiminnon hallintaan. ISO 28000 standardi on nimensä mukaisesti suunniteltu parantamaan toimitusketjun turvallisuutta (ISO 28000, 2012, s. 6). Standardi käsittelee asioita organisaatiotasolla, koosta riippumatta, ja vaatii organisaatiota arvioimaan ja määrittelemään erilaisia turvallisuuden elementtejä toimintoympäristössään liittyen toimitusketjuturvallisuuteen. Standardi on helppokäyttöinen ja muodollisella lähestymisellä turvallisuuden hallintaan voidaan myötävaikuttaa suoraan liiketoiminnan tuottavuuteen ja uskottavuuteen organisaatiossa. Standardin vaatimusten täyttäminen ei kuitenkaan automaattisesti täytä lakisääteisiä velvoitteita (ISO 28000, 2012, s. 8).

Standardissa määritellään myös jatkuvan parantamisen elementit hallintajärjestelmässä (kuvio 4), jonka avulla säännöllisesti toistuvan prosessin mukaisesti organisaatio kykenee oman turvallisuuspolitiikan mukaisesti parantamaan omaa turvallisuuden suorituskykyään. Hallintajärjestelmän ylläpito vaatii luomista, dokumentointia, toteutuksia ja tehokasta käyttöä organisaatiolta, jotta se voi tunnistaa mahdolliset turvallisuusuhat ja riskit sekä lieventää niiden vaikutuksia (ISO 28000, 2012, s. 14). Tehokkaisiin turvallisuuden hallintajärjestelmän elementteihin kuuluvat seuraavat ylätason elementit standardin 4. luvussa:

- Yleiset vaatimukset
- Turvallisuuden hallintapolitiikka

- Turvallisuusriskien arviointi ja suunnittelu
- Järjestelmän toteuttaminen ja toiminta
- Arviointi ja korjaava toiminta
- Sisäinen auditointi ja jatkuva parantaminen

Jokainen ylätason elementti jakautuu vielä alemman tason elementteihin, jotka täydentävät toisiaan muodostaen yhtenäisen ja kokonaisvaltaisen turvallisuuden hallintajärjestelmän (ISO 28000, 2012, 14-30).



KUVIO 4 Jatkuvan parantamisen elementit hallintajärjestelmässä (ISO 28000, 2012, s. 14)

International Organization for Standardization tarjoaa yli 22000 standardin kokoelman erilaisiin käyttötapauksiin. Sen etuina voidaan pitää muun muassa arvoja kuten itsenäisyys, kansainvälisyys ja taloudellinen riippumattomuus (ISO, 2019, s. 3).

ISO-perheen standardit vastaavat erinomaisesti turvallisuusjärjestelmien toimitusketjujen haasteelliseen ympäristöön, jossa toimijoita voi olla monessa tahossa eri sidosryhmien, toimittajien, valmistajien ja valvonnan tai käsittelijän roolissa. Vastuulliset organisaatiot ottavat turvallisuuden tosissaan ja pyrkivät parantamaan sen kokonaisvaltaista hallintaa monesti eri keinoin, kuten erilaisilla standardeilla, kriteeristöillä tai muilla hyväksi todetuilla keinoilla. Standardinmukaisuus nähdäänkin usein organisaatioissa myös jatkuvuuden ja laadun takaajana, jolla luodaan lisäarvoa luotettavuuden ja kilpailuedun muodossa. Yhä kompleksisemmassa tulevaisuuden toimintaympäristössä turvallisuuden hallinnan merkitys korostuu muun muassa uusien teknologioiden käytön lisääntyessä ja datan merkityksen korostuessa. Kokonaisuuden hallinta voi olla hankalaa, kun turvallisuus ei rajoitu vain laitteiden käyttäjiin tai omistajiin. Riskit voivat myös olla tahallisia tai tahattomia. Haavoittuvuudet voivat olla

ohjelmistoon koodattuna tai laitteeseen fyysisesti valmiina asennettuna. Hyökkääjät hyödyntävät nollapäivähaavoittuvuuksia aktiivisesti ja etsivät sopivia kohteita. Tiedon on todettu olevan valtaa ja sitä on tavoiteltu historian saatossa monien tahojen toimesta, monella eri tavalla. Tietoja on hankittu, laillisesti tai laittomasti, aina esimerkiksi valtioiden päätöksenteon tukemiseksi, oman taloudellisen edun vuoksi tai yritysmaailman teknologiajohtajuuden saavuttamiseksi. Lopulta on kysymys kohteen riskienarvioinnista omien tietojensa käsittelyn ja säilyttämisen suhteen. Lisäksi valintaan luonnollisesti voivat vaikuttaa turvallisuuden lisäksi eettiset kysymykset tai kansallinen lainsäädäntö.

3.9 Tapaus Hikvision ja Dahua

Hikvision on yksi maailman suurimmista videovalvontamarkkinoiden tuottajista. Yritys tuottaa kameravalvontatuotteita globaalisti useille eri toimijoille, mukaan lukien julkinen sektori ja viranomaiset. Yritys on perustettu vuonna 2001 ja sen omistuspohja on osin valtio-omisteinen. Yrityksen pääkonttori sijaitsee Hangzhoussa Kiinassa (Hikvision, 2019, s. 21).

Vuonna 2017 Hikvisionin kameramalleista löytyi vakava haavoittuvuus. Haavoittuvuuden avulla hyökkääjä pystyi luomaan järjestelmään autentikoidun käyttäjän tunnuksen ja salasanan itselleen. Hyökkääjän oli mahdollista saada haltuunsa ylläpitäjäoikeuksilla kokonaisia järjestelmiä. Haavoittuvuus oli sisäänrakennettu kameroiden laiteohjelmistoon, eikä laiteohjelmistoa ollut päivitetty muutamaan vuoteen. Yhdysvaltain turvallisuusviranomainen CISA (Cybersecurity and Infrastructure Security Agency) ja useat muut tahot vahvistivat haavoittuvuuden ja arvioivat sen vaikutuksiltaan kriittiseksi ja helpoksi hyödyntää (CISA, 2017).

Hikvision ei ole yksin näiden ongelmien kanssa. Maailman toiseksi suurin toimittaja, kiinalainen Dahua on myös ollut myrskyn silmässä viime aikoina. Dahuan kameroista on löydetty haavoittuvuus, jonka avulla kameraa on pystytty käyttämään salakuunteluun. Kameran ääni ominaisuuden deaktivointi asetuksista ei vaikuta laitteen ominaisuuksiin (IPVM, 2019). Dahuan tuotteista on aikaisemmin löydetty myös toinen vakava haavoittuvuus, jolla hyökkääjä pääsee käsiksi kameroiden ja tallentimien dataan ilman autentikointia. Yhdysvallat on tämän vuoksi säätänyt erillisen lain, jonka myötä muun muassa Hikvisionin ja Dahuan tuotteet kielletään (US Congress, 2018).

Kyse ei kuitenkaan ole vain kiinalaisista kameravalmistajista, vaan ongelma on usein riittävän suunnittelun, riskienarvioinnin, elinkaaren huomioimisen ja kokonaisuuden hahmottamisen puute. Näiden esimerkkitapausten myötä kuitenkin korostuu erityisesti järjestelmien, tallentimien ja muiden oheislaitteiden ylläpito, säännöllinen päivittäminen sekä standardinmukaisuus. Sataprosenttisen turvallisuuden saavuttaminen on mahdotonta mutta pyrkimys jatkuvaan turvallisuuden kokonaisvaltaiseen parantamiseen on keino, jolla voidaan saavuttaa merkittäviä hyötyjä.

4 TEKOÄLY KAMERAVALVONNASSA

4.1 Tekoälyn määritelmä

Tekoälyä voidaan nykyisin pitää varsin kiinnostavana aiheena. On lähes mahdotonta olla törmäämättä tekoälyä koskevaan uutisointiin ja keskusteluihin (Elements of AI, 2020). Sen määrittely ei kuitenkaan ole ihan yksinkertainen asia. Merilehto (2018, s. 8) määrittelee tekoälyn koneen suorittamana toimintana, esimerkiksi päättelynä, oppimisena, ennakoimisena, päätöksentekona, näkönä ja kuulona, jotka ihmisen suorittamana olisivat älykästä toimintaa. Nokian hallituksen puheenjohtaja Risto Siilasmaan mukaan ihmiset vertaavat tekoälyä sähköön, koska sillä tulee olemaan yhtä suuri vaikutus jokaiseen ihmiselämän sektoriin (Wired, 2019). VTT:n tutkijat määrittelevät tekoälyn välineeksi, jonka avulla koneet, laitteet, ohjelmat, järjestelmät ja palvelut voivat toimia tehtävän ja tilanteen mukaisesti järkevällä tavalla (Valtioneuvosto, 2018, s.1). Tekoälylle ei kuitenkaan ole olemassa yhtä yhteistä määritelmää, vaan sitä määritellään eri lähteiden mukaan hieman eri tavalla. Edes tekoälytutkijat eivät käytä yhtä yleisesti hyväksyttyä määritelmää. Tekoälyn määritelmä määritellään sitä mukaa jatkuvasti uudelleen, kun tiettyjen aihepiirien ei enää katsota kuuluvan siihen tai uusia erikoisalueita syntyy (Elements of AI, 2020).

Tekoäly on käsitteenä siis laaja ja moniulotteinen, jonka alle kuuluu joukko erilaisia menetelmiä, teknologioita, sovelluksia ja tutkimussuuntia. Teknologisen kehityksen lisäksi tekoäly vaikuttaa koko yhteiskuntaan ja ihmisiin, jonka myötä tekoäly voidaankin liittää useisiin tieteenaloihin. Tekoälytekniikoita voidaan hyödyntää ja soveltaa useilla eri aloilla, kuten esimerkiksi lääketieteessä, kaupassa, teollisuudessa, poliisitoimessa tai sodankäynnissä (Valtioneuvosto, 2018, s.6).

Tekoälyn oppi-isänä pidetään englantilaista matemaatikko, loogikko ja kryptoanalyytikko Alan Turingia (1912-1954). Hänet muistetaan panostuksistaan tekoälyn ja nykytietojärjestelmätieteen saralla. Erityisesti hänen saavutuksensa saksalaisen salakirjoitusjärjestelmä Enigman murtamisessa toisen maailmansodan aikana ovat nousseet esille. Parhaiten Turing tunnetaan kuitenkin ns.

Turingin testistä, jonka avulla testataan koneen kykyä ajatella ihmisen tavoin. Testissä ihminen asetetaan tuomarin rooliin ja eristetään kahdesta keskustelijasta, joista toinen on kone ja toinen ihminen. Tuomari käy keskustelua molempien kanssa. Jos kone onnistuu huijaamaan tuomaria uskomaan kykenevänsä uskottavaan ja ihmismäiseen keskusteluun, voidaan sanoa, että kone on läpäissyt Turingin testin (CIA, 2015).

Vaikka monimutkaisten matemaattisten tehtävien ratkaiseminen tietokoneen avulla on nopeuttanut maailman kehittymistä monin tavoin, ihmiselle intuitiivisten mutta vaikeasti formaalissa muodossa esitettävien tehtävien ratkaiseminen on tekoälylle suuri haaste. Modernit tekoälysovellukset perustuvat pääosin datasta oppimiseen. Ollakseen älykäs ja vuorovaikutuskykyinen tietokoneen täytyy pystyä oppimaan asioita esimerkiksi kuvista, äänistä, teksteistä, sähkösignaaleista ja tapahtumasekvensseistä eli suurista tietomassoista. Menetelmien älykkyydestä ja oppimiskyvystä huolimatta tieto on kuitenkin datassa. Tekoäly ei pysty lisäämään, luomaan tai oppimaan sellaista tietoa, jota niiden käyttämä data ei sisällä (Tuominen, H., Neittaanmäki, P., Niinimäki, E., Pölönen, I., Rautiainen, I., Äyrämö, S., Ruohonen, T. & Nyrhinen, R, 2019, s. 2-3).

4.2 Tekoälyn käsitteistö

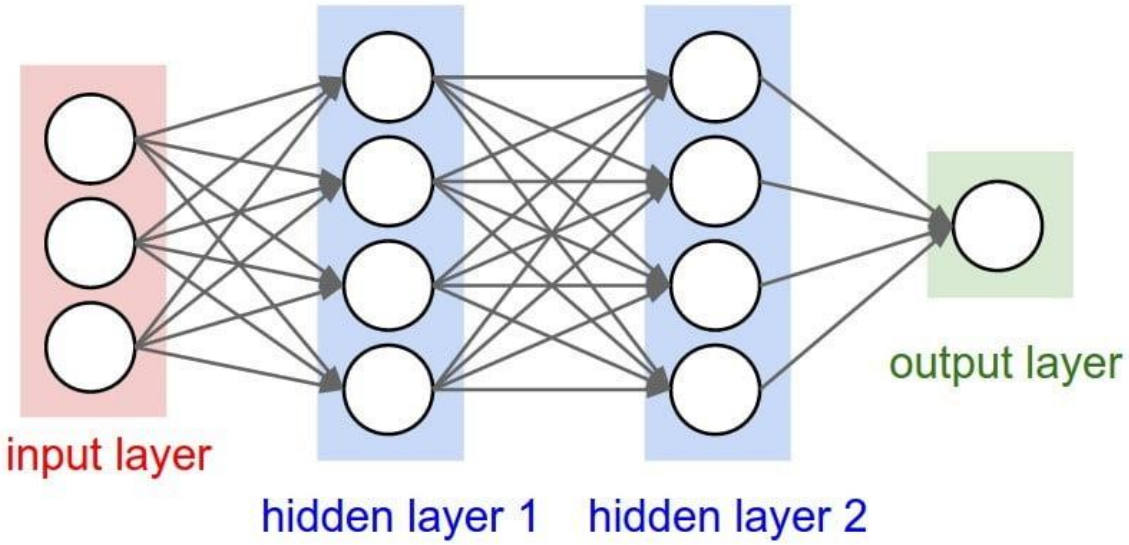
4.2.1 Koneoppiminen, syväoppiminen ja neuroverkot

Koneoppiminen (machine learning) on yksi tekoälyn osa-alue, jonka tarkoituksena on saada ohjelma toimimaan entistä paremmin pohjatiedon ja mahdollisen käyttäjän toiminnan perusteella. Koneoppimisessa kone oppii toistuvista tapahtumista ilman, että ihminen erikseen opettaa sitä. Koneoppimisella pyritään automatisoimaan tiedon tulkintaa ja laajentamaan koneen havainnointikykyä monimutkaisten algoritmien avulla perinteisen raja-arvoihin tukeutuvan mallin sijasta. Koneoppiminen voidaan jakaa kolmeen eri kategoriaan, ohjattuun oppimiseen, ohjaamattomaan oppimiseen ja vahvistettuun oppimiseen (Tuominen ym., 2019, s. 6). Merilehto jakaa koneoppimisen myös kolmeen vaiheeseen, joita voidaan hyödyntää liike-elämässä. Ensimmäisessä vaiheessa tehostetaan liiketoimintaprosesseja, tunnistetaan niiden välivaiheita, esimerkiksi päätöksiä, ja vähennetään niitä. Toisessa vaiheessa keskitytään mahdollisimman selkeisiin haasteisiin, jotka ovat tarkoin määritelty ja rajattu. Kolmannessa vaiheessa käsitellään monimutkaista ongelmanratkaisua tai päätöksentekoa, josta koneen tulee selviytyä tai olla osa monimutkaista kokonaisuutta. Tulevaisuudessa kuvatun kolmannen vaiheen kaltaiset, ihmisen ja koneen välisen yhteistyön ymmärtäminen ja hyödyntäminen, tulevat olemaan ratkaisevia kilpailuetuja (Merilehto, 2018, s. 41-43).

Syväoppiminen (deep learning) termi on saanut nimensä siitä, että neuroverkoissa käytetään monia piilokerroksia, joilla kullakin on oma tehtävänsä. Syvät neuroverkot ovat piirteenmuodostukseen kykeneviä monikerroksisia

neuroverkkoja. Syväoppimisen haasteena on opettamiseen tarvittavan datan määrä. Syvissä neuroverkoissa voi olla miljoonia neuroneita ja siten miljoonia muutettavia parametreja, opetusdataa tarvitaan valtavasti. Mikäli dataa on liian vähän, verkot ylioppivat helposti, eivätkä tulokset yleisty uusiin ennalta tuntemattomiin havaintoihin (Tuominen ym., 2019, s. 6). Merilehdon mukaan syväoppiminen on osa koneoppimista ja sen uudempi osa-alue, jonka tarkoituksena on optimoida syviä neuroverkkoja monimutkaisten ongelmien ratkaisemiseksi. Yksi syväoppimisen ja neuroverkkojen kyky tällä hetkellä on muuntaa puhetta tekstiksi tai valokuva tunnetun maalarin tyylin mukaiseksi tauluksi (Merilehto, 2018, s. 20, s. 46). Syväoppimista on hyödynnetty esimerkiksi kuvien, videoiden, puheen ja äänen käsittelyssä. Sen avulla on tehty läpimurtoja ja se onkin yksi vahva suuntaus ja iso osa arkea tulevaisuudessa (Hyacinth, 2017, s. 18).

Neuroverkot (artificial neural network) ovat informaation käsittelyn, matematiikan tai laskennan malleja, jotka perustuvat yhdistävään laskentaan. Ihmisen aivojen toimintaa jäljittelevät keinotekoiset neuroverkot keksittiin jo 1940-luvulla. Neuroverkkojen uusi aalto alkoi 1990-luvulla mutta niiden käyttöinto hiipui nopeasti siihen, että ne eivät olleet muita menetelmiä parempia ja silloisilla tietokoneilla ei ollut mahdollisuutta käsitellä neuroverkkojen koulutuksessa tarvittavia suuria datamääriä. 2010-luvulla koneiden kehittyminen ja datan määrän valtava kasvaminen ovat kasvattaneet innostusta syväoppimiseen. Neuroverkkoja käytetään esimerkiksi kuvantunnistuksessa, konenäössä, puheentunnistuksessa, kieltenkääntäjissä, peleissä ja lääketieteellisissä diagnooseissa. Neuroverkko koostuu syöte- ja ulostulokerroksesta ja niiden välissä olevista piilokerroksista (kuvio 5), jotka koostuvat neuroneista (Tuominen ym., 2019, s. 6-7).

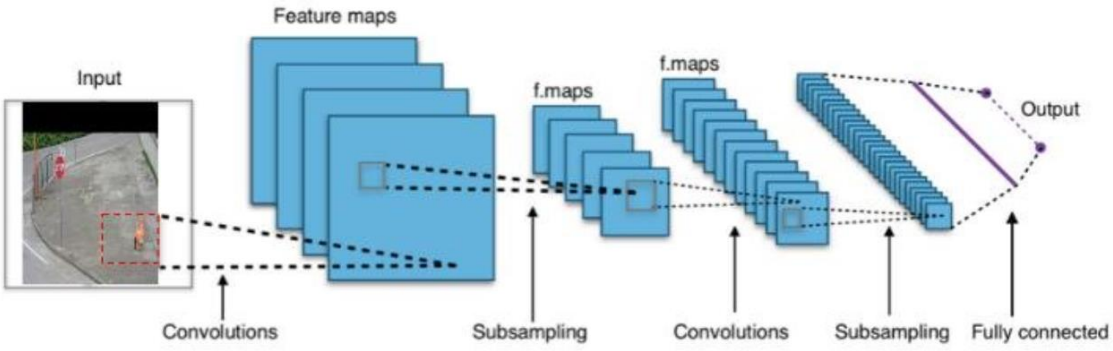


KUVIO 5 Neuroverkkojen perusrakenne (Digital Trends, 2019)

4.2.2 Tekoälyn yksinkertaistettu toimintaperiaate kuvankäsittelyssä

Kameravalvonnassa tekoälyn keinoin pyritään kuvista prosessoimaan laaja määrä yksittäisiä pikseleitä. Tietokoneiden näytönohjainten tehokkuuden kehittyessä niiden kyky käsitellä yksittäisiä pikseleitä on kasvanut niin hurjasti, että reaaliaikaisesti voidaan prosessoida jopa kuvia ja videovirtaa. Lisäksi tietokannat, joiden avulla tekoälyalgoritmeja voidaan opettaa, ovat suurentuneet ja tulleet kaikkien saataville. Tyypillisiä tekoälyalgoritmeja on saatavilla ilmaiseksi ja niiden opettaminen on kohtuullisen yksinkertaista. Esimerkiksi ImageNet tietokantaan on kategorioituna 1000 erilaista mallia, joita tyypillisesti hyödynnetään kuvan-, objektin- tai toiminnantunnistuksessa (Hollywood, Vermeer, Woods, Goodison & Jackson, 2018, s. 5).

Kuvan mallinnuksessa ensimmäisenä kuvasta tai videosta prosessoidaan keskenään päällekkäiset pikselitiilet. Ensiksi näistä pyritään löytämään keskenään samanlaiset tiilet, jotta analysoitavien tiilien määrä olisi mahdollisimman vähäinen. Sen jälkeen näistä pyritään tunnistamaan tyypilliset attribuutit, esimerkiksi neliöt tai viivat. Alemman tason mallit johdetaan kerroksittain ylemmäs, kunnes tiilistä voidaan päätellä objekteja kuten pää, kasvot, ihminen tai auto. Tällä tavoin kuvatunnistuksesta voidaan erotella erilaisia attribuutteja ja niille voidaan antaa yksittäisiä laskennallisia arvoja. Näiden arvojen perusteella videodata muokataan haettavaksi ja sieltä voidaan suodattaa yksittäisiä laskennallisten arvojen perusteella, esimerkiksi kaikki henkilöauton arvon saaneet objektit. Koneoppiminen mahdollistaa useiden erilaisten neuroverkkojen hyödyntämisen samanaikaisesti siten, että niiden toimintaperiaate lomittuu tuottamaan tekoälylle opetettua tehtävää. Alla olevassa kuvassa (kuvio 6) on visualisoituna neuroverkon toimintaperiaate siitä, miten yksittäisistä kuvassa havaituista pikselitiilien attribuuteista voidaan johtaa päätelmä, että kuvassa on tulipalo (Hollywood ym., 2018, s. 5).



KUVIO 6 Tyypillinen konvoluutioneuroverkon toimintaperiaate (Researchgate, 2019)

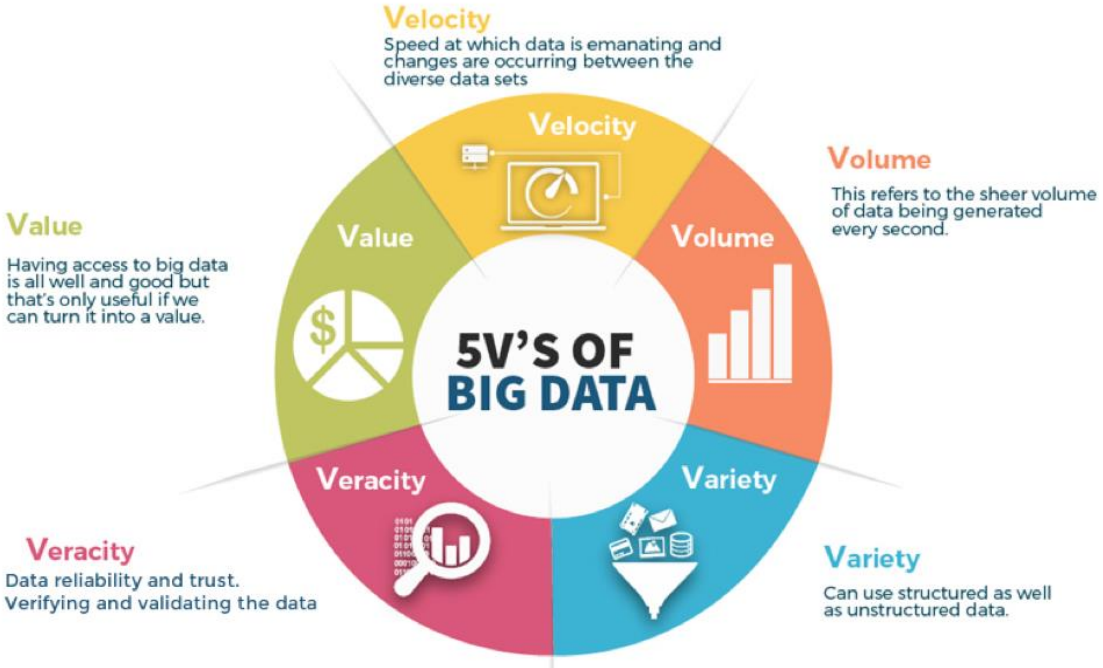
4.2.3 Big data - massadata

Nimensä mukaisesti Big datalla tarkoitetaan massiivisten, jatkuvasti kasvavien, strukturoitua ja strukturoimatonta tietoa, kuvia, äänitteitä ja videoita sisältävien

tietojoukkojen keräämistä, säilyttämistä ja tiedon käyttämistä. Tällaisten datamäärien hallitseminen ja tiedon analysoiminen ovat perinteisillä tietokantatyökaluilla joko mahdotonta tai erittäin vaikeaa. Big datalle tyypillisiä tunnusmerkkejä (kuvio 7) ovat:

1. Määrä (volume) – luodun ja varastoidun datan määrä on niin suurta, että sitä on mahdoton käsitellä perinteisin menetelmin.
2. Valikoima (variety) – datan tyyppi, laatu ja alkuperä vaihtelevat suuresti. Dataa tulee monista lähteistä, se koostuu erilaisista osista, eikä se ole jäsenneltyä.
3. Nopeus (velocity) – datan tuottonopeus, analysointi ja käsittely on nopeaa.
4. Arvo (value) – data ja siitä saatava tieto on yrityksille hyödyllistä.
5. Todenmukaisuus (veracity) – datan laatu ja luotettavuus ovat tärkeitä.

Dataa kasvaa ja syntyy nykyisin monesta eri lähteestä, kuten esimerkiksi internetsivujen ja sosiaalisen median käyttötiedot, sää- ja navigointidatasta, terveydenhuollon tiedoista ja IoT-laitteiden (Internet of Things) toimintatiedoista (Tuominen ym., 2019, s. 5).



KUVIO 7 Big datan 5V-tunnusmerkistö (Techentice, 2019)

4.3 Ihmisen heikkoudet videovalvonnassa

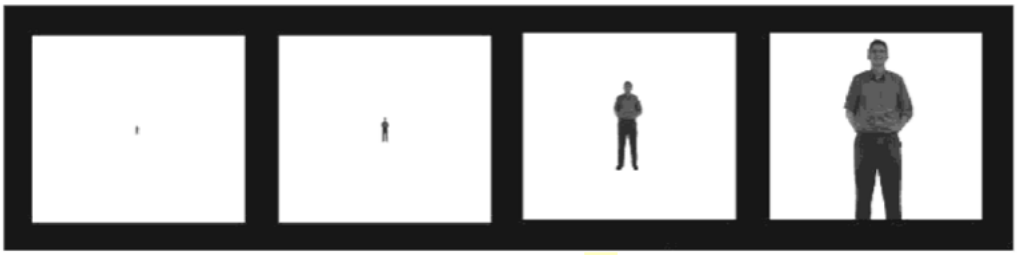
Kamerateknologian edullisuus, niiden käytettävyys ja IP-kameroiden myötä videovirran jakaminen jopa langattomasti, on luonut tilanteen, jossa videovirtaa voidaan käsitellä lähes rajattomasta määrästä lähteitä. Ihmisen kyvyt käsitellä

materiaalia ovat kuitenkin äärimmäisen rajalliset (kuvio 8). Operatiivisissa tilanteissa on huomattu, että yksittäinen ihminen pystyy samanaikaisesti hyödyntämään maksimissaan noin kymmenen videolähteen tietoa. Näidenkin osalta käsittely on hyvin pinnallista (Hollywood ym., 2018, s. 4). Mikäli kuvanauhalta pitää pystyä tunnistamaan kohde varmuudella ihmisen kykenee tarkkailemaan vain yhtä kuvavirtaa kerralla (Pikaar, Knongsveld & Settels, 2007, s. 286).

Monitor numbers	Accuracy scores (%)
1	85
4	74
6	58
9	53

KUVIO 8 Monitoreiden määrän vaikutus tunnistusprosenttiin (Pikaar, ym., 2007, s. 286)

Kameravalvontaa käytetään moneen tehtävään, kuten henkilöllisyyden tunnistamiseen tai poikkeavan toiminnan havaitsemiseen. Ihmisen kykyyn tehdä kameradatasta päätelmiä, vaikuttaa muutkin seikat kuin ruutujen määrä. Riippuen suoritettavasta tehtävästä tunnistettavan objektin koko videopäätteellä vaikuttaa (kuvio 9) merkittävästi ihmiseen kykyyn tehdä havaintoja (Pikaar ym., 2007, s. 286).



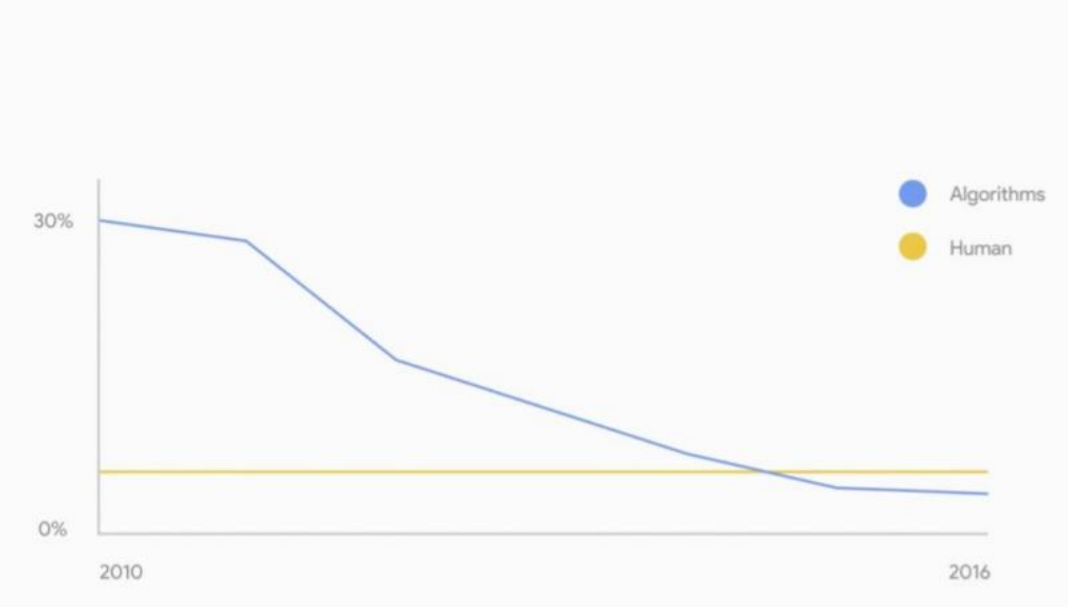
KUVIO 9 Objektin koon vaikutus tunnistusprosenttiin (Pikaar ym., 2007, s. 286)

Yllä olevan kuvan perusteella voidaan havainnoida ruudulla olevan objektin koon merkitys ihmisen kykyyn tehdä tunnistus. Henkilön identifioiminen varmuudella onkin kohtuullisen hankalaa, jopa hyvin läheltä kuvaavasta kamerasta (Pikaar ym., 2007, s. 286). Kaupunkien yleisvalvontaan tarkoitetut kamerat ovat lähtökohtaisesti sijoitettu ylös, jotta niillä voidaan valoa suuria alueita kerralla. Näin kuva-alassa objektit ovat hyvin pieniä ja niitä on vielä lukumääräisesti paljon. Tämä tekee ihmiselle kameravalvonnan suorittamisesta hyvin työlään prosessin.

Ihmisen kyky pysyä tarkkaavaisena paljon keskittymistä vaativassa tehtävässä on hyvin rajallinen. Lisäksi tähän vaikuttavat paljon henkilön yksilölliset ominaisuudet ja koulutus. Mikäli videovirrasta pitää pystyä löytämään kohdehenkilö, yhtäjaksoinen valvontatyöskentely ei saisi kestää yli kolmea tuntia. Tämän jälkeen henkilön kyky tehdä oikeita päätelmiä laskee merkittävästi. Lisäksi ihmisen tekemä työmäärä vaikuttaa toimintaan kumulatiivisesti, jolloin yhden päivän aikana ihmisen kykenee tehokkaasti suorittamaa valvontaa vain kuuden tunnin ajan. Järkevää olisi, että valvonta jaettaisiin 20 minuutin osiin, joiden välissä olisi 5 minuutin tauko (Pikaar ym., 2007, s. 284-285).

Teknologinen kehitys on edennyt siihen pisteeseen, että yksittäisillä asioilla tekniikan keinoin pystytään päihittämään ihmisen kyvyt lähes kaikilla elämän osa-alueilla. Oli kyse sitten shakista, pörssien tulkinnasta tai videoprosessoinnista. Kameravalvonnan osalta oikeastaan ainut seikka, missä tekoälyllä on vielä heikkouksia, on toiminnan tulkinnassa. Ihminen kykenee paremmin tekemään tulkintoja tapahtumista. Tekoälyä kuitenkin ollaan jatkuvasti kehittämässä juuri tällä osa-alueella. Tekoälylle tulkinta on vaikeaa, koska toiminnan analysointi vaatii attribuuttien tunnistamisen lisäksi niin avaruudellista kuin aikaan liittyvää hahmotusta (Cheng, Lubamba, Rabia & Maozhen, 2020, s. 307). Esimerkiksi tekoälyn on helppo tunnistaa henkilön juoksevan, mutta sen on vaikea ymmärtää, minkä vuoksi henkilö juoksee. Ihminen pystyy videolta ymmärtämään juoksun tarkoituksen olevan se, että lähellä oleva bussi on lähdössä, mutta tekoäly on vielä toistaiseksi vaikea linkittää tapahtumia yhteen.

Tekoäly on väsymätön työntekijä, joka pystyy prosessoimaan videovirrasta jokaisen tunnistamansa objektin ja säilömään sen sellaisenaan haettavaan muotoon (kuvio 10). Tarpeen vaatiessa kone voidaan laittaa prosessoimaan taltioitua tietoa ja tuottamaan siitä esimerkiksi kuvavertailua, hälytyksiä tai dataanalyyseja. Pilvilaskennan aikaudella järjestelmään liitettyjen kameroiden määrällä ei periaatteessa ole merkitystä, sillä laskentaan käytettäviä näytönohjaimia voidaan skaalata käytön ja tarpeen mukaan.



KUVIO 10 Ihmisen ja tekoälyn erot kuvantunnistuksessa (Brynjolfsson, Rock & Syverson, 2017, s. 3)

4.4 Kameravalvonnassa hyödynnettävät tekoälymahdollisuudet

Tekoäly on noussut osaksi päivittäistä keskustelua ja elämäämme. Sitä pidetään uutena teknologiana, joka mullistaa maailman. Tekoälyyn panostetaan runsaasti sekä teollisuudessa että tutkimuksessa. Yhdysvaltoja ja Kiinaa pidetään tekoälyn edelläkävijöinä, mutta kilpajuoksu on täydessä vauhdissa useiden eri valtioiden kesken. Valtavaan kasvuun ja lisääntyneeseen käyttöön sisältyy myös huolestumista. Tekoälyn pelätään vievän runsaasti työpaikkoja. Lisäksi sen uskotaan tulevan lähivuosikymmeninä ihmistä älykkäämmäksi supertekoälyksi ja ottavan vallan ihmisiltä (Pietikäinen & Silvén, 2019, s. 1).

Suomessa elinkeinoministeri Mika Lintilä käynnisti tekoälyohjelman vuonna 2017. Ohjelman myötä asetettiin työryhmä pohtimaan tekoälyn soveltamisen tulevaisuutta. Samalla tekoäly nostettiin hallituksen kärkihankkeeksi, jonka tarkoituksena oli johdattaa Suomi tekoälyä soveltavien maiden kärkijoukkoon (Työ- ja elinkeinoministeriö, 2017). Tekoälyohjelman loppuraportin mukaan tekoälyn käyttöönottoon ja hyödyntämiseen sisältyy valtavasti potentiaalia ja muutosvoimaa. Tekoäly voi auttaa ratkaisemaan globaaleja ongelmia, siivittämään talouskasvua samalla kun se luo uusia eettisiä haasteita yhteiskunnan eri tasoilla. Potentiaalin toteutuminen ja mahdollisten riskien minimointi on kiinni meidän omista toimistamme ja valinnoistamme (Työ- ja elinkeinoministeriö, 2019, s. 9). Nykyhallitus pääministeri Sanna Marinin johdolla on asettanut hallitusohjelmaan strategisen tavoitteen elinvoimaisesta Suomesta. Tavoitteen myötä on luotu vuoteen 2022 saakka kansallinen AuroraAI-tekoälyohjelma, jonka tavoitteena on tehdä arjesta ja liiketoiminnasta sujuvampaa tietoturvallisesti ja eettisesti kestävällä tavalla. Ohjelma on asetettu aikaisemman tekoälyohjelman loppuraportin suositusten mukaisesti. Suomi halu-

taan tuntea teknologisen kehityksen, innovatiivisten hankintojen ja kokeilukulttuurin edelläkävijänä, jossa digitalisaation ja teknologisen kehityksen luomia mahdollisuuksia kehitetään ja otetaan käyttöön yli hallinto- ja toimialarajojen (Valtiovarainministeriö, 2019). Poliittinen paine ja digitalisaation hurja vauhti on saanut niin viranomaiset kuin yrityksetkin ottamaan tarvittavia askelia tekoälyn hyödyntämisessä. Tekoäly eteneekin monella rintamalla. Tekoälyä käytetään asiantuntijoiden ja työntekijöiden työnteon helpottamiseen sekä tukemaan päätöksentekoa. Ratkaisut pohjautuvat pitkälti vielä saadun datan analysointiin ja sääntöpohjaisesti luotuihin ohjelmistoihin. Viranomaiset hyödyntävät palveluita mm. erilaisten tilannekuvien laadukkaammassa muodostamisessa tai isojen datamassojen analysoinnissa, on sitten kyseessä ennakoivien anomalioiden tunnistaminen ja tietoturvaloukkausten selvittäminen tai uusien tietolähteiden käyttäminen ja tietoaineiston tarkastaminen, validointi sekä käsittely (Valtioneuvosto, 2019, s. 26). Kansallisen tekoälyohjelman myötä tehdyn tutkimuksen mukaan suurin osa suomalaisista luottaa, että tekoäly parantaa elämää tulevaisuudessa. Ihmiset kokevat tekoälyn voittopuolisesti hyödyllisenä mutta vastaavasti optimismin rinnalla on nähty pessimistisiä näkemyksiä työn tulevaisuudesta ja yhteiskunnallisten erojen kehityksestä. Suomea koskevan raportin mukaan tekoäly tuhoaa n. 15 % työpaikoista vuoteen 2030 mennessä ja muuttaa työn luonnetta huomattavasti tätä suuremmassa osassa tehtäviä. Vastaavasti tekoälyn edistyksellinen soveltaminen mahdollistaa monia kokonaan uusia tuotteita ja ammatteja (Työ- ja elinkeinoministeriö, 2018, s. 10).

Tekoälyn käyttöönottoa on perusteltu myös yhteiskunnan toimivuudella tai edulla ja turvallisuuden takaamisella. Rajavartiolaitoksella on esimerkiksi valtakunnallisesti automaattisia kasvojentunnistusjärjestelmiä, joilla tarkastetaan ihmisten henkilöllisyys Suomen Schengen-rajoilla sekä satamissa ja lentokentillä. Tämän lisäksi rajaturvallisuuden valvonnassa hyödynnetään hahmontunnistusta lennokki- ja dronejärjestelmillä, joilla kuvataan ja reagoidaan aiheutuviin hälytyksiin (Erillisverkot, 2019). Finavia on myös testannut lentoasemilla konenäköä biometristen kasvojen tunnistuksessa. Ajatuksena, että tarkastuksista voisi tulevaisuudessa päästä lävitse ilman matkustusasiakirjoja. Kehitystyö vaatii kuitenkin aikaa, koska asiaan liittyy paljon säännöksiä ja lainsäädäntöä (Finavia, 2019). Myös poliisilla on jo käytössään tekoälyratkaisuja kuten Revika-järjestelmä, rekisterinkilvenlukuun käytettävä konenäköä hyödyntävä järjestelmä. Miehittämättömien tukiyksiköiden hyödyntäminen hahmontunnistuksen avulla yhteistoiminnassa poliisin kenttätoiminnan kanssa on yksi poliisin tulevaisuuden mahdollisuuksista (Poliisihallitus, 2019, s. 117). Poliisilla on myös tulevaisuudessa tahtotilana tunnistaa reaaliaikaisesti kasvojentunnistuksen avulla etsintäkuulutettuja tai maahantulokiellossa olevia henkilöitä satamissa ja Schengen-rajoilla niin, että kaikki matkustajat kuvataan ja kuvien biometriset tunnisteet säilytetään kuukauden ajan. Kasvojentunnistusteknologiaan sisältyy rikostorjunnan hyötyjen lisäksi myös suuria riskejä, sillä sitä voidaan käyttää yksityisyyttä loukkaaviin tai muutoin vahingollisiin tarkoituksiin kuten vakoiluun. Median haastattelemana apulaistietosuojavaltuutettu Jari Råmanin mukaan reaaliaikaisesta kasvojentunnistusteknologiasta julkisilla paikoilla on

helppo maalailla synkkiä uhkakuvia, eri asia on kuitenkin kuinka todellisia ne ovat (Helsingin sanomat, 2019).

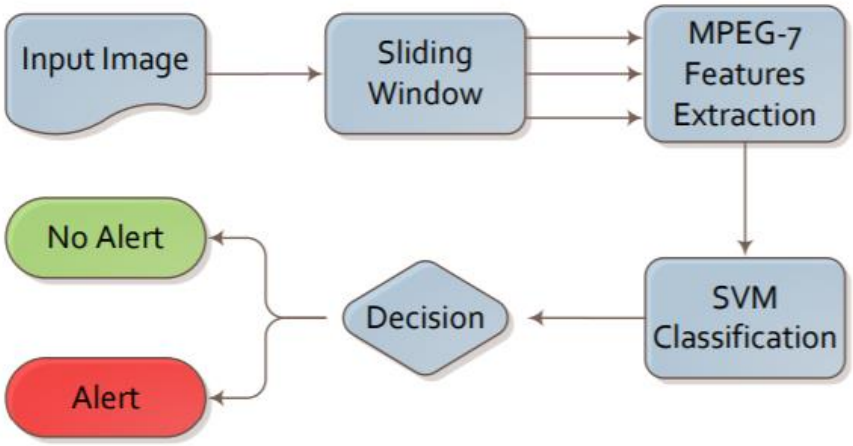
Kameravalvonnassa hyödynnettävien tekoälypohjaisten sovellusten käyttö on kasvanut räjähdysmäisesti viimeisten vuosien aikana. Kaksi maailman isointa kameravalvontajärjestelmä toimittajaa ovat ruotsalainen Milestone ja kanadalainen Genetec (IfSecGlobal, 2019). Milestone kameravalvontajärjestelmän 2019 avatusta kauppapaikasta on löydettävissä jo 229 Milestoneen integroitavaa erilaista kameravalvontaan liittyvää ohjelmistoa. Näistä ihmisen tunnistamiseen tarkoitettuja sovelluksia on 41 kappaletta. Ohjelmistot tarjoavat yleisesti ratkaisuja yksittäisiin käyttökohteisiin kuten, kasvojentunnistukseen, hahmontunnistukseen, väenlaskentaan tai tietyn toiminnan tunnistamiseen kuten norkoilun havaitsemiseen. Kokonaisvaltaisia kaikkeen kykeneviä ohjelmistoja ei vielä ole kunnolla markkinoilla, vaan yritykset keskittyvät täyttämään vain tietyn asiakkaalta tulevan tarpeen (Milestone, 2020). Osaltaan tätä selittää se, että kilpailu alalla on kovaa sekä uusien järjestelmien luominen ja tekoälyohjelmointi vaativat paljon resursseja.

4.4.1 Analytiikasta biometriikkaan

Kameravalvontajärjestelmän analytiikkakykyjä käytetään yleisesti hahmontunnistuksessa. Tällöin videokuvasta tunnistetaan erilaisia objekteja ja niitä voidaan taltioida laskennallisiksi malleiksi. Lisäksi näitä matemaattisia malleja voidaan vertailla keskenään, esimerkiksi onko kuvassa oleva henkilö tallentunut johonkin muuhun valvontakameraan. Lisäksi järjestelmään voidaan tuoda ulkopuolelta kuvia tai videota, jota voidaan muuttaa järjestelmän algoritmilla samanlaisiksi laskennallisiksi malleiksi. Ihmisen luomien algoritmien avulla voidaan luoda hyvinkin tarkkoja määritelmiä halutuista arvoista, joita tekoälyllä avustettu järjestelmä hakee tietokannastaan tai saamastaan datasta ja vertailee niitä samankaltaisuuksien perusteella. Tyypillisiä arvoja voivat olla esimerkiksi muoto, koko tai väri. Nämä voivat kuitenkin olla huonoja arvoja, koska esimerkiksi väri voi muuttua valonheijasteiden tai määriteltyjen väriarvojen mukaisesti riippuen kameroista, keliolosuhteista, vuoden- tai kellonajasta. (Grega, Matiolanski, Guzik & Leszczuk, 2016, s. 4-5)

Analysoitua hahmontunnistusta voidaan käyttää monenlaisiin tarpeisiin. Viimeaikaisten tutkimusten myötä tekoälyä on pyritty tunnistamaan esimerkiksi vaarallisia esineitä, kuten veitsi tai ase (kuvio 11). Isoista massoista dataa voi olla vaikeaa ja hidasta etsiä yhtä tiettyä hahmoa, jolloin algoritmin pitää olla tarkkaan määritetty mistä ja miten etsiä. Algoritmin luomisessa voidaan hyödyntää tunnistettuja standardeja luotettavuuden lisäämiseksi. Veistä tai asetta voidaan etsiä määrittelemällä hahmolle arvoja kuten esimerkiksi tyypilliset kulmat, suunnat, materiaali, karkeudet, kuvioiden homogeenisyys ja muita tarkkaan määriteltyjä arvoja. Näiden avulla lisätään todennäköisyyttä tunnistukselle. Algoritmiin voidaan lisätä myös muita tunnisteita, joilla nopeutetaan ja nostetaan tunnistamisen varmuutta. Tällaisia arvoja voivat olla esimerkiksi puukon tai aseen pitäminen kädessä. Ihmisen käden ja veitsen määritellyt arvot

tai palasia niiden arvoista yhdistetään, jotta tekoälyn on mahdollista tehdä tulkinta vaarallisesta toiminnasta. Tämä lisää entisestään tunnistuksen varmuutta, auttaa päätöksenteossa sekä parantaa todenmukaisten hälytysten välittämisessä. (Grega ym., 2016, s. 4-5)



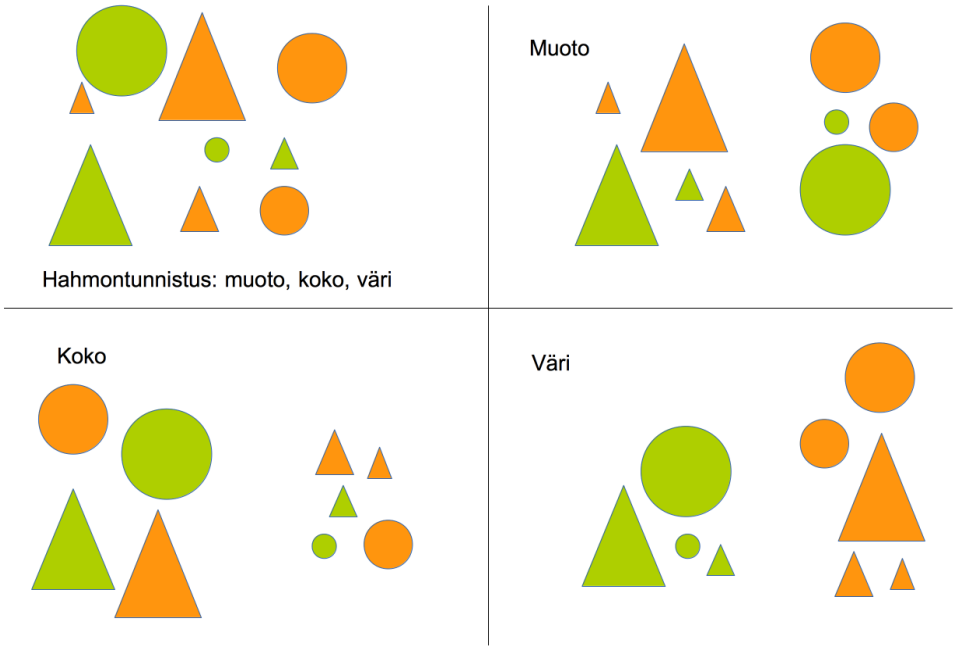
KUVIO 11 Veitsen tai aseen tunnistamisen algoritmi (Grega, Matiolanski, Guzik & Leszczuk, 2015, 5)

Hahmoja voidaan hakea datasta useilla erilaisilla arvoilla tai tunnisteilla (kuvio 12), jotta haluttu toimenpide saadaan aikaan. Tunnisteita voidaan luoda esimerkiksi henkilöille tai hahmoille, joilla on useita erilaisia ominaisuuksia. Hahmoille tai henkilöille voidaan antaa väliaikainen numeerinen tai jokin muu yksilöity arvo. Yleisesti tällaisista arvoista puhutaan laskennallisena mallina. Ongelmalliseksi tilanteen kameravalvontajärjestelmän näkökulmasta tekevät biometriset tiedot, joita ei lähtökohtaisesti saisi edes käsitellä kameravalvontajärjestelmissä, pois luettuna tämän tutkimuksen 2.1.2 kappaleen kaltaisissa käyttötapauksissa. Hahmolle tai ihmiselle tekoälyn avulla määritellyt arvot, tunnisteet tai tiedon indeksointi voivat muuttaa henkilötietojen luokittelua ja muodostua erityisiksi henkilötiedoiksi. Tämän vuoksi onkin erityisen tärkeätä jo järjestelmän suunnitteluvaiheessa tehdä perusteellinen tietosuojaseloste, jossa määritetään henkilötietojen käsittelyn käyttöperusteet ja arvioidaan niistä muodostuvia riskejä. Käyttöperustetta ei voi muuttua, eikä näin ollen henkilötietojen luokittelukaan voi tahattomasti, suoraan, johdettuna tai muutoin elinkaarensa aikana muuttaa. Rekisterinpitäjä viime kädessä on vastuussa järjestelmän laillisuudesta ja vaatimustenmukaisuudesta. Väärin perustein kerättyjen henkilötietojen keräämisestä rekisterinpitäjä voi syyllistyä tietosuojarikokseen (Oikeusministeriö, 2018).

4.4.2 Hahmontunnistus

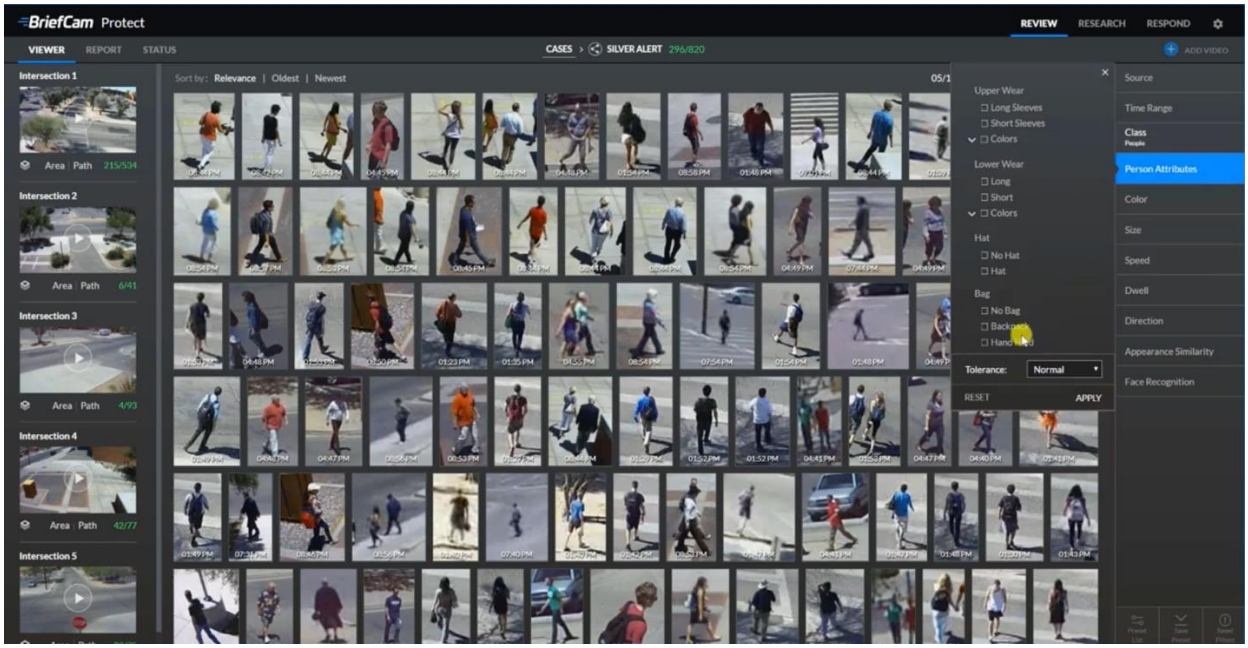
Hahmontunnistus (pattern recognition) on koneoppimisen osa-alue, jonka avulla datasta voidaan kehittää malleja tai kaavoja tunnistavia järjestelmiä. Hah-

montunnistusmenetelmät voidaan jakaa kolmeen luokkaan: tilastollinen hahmontunnistus, syntaktinen hahmontunnistus ja neuraalinen hahmontunnistus. Tilastollisessa hahmontunnistuksessa oletetaan, että etsittävällä hahmolla on tilastollinen jakauma kussakin luokassa, joihin kyseisen piirteen avulla halutaan luokitella. Syntaktisessa hahmontunnistuksessa vastaavasti oletetaan, että on olemassa jokin rakenne, jonka perusteella luokittelu voidaan tehdä. Neuraalinen hahmontunnistus taas on epälineaarinen regressiomalli, joka osaa itsenäisesti kaivaa datasta olennaiset piirteet ja muodostaa näiden välille monimutkaisia riippuvuussuhteita (Tuominen ym., 2019, s. 9-10).



KUVIO 12 Hahmontunnistus: muoto, koko, väri (Tuominen ym., 2019, s. 10)

Milestonen kauppapaikasta nähtävillä olevat, hahmontunnistukseen käytettävät sovellukset, ovat pitkälti useamman koneoppimisen osa-alueen symbiooseja, Esimerkiksi BriefCam ohjelmiston (kuvio 13) avulla kuva-alasta ohikulkevat henkilöt jaetaan hakukelpoisiksi tiettyjen attribuuttien avulla. Nämä attribuutit ovat jaettuna erilaisiin hakuparametreihin, joiden avulla voidaan tuloksia supistaa. Videovirrasta tuotetaan hakukelpoista materiaalia ja jokaiselle kuvasta tunnistetulle objektille määritetään omat attribuutit. Näin videodatasta voi hakea mm. henkilön vaatteiden, objektin värin, sukupuolen, ajan ja paikan sekä objektin kategorian mukaan tuloksia. Esimerkiksi tietyn aikaikkunan sisältä pyritään luetteloimaan kaikki punapukuiset mieslenkkeilijät tai keltaiset rekka-autot, jotka kulkivat kameran kuvaussuunnasta katseltuna ylhäältä alas. Ohjelmiston avulla voidaan myös hakea tietyllä alueella pidempiaikaisesti oleskelleita ihmisiä tai valikoida vain ne ihmiset ketkä ovat menneet sisälle tiettyyn asuntoon (Milestone Marketplace, 2020).



KUVIO 13 BriefCam ohjelmiston suodatusmahdollisuuden kuvakaappaus (Milestone Marketplace 2020)

Sovelluksen avulla voidaan myös luoda ns. videosynapseja, joissa attribuuttien mukaan valikoidut objektit koostetaan kerroksiin videon päälle. Näin voidaan esimerkiksi tunnin videotallenne tiivistää pariin minuuttiin, jossa kaikki punapukuiset lenkkeilijät näkyvät. Hakutoimintojen ja videosynapsin avulla videon käsittelyyn käytettävää aikaa voidaan huomattavasti vähentää (Milestone Marketplace, 2020).

Ohjelmiston avulla videoita voidaan käsitellä takautuvasti syöttämällä siihen videodataa useasta eri lähteestä. Lisäksi reaaliaikaista videovirtaa voi indeksoida. Ohjelmiston tuottaa henkilöistä yksilöiviä tunnisteita ja näitä tunnisteita voidaan hakea kaikista järjestelmään liitetyistä kameroista. Lisäksi takautuvasti voidaan materiaalia syöttää periaatteessa rajaton määrä. Hakutoiminnot tapahtuvat nopeasti, koska tekoälyllä tuotettu haettava matemaattinen arvo on pieni (Milestone Marketplace, 2020). Ohjelmiston tekoälyalgoritmeista ei ole saatavissa julkisia tietoja, koska ne ovat liikesalaisuuksia. Edellä kuvatuissa tilanteissa yksilöstä ei kuitenkaan luoda erityisiä henkilötietoja. Tallennetut attribuutit eivät identifioi yksilöivästi henkilön fysiologisia piirteitä, kuten kasvokuvia tai kävelytyyliä. Vaikka henkilön liikkeet ovatkin selvitettävissä hyvinkin laajalti, vaihtamalla vaatetusta henkilö pitää uudelleen etsiä datasta (EDPB 3/2019, s. 13-14).

Ohjelmistossa on kuitenkin mahdollisuus hakea kasvokuvaa apuna käyttäen henkilöitä videomateriaalista. Järjestelmään syötetään vertailukuva, jota haetaan järjestelmään tallennetusta materiaalista. Ominaisuuden myötä ohjelmistoon luodaan biometrisia tietoja ja lisäksi ohjelmisto luo kaikesta videomateriaalilla liikkuvista henkilöistä biometrisiä hakuparametreja. Lisäksi ohjelmistossa voidaan materiaalista valikoida tietty henkilö ja hakea tätä vastaavia hen-

kilöitä (Milestone Marketplace, 2020). Kyseisen ominaisuuden myötä pitäisi tarkkaan selvittää mihin tietoon pohjautuen hakualgoritmi toimii. Hakeeko ohjelmisto esimerkiksi samoihin vaatteisiin pukeutuneita vai hyödynnetäänkö haussa jollain tapaa henkilön biometrisia ominaisuuksia, jotka ovat tätä henkilöä yksilöiviä? Otettaessa käyttöön BriefCam-ohjelman kaltaisia tekoälysovelluksia, tulee huomioida, että rekisteröityjen henkilötietoihin käytetään uudenlaista teknologiaa. Tietosuoja-asetuksen (2016/679) mukaisesti asiasta tarvitsee luoda vaikutustenarviointi (ks. 2.1.5) ja konsultoida tietosuojavaltuutettua.

4.4.3 Tapaus Amsterdamin lentokenttä

Schipholin lentokentällä Amsterdamissa on testattu kasvojentunnistusohjelmaa vuodesta 2019 lähtien. Järjestelmän tarkoituksena on tehostaa lentoliikenteen sujuvuutta siten, että henkilö voi käyttää kasvojaan lentäessään tietyn lentoyhtiön koneilla. Järjestelmä vaatii toimiakseen vapaaehtoisen rekisteröitymisen, joka tehdään lentokentällä erityisessä kasvojentunnistuskioskissa. Henkilön kasvojen kuvaa verrattaan laitteeseen syötettyyn passiin. Tapahtumasta tallennetaan järjestelmään biometrinen profiili, jota verrataan lennon yhteydessä tarkastuskortissa oleviin tietoihin ja valvontakameran tunnistukseen. Kasvojentunnistus suoritetaan erikseen kasvojentunnistukseen merkityllä portilla, niin turvatarkastuksen jälkeisessä passintarkastuspisteessä kuin portilla noustessa lentokoneeseen. Oman kasvokuvan hyödyntäminen laillisuusperuste pohjautuu vapaaehtoisuuteen ja osallistujan tulee olla vähintään 16-vuotias (Schiphol, 2019).

Järjestelmään tallentuu näkyvä vertailukuva ja tästä kuvasta tehdään kasvojen biometrinen malli, joka tallennetaan kuvan yhteyteen. Tätä mallia verrataan aina henkilöstä otettuihin kuviin ja niistä luotuihin biometrisiin tallenteisiin, niin lähtöselvityksessä kuin portilla. Tietosuojaselosteessa mukaan kuvia säilytetään vain niin kauan kuin se on tehtävän suorittamiseksi tarpeellista ja enintään 24 tuntia rekisteröitymisestä. Tämän jälkeen kaikki tiedot henkilöstä hävitetään. Henkilö voi myös lopettaa vapaaehtoisuutensa, milloin haluaa, jolloin kaikki hänestä kerätty data hävitetään välittömästi. Selosteessa on myös maininta, että tietoja voidaan luovuttaa myös kolmansille tahoille, mutta näiden tahojen on tarvinnut tehdä tietojenluovutussopimus rekisterinpitäjän kanssa. Tällaisia tahoja ovat ilmeisesti ainoastaan yritys, joka on toteuttanut kasvojentunnistusjärjestelmän. Erikseen on mainittu, että tietoja ei luovuteta sellaisille tahoille, joille tietojenluovutussopimusta ei ole tehty, ellei kyseessä ole sellainen taho, jolla on laillinen oikeus kysyä tietoa. Yhtenä tahona on mainittu Royal Netherlands Marechaussee, mikä on yksi Hollannin armeijan haara (Schiphol, 2019). Yhdysvalloissa yli 30 eri lentokentällä suoritetaan samankaltaista kasvojentunnista, jonka on todettu nopeuttavan merkittävästi etenkin paljon matkustavien henkilöiden aikaa (CNN, 2019).

4.4.4 Konenäköpohjainen henkilölaskenta

Konenäöllä (machine vision) pyritään jäljittelemään ihmisnäköä tai laajentamaan sen mahdollisuuksia. Konenäköä hyödyntävä järjestelmä koostuu valonlähteestä, kohteesta, kamerasta, tietokoneesta ja siinä olevasta kuvankäsittelyohjelmasta, joka tulkitsee kuvan automaattisesti. Konenäkö on tarkka, nopea ja väsymätön rutiinitehtävien suorittaja. Konenäkö yhdistettynä hahmontunnistukseen, voidaan saada hyödyllisiä ja merkittävää lisäarvoa tuottavia sovelluksia aikaan hyödyntämällä digitaalista kuvankäsittelyä ja kuva-analyysiä (Tuominen ym., 2019, s. 9).

Data-analyysia on tehty niin kauan, kun tietoa on kerätty. Yleisin data-analyysin muoto on tilastointi. Kameravalvonnassa käytettävien tekoälysovellusten avulla saadaan tietystä kameran kuva-alasta laskettua automaattisesti alueella liikkuvien ihmisten määrä. Osa ohjelmista toteuttaa analyysin videolta tallennetun yksittäisen kuvan kautta, mutta kehittyneemmät ohjelmat laskevat sitä suoraan reaaliaikaisesta videovirrasta. Ohjelmistot kuten, Up Xtreme Smart Surveilance (kuvio 14) tuottavat videovirrasta erilaista henkilölaskentaa, tietyn kohdan tai kameran koko kuvanalan kautta. Lisäksi ohjelmistosta voidaan laatia lämpökarttoja, joiden avulla visuaalisesti saadaan näkyville liikennöidyimmät kohdat. Näin esimerkiksi voidaan parantaa liikennesuunnittelua jalankulun ruuhkakohtien purkamiseksi. Myös isojen yleisötapahtumien osalta ihmismäärien seuranta helpottuu. Esimerkiksi voidaan määrittää hälytyksiä, kun tietty ihmismäärä alueella ylittyy, jolloin tapahtumanjärjestäjä voi rajoittaa alueelle pääsyä (Milestone UXSS, 2020).

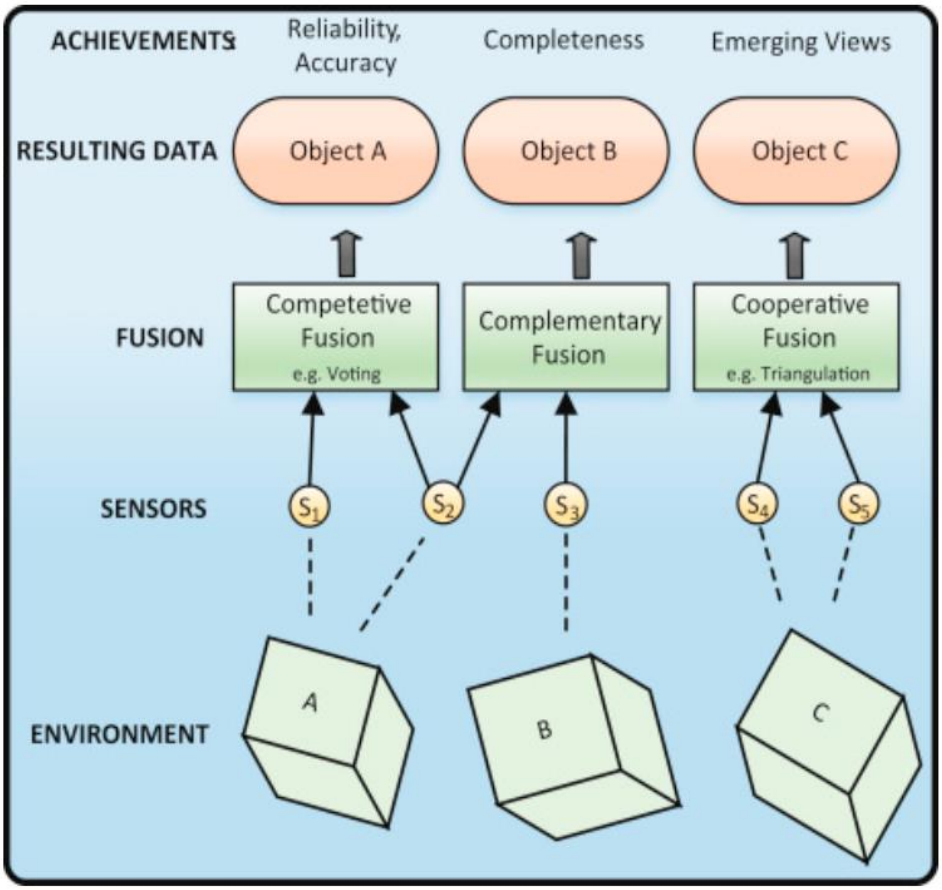
KUVIO 14 Up Xtreme Smart Surveillance ohjelmiston kuvakaappaus (Milestone UXSS 2020)

Data-analytiikkaan hyödynnettävien tekoälysovellusten käytössä tulee huomioida tarkasti toiminnan laillinen käsittelyperuste. Ohjelman avulla henkilötiedoista luodaan uutta tietoa, joka on osaltaan sidoksissa rekisterinpidon alla oleviin henkilötietoihin. Itse tilastot henkilöiden lukumäärästä ovat kuitenkin anonymisoituja, jolloin ne eivät ole yhdistettävissä rekisteröidystä tallennettuun tunnistettavaan kuvaan. Mikäli tilastoja tai muuta jatkojalostettua tietoa käytetään muualla ja ne siirretään pois järjestelmästä, tulee tietosuoja-asetuksessa olevat vaatimukset täyttyä. Tiedon siirron (ks. kohta 3.6) osalta sopimukset tietoja käsittelevän tahon kanssa on tehtävä. Lisäksi tietosuojaselosteessa ja vaikutustenarvioinnissa on tuotava tehtävänmukainen tarpeellisuusperuste sekä arvioida käsittelystä muodostuvat riskit. On myös tärkeää ymmärtää, että ohjelmistot ovat pääosin aina integroitu suoraan käytettäväksi varsinaisen valvontakamerajärjestelmän kautta. Tällöin käyttöoikeuksien hallinnassa tulee huomioida data-analyysia tekevien henkilöiden roolit ja rajata pääsyä sen mukaisesti mikä on tehtävän suorittamiseksi tarpeellista.

4.4.5 Sensorifuusio

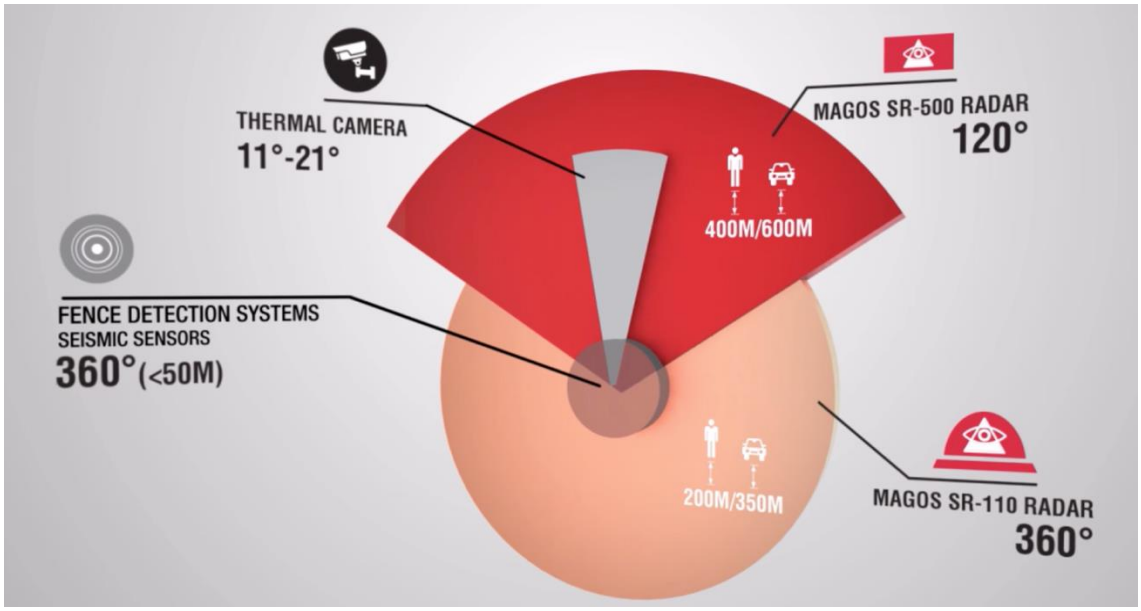
Sensorifuusiolla tarkoitetaan sitä, että eri lähteistä tuodaan erilaista dataa yhden hallintajärjestelmän alle. Rikastamalla tilannekuvaa monesta lähteestä voidaan nopeammin reagoida tilanteisiin. Sensorifuusion tarkoituksena on tuottaa uutta tietoa keräämällä sitä useammasta lähteestä. Tällöin yhteen kasattu tiedon avulla voidaan havaita jotain sellaista mikä ei yksittäisenä asiana johtaisi toimintakynnyksen ylitykseen (Galar & Kumar, 2017, s. 19).

Sensorifuusio voidaan jakaa kolmeen osa-alueeseen (kuvio 15), joista ensimmäinen on täydentävä sensorifuusio. Tällä tarkoitetaan sitä, että sensorit toimivat itsenäisinä, mutta niitä voidaan hyödyntää yhdessä paremman ymmärryksen saamiseksi tilanteesta. Kilpailullisella sensorifuusiolla tarkoitetaan taas toimintaa, jossa eri sensorit tarkkailevat samaa tapahtumaa, mutta tuottavat asiasta erilaista tietoa. Tästä esimerkkinä toimii erilaiset vikasietohälyttimet, joissa useamman eri sensorin tuottaessa samanaikaisesti hälytyksen laukeaa lopullinen hälytys. Yhteistoiminnallisella sensorifuusiolla tarkoitetaan, kun vähintään kahden sensorin turvin tuotetaan tapahtumasta informaatio, jota ei voitaisi yhdellä sensorilla tuottaa. Ihmisen silmät toimivat yhteistoiminnallisesti luoden aivoihin kolmiulotteisen kuvan (Galar & Kumar 2017, s. 26-27).



KUVIO 15 Sensorifuusion kolme ulottuvuutta (Elmenreich, 2001, s. 9)

Kameravalvonnassa erilaisia tekoälypohjaisia sensorifuusio toiminteita löytyy jo jonkin verran. Yleisesti ne painottuvat tilaturvallisuuteen (kuvio 16), jossa tietyn alueen valvontaan käytetään yhdessä kameroita, tutkia ja muita fyysisen turvallisuuden sensoreita kuten, erilaisia hälyttymiä (Milestone Marketplace). Järjestelmien tarkoituksena on tehdä automaattista valvontaa ja tunnistaa kohteita ilman ihmisen aktiivisia toimia. Pääosin järjestelmiä käytetään hyvin vartioitujen kohteiden ulkokuoren valvonnassa tai rajavalvonnassa. Esimerkiksi Magos Area Surveillance -ohjelmiston avulla voidaan sulauttaa alueen valvontaan tarkoitettujen eri sensorien hälytyksiä ja luoda niistä operaattoria tukeva automaattinen järjestelmä. Sensorin aktivoidessa hälytyksen järjestelmä kääntää tarkennettavia PTZ-kameroita kohteeseen, jolla valvoja saa reaaliaikaista kuvaa tunkeutujasta. Lisäksi ohjelma piirtää henkilön liikkeistä päivittyvää visuaalista karttaa, joka helpottaa henkilön paikantamista. Toimiakseen järjestelmä hyödyntää erilaisia ulkokuoreen asennettavia lasertutkia, valvontakameroita, ja hälyttymiä, kuten painesensoreita tai sähköisiä lukitusjärjestelmiä (Magossystems 2020).



KUVIO 16 Havaintokuva sensorifuusiosta tilaturvallisuudessa (Magossystems, 2020)

Sensorifuusion hyödyntäminen on kokonaisuudessaan henkilötietojentietojen prosessointia, koska GDPR:n (2016/679) artikla 4 kohta 2 mukaisesti henkilötietojen käsittelyä on tietojoukkojen yhdistäminen tai yhteensovittaminen. Etenkin kun toiminnan tarkoituksena on yhdistää erilaisia datalähteitä henkilöstä tunnistettavaan videokuvaan. Tällöin kaikkia tallennettuja tietoja tulee soveltaa GDPR:n mukaisesti.

4.5 Tekoälyn eettinen käyttö kameravalvonnassa

Sana etiikka tulee kreikankielisestä sanasta *ethos*, jolla tarkoitetaan moraaliin liittyvien kysymysten, esimerkiksi oikean ja väärän, arvojen, hyvän elämän pohdintaa. Eettiset periaatteet muodostuvat säännöistä, jotka ovat normeja, oikeuksia ja velvoitteita. Näillä säännöillä ohjataan ihmisten päätöksentekoa. Säännöt käsittelevät esimerkiksi kieltoja, kuten ”älä vahingoita” sekä ihanteita yksilön arvostamisesta ja kunnioittamisesta. Eettinen dilemma muodostuu yleensä, kun yksilö joutuu tekemään valinnan kahden erilaisen mutta mahdollisen ongelman ratkaisuvaihtoehdon kanssa. Tällaisissa tilanteissa haetaan ratkaisua yleisesti hyväksytyistä eettisistä periaatteista. Etiikassa ei ole yhtä oikeata ratkaisua, eikä niihin voi soveltaa standardinomaisia ratkaisuja. Tarkkojen tai yksityiskohtaisten vastausten puuttumisesta huolimatta eettisiin kysymyksiin tulisi aina suhtautua tunnollisesti (Leikas, 2008, s. 59).

Keskeisin yksilön ihmisarvoa ja vapautta ilmaiseva periaate on itsemääräämisoikeuden kunnioittaminen. Ihmisen aito kyky ilmaista omia tunteitaan, arvojaan ja pyrkimyksiään sekä tehdä itse omat tärkeät valintansa on äärimmäisen tärkeää. Itsemääräämisoikeuden perusta on vahva. Vaikka yksilön päätökset tuntuisivat huonoilta tai vääriltä, niitä ei saa pakottamalla, uhkailemalla tai

millään muullakaan vapautta rajoittavalla tavalla kiistää (Valtioneuvosto 2019, s. 12).

Itsemääräämisoikeuden ohella tulee huomioida yhteisen hyvän, yhteisöllisyyden ja oikeudenmukaisuuden periaatteet. Tarkastelemalla, miten yhteisön jäsenten tulisi toimia sekä miten haittojen ja hyötyjen tulisi jakautua yhteisössä vastataan oikeudenmukaisiin periaatteisiin. Yhteisö valitsee oman näkökulmansa ja määrittelee oikeudet ja velvoitteet jäsenilleen. Valinnan oikeudenmukaisuus voidaan ymmärtää monella eri tavalla riippuen yhteisön näkökulmasta. Tasa-arvoisuusperiaatteen mukaan kaikkia ihmisiä tulee kohdella samalla tavalla huolimatta heidän asemastansa tai taustastaan. Kun etuja ja haittoja arvioidaan, rikkaita ei suosita köyhien, vahvoja heikkojen, miehiä naisten, valkoihoisia värillisten, nuoria vanhojen, terveitä vammaisten jne. kustannuksella (Valtioneuvosto 2019, s. 13).

Euroopan komissio (2019, s.16) pitää parhaana lähestymistapana tekoälyn etiikkaan tapaa, joka perustuu EU:n perussopimuksiin, EU:n perusoikeuskirjaan ja kansainvälisen ihmisoikeuslainsäädännön perusoikeuksiin. Näillä voidaan luoda perusta abstrakteille eettisille periaatteille ja arvoille sekä konkretisoida luotettava tekoäly. Näistä oikeuksista monet ovat oikeudellisesti täytäntöönpanokelpoisia ja pakollisia. Komissio on määritellyt seuraavat perusoikeuksien ryhmät, jotka soveltuvat erityisen hyvin tekoälyjärjestelmiin:

- Ihmisarvon kunnioittaminen
- Yksilön vapaus
- Demokratian, oikeudenmukaisuuden ja oikeusvaltaperiaatteen kunnioittaminen
- Tasa-arvo, syrjimättömyys ja yhteisvastuu
- Kansalaisten oikeudet

Euroopan komission (2019, s.16) mukaan tekoälyjärjestelmien olisi myös parannettava yksilöllistä ja kollektiivista hyvinvointia. Eettisiä periaatteita on täsmennetty vaatimuksiksi, joista erityisesti neljää periaatetta on noudatettava sen varmistamiseksi, että tekoälyjärjestelmiä kehitetään, otetaan käyttöön ja käytetään luotettavasti:

- Ihmisen itsemääräämisoikeuden kunnioittaminen
- Vahinkojen välttäminen
- Oikeudenmukaisuus
- Selitettävyys

Euroopan komissio on tuoreeltaan julkaissut komiteamietinnön ns. white paperin tekoälyn eurooppalaisesta lähestymisestä kohti erinomaisuutta ja luottamusta. Mediat spekuloivat vuoden alussa vielä ennen julkaisua, että esimerkiksi kasvojentunnistaminen kiellettäisiin EU:n alueilla määräaikaisesti viideksi vuodeksi teknologian nopean kehityksen ja puutteellisen regulaation vuoksi (Euractiv, 2020). Yhdysvalloissa esimerkiksi San Franciscon kaupunki kielsi

kasvojentunnistamisen, kun taas Shanghaissa apteekit määräävät tiettyjä lääkkeitä sen perusteella (BBC, 2020). Helmikuussa julkaistussa mietinnössä kasvojentunnistusta ei kuitenkaan ollut rajattu pois. Komission mielestä EU:n laajuinen keskustelu biometrisen etätunnistuksen käytöstä olisi aloitettava. Lisäksi siinä korostettiin EU:n tieteellistä läpimurtokyvyn mahdollistamista parantaen ihmisten elämää ja samalla kunnioittaen heidän oikeuksiaan. Mietinnön mukaan datan määrä tulee kasvamaan voimakkaasti, jonka myötä Euroopan teknologiset mahdollisuudet kasvavat muun muassa tuotantotaloudessa, energiantuotannossa ja lääketieteessä. Tunnistettuja riskejä vastaan komission paperi ehdottaa tekoälyn lainsäädännöllistä viitekehystä, jota sovellettaisiin tuotteisiin ja palveluihin, jotka hyödyntävät tekoälyä (Euroopan komissio, 2020).

Yhteenvetona voidaan todeta, että eettiset periaatteet eivät ole yksioikoisia tai helppoja. Asioihin liittyy aina monta puolta. Suomalaiset ovat luottavaisia viranomaisiin, nykyregulaatioon ja teknologiaan, vaikka samaan aikaan elokuvat, kirjallisuus ja media maalailevat erilaisia uhkakuvia superihmisistä ja tekoälyn vallan ottamisesta. Asioita tarkasteltaessa pitää kyetä myös erottelemaan eettiset kysymykset oikeudellisista kysymyksistä. Esimerkiksi oikeudellisesti voi olla kysymys siitä, voidaanko biometrisia tietoja käyttää tunnistamisessa lainmukaisesti. Eettisesti taas tarkastellaan sitä, onko kameravalvonnassa käytetty biometrinen tieto tarpeellinen, käytettävä tai oikea ratkaisu tunnistettavuuteen (Korja, 2016, s. 417).

4.5.1 EU:n komiteamietintö (white paper) tekoälyn käytöstä

Helmikuussa 2020 Euroopan komissio julkaisi strategisen tason komiteamietinnön liittyen tekoälyn hyödyntämiseen tietoteknisessä ympäristössä. Mietintö itsessään ei sisällä EU:n laillista viitekehystä tekoälyn suhteen, vaan se antaa ylätasolla ymmärryksen siitä, millä tavoin ja miten komissio haluaa tekoälyä hyödynnettävän tulevaisuudessa. Linjauksilla on tarkoitus tehdä EU:sta tekoälyn osalta johtava toimija niin eettisen kuin teknisen tekoälyn hyödyntämisen suhteen. Komiteamietintö on jaettu neljään osaan, joista kaksi osaa käsittelee tekoälyä, kolmas Euroopan digitaalista tulevaisuutta ja viimeisin osa datataloutta (Euroopan komissio - COM 2020, s. 1-2).

Datan tehokkaammalla hyödyntämisellä, etenkin tekoälyn keinoin, voidaan parantaa merkittävästi yhteiskunnan toimintaa monella eri sektorilla. Tekoälyä on kuitenkin kehitettävä EU:n perusarvojen mukaisesti siten, että toiminta on läpinäkyvää ja eettistä. Toiminnan on oltava säädeltyä, mutta regulaatio ei saa tukahduttaa innovointia. Komissiomietinnön tarkoituksena oli tuoda esille se, että EU tulee vahvasti panostamaan tekoälyn kehittämiseen (kuvio 17) nyt ja tulevaisuudessa niin yksityisellä kuin julkisella sektorilla (Euroopan komissio - COM 2020, s. 3-4). Komiteamietintö tekoälystä on jatkoa Euroopan unionin massiiviseen panostukseen tutkimuksen ja innovoinnin saralla. Horisontti 2020 ohjelman aikana 2014-2020 myönnetään rahoitusta lähes 80 miljardia euroa (Euroopan komissio - Horisontti 2014, s. 5). Komissiomietinnössä tekoälyyn halutaan panostaan merkittävästi myös tulevaisuudessa, sillä yli 25 %

kaikista teollisuus- ja palveluroboteista valmistetaan Euroopassa (Euroopan komissio 2020).

KUVIO 17 Tekoäly ja EU lukuina (Euroopan komissio 2020)

Uudet teknologiat tuovat mukanaan myös uusia riskejä, jotka voivat vaikuttaa ihmisoikeuksiin. Mikäli tekoälyn annetaan tehdä itsenäisiä päätöksiä, niihin johtaneet päätelmät voivat tekoälyalgoritmien monimutkaisuuden vuoksi olla äärimmäisen vaikeat tulkita. Tekoälyn avulla ihmisten seuranta ja heidän päivittäisten askareiden analysoiminen on nopeaa ja helppoa. Tämä luo selkeän riskin sille, että tekoälyä voidaan käyttää tahallisesti väärin. Esimerkiksi valtiollisen tahon tai yksityisellä sektorilla työnantajan puolelta. Tekoälyä voidaan myös käyttää muuttamaan anonymisoitu tieto takaisin henkilöön liittyväksi tiedoksi. Riskejä voi myös syntyä tekoälyalgoritmien kehitysvaiheessa. Ohjelmiin päätyneet virheet voivat johtaa vääriin tulkintoihin, joiden alkuperää on vaikea selvittää. Tämä voi pahimmillaan johtaa henkeen kohdistuviin onnettomuuksiin, esimerkiksi tekoälyohjattavien ajoneuvojen kolareihin (Euroopan komission - COM, s. 10-12).

Komiteamietinnössä painotetaan sitä, että EU:n sisällä tekoälyn hyödyntäminen tulisi olla yhdenmukaista. Näin EU:n sisämarkkinoilla ei synny turhaa ristiriitaa siitä millä tavoin tekoälyä kehitetään ja käytetään. Riskilähtöisen lähestymistavan avulla voidaan ennalta estää ongelmia liittyen tekoälyyn. Lisäksi tulisi tunnistaa erityisen korkean tason riskit, jotka koostuvat niin ohjelmistoista kuin niitä käyttävistä tahoista. Korkea riskin kohteina on mainittu erikseen terveydenhuolto ja kuljetus- tai energiasektorit. Sovelluksista korkeaan riskikategoriaan kuuluu erityisiä henkilötietoluokkia käsittelevät sovellukset, kuten biometrinen tunnistaminen ja siihen liittyvät henkilöiden seurantaan tarkoitetut järjestelmän, kuten automaattinen kasvojentunnistus. Tunnistettuihin korkean riskin kohteiden tulisi erityisesti kiinnittää huomiota toiminnan läpinäkyvyy-

teen. Kohteilla olisi myös pakolliset yhdenmukaisuutta tukevat vaatimukset, jotka olisi toteutettu ennen markkinointia. Myös normaalin riskitason kohteille olisi tärkeää luoda arviointimenetelmä. Tämä tukisi erilaisten tekoälytuotteiden markkinointia ja niiden luotettavuutta. Läpinäkyvyyden lisäämiseksi ja toiminnan mittareiksi komiteamietinnössä on tuote esille muutamia kohtia (Euroopan komissio - COM, s. 17-24).

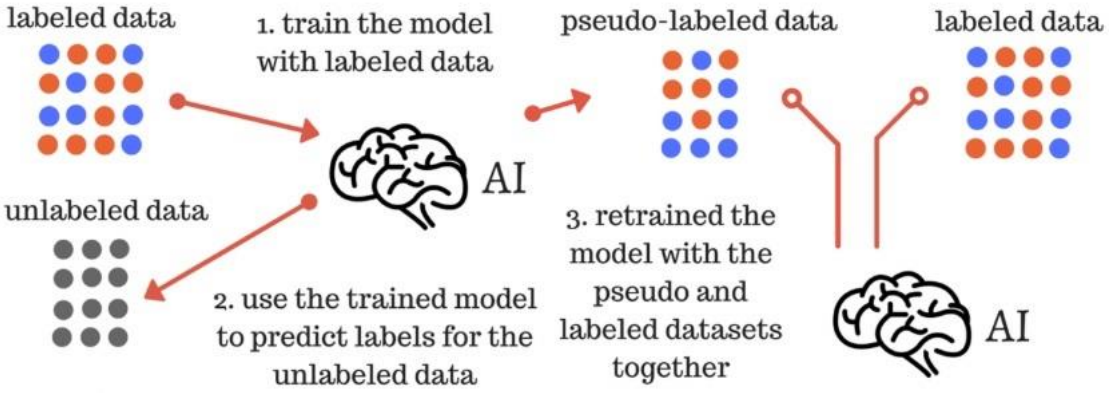
- Tekoälyn opetusmateriaalin laatu ja tietosuoja
- Datan hyödyntäminen ja laadukas dokumentointi
- Informaation avoimuus
- Tiedon oikeellisuus
- Ihmisen valvonta niin tekoälyn kehityksessä kuin käytössä
- Lisäksi erityiset edellytykset biometriseen tunnistamiin liittyen

Euroopan komission tarkoituksena on luoda visio yhtenäisestä Euroopasta, jonka yhtenä kantavana voimana on digitaaliset ratkaisut. Näiden avulla voidaan myös taata eurooppalaiset arvot siitä, että teknologia tukee ihmisiä ja talous sekä siihen liittyvä kilpailu on oikeudenmukaista, avointa ja demokraattisten arvojen mukaista. Komission mukaan EU:n tulisi olla roolimallina sille, miten yhteiskunta tekee parempia ratkaisuja, jos se pystyy tehokkaasti hyödyntämään dataa (Inside Privacy, 2020).

4.5.2 Kasvojentunnistusteknologia

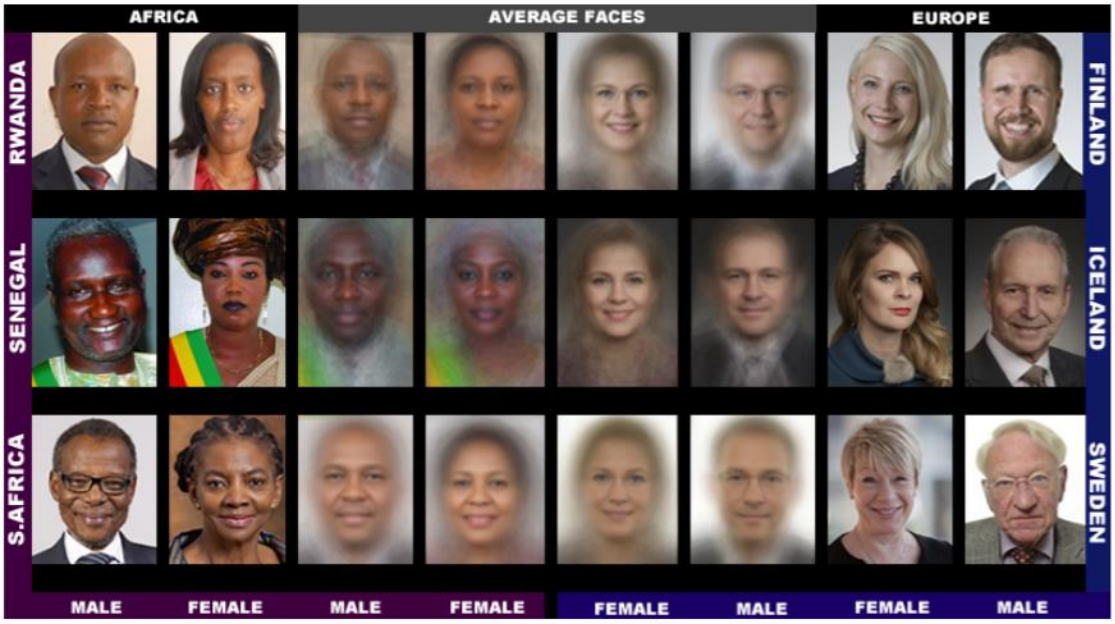
Viimeisimmät tutkimukset kasvojentunnistusteknologiassa ovat osoittaneet, että koneoppimispohjaisissa algoritmeissa on ollut rodun tai sukupuolen perusteella syrjiviä piirteitä. Tekoälypohjaiset ohjelmistot itsessään eivät tietenkään tee päätöksiä oikeusasteessa, mutta sitä voidaan käyttää apuna tunnistamaan epäiltyjä. Virheellä ohjelmiston algoritmissa voi olla vakavia seurauksia. Mikäli kasvojentunnistusteknologiaa voidaan käyttää oikeudessa todisteena tai tukevana näyttönä, joku voi joutua rikoksesta tuomituksi virheellisen mutta luotettavan tunnistuksen perusteella (Buolamwini & Gebru, 2018, s. 1).

Oikeudenmukaisempia ja tarkempia algoritmeja (kuvio 18) on yritetty luoda, mutta vain kourallinen toimijoista ovat tehneet sitä tekoälyn ja konenäön kanssa. Esimerkiksi melanoomaa on yhdysvaltalaisen tutkimuksen mukaan kyetty tunnistamaan kuvista konenäköä hyödyntävällä järjestelmällä yhtä suurella tarkkuudella kuin asiantuntijoiden toimesta (Esteva, 2017, s. 115-118). Tarkkuutta ei voida kuitenkaan mitata eri ihotyypeille ilman, että järjestelmä ja sen algoritmi hyödyntää sille annettua luokiteltua tietoa, kuten erityyppiset ihonvärit, ihon syvyydet tai ihon karvoitukset. Vääristyneestä automaattisesta tunnistamisesta voisi terveydenhuollon tilanteissa koitua ongelmia potilaille, joille määrätään lääkkeitä tai hoitoja sen perusteella (Buolamwini ym., s. 2).



KUVIO 18 Yksinkertainen tekoälyn pseudonymisoinnin malli (Kodoman, 2017)

Kasvojentunnistusteknologiaa hyödyntävissä järjestelmissä tämä voi muodostua ongelmaksi, jos järjestelmälle syötetty data ja sen algoritmi eivät saa riittävän tarkkaa luokiteltua dataa. Käytännössä tämä tulee esiin siten, että tietyt aliedustettuina olevat sukupuolet, ihonvärit tai rodut tuottavat enemmän false positive tuloksia ja voivat joutua sen myötä viranomaisen tarkastettavaksi. Ensimmäisiä tutkimuksia asian eteen on tehty ja esimerkiksi ihotyyppiä voidaan arvioida konenäöllä useilla eri asteikoilla, jolloin sukupuoli voidaan määritellä ihotyypin perusteella. Lisäksi erilaisia aliryhmiä luokitellulle datalle voidaan määritellä tarkkuuden lisäämiseksi. Tunnistuksella ei välttämättä haeta yksilöivää tunnistusta, vaan riittävä todennäköisyys luokitellun datan tunnisteilla. Muutamat tutkimukset ovat vieneet automaattisen kasvojentunnistuksen tutkimuksiaan pidemmällekin. Ne ovat kasvojen ilmeiden perusteella luokitellun datan avulla pyrkineet tunnistamaan henkilöiden tunnetiloja, luonteenpiirteitä, taipumuksia tai seksuaalisuutta. Tutkimuksessa tunnistettuja heikkouksia tukevat useiden muiden tutkimusten tulokset, joiden mukaan kasvojentunnistusalgoritmeja hyödyntävissä järjestelmissä ovat olleet systemaattisesti alhaisempia tummaihoisille naisille tai henkilöille, jotka ovat iältään 18 – 30-vuotiaita. Useissa tutkimuksissa on käytetty yleistä vertailuanalyysitaulukkoa julkisuuden henkilöiden kuvista (kuvio 19), jotta merkittävää eriarvoisuutta voitaisiin välttää. (Buolamwini ym., s. 3-4)



KUVIO 19 PPB - Parlamentin vertailuanalyysitaulukko (Buolamwini & Gebru, 2018, s. 4)

Buolamwinin ja Gebrun tutkimuksessa vertailtiin kolmea kaupallista algoritmia. PBB:n vertailuanalyysitaulukko antoi aluksi kiitettäviä tuloksia kasvojentunnistusalgoritmille tunnistuksen tarkkuuden todennäköisyysarvioilla välillä 87,9 % - 93,7 %. Tästä olisi voitu vetää johtopäätöksiä, että algoritmit soveltuvat kaikille kansanryhmille. Kuitenkin, kun analyysiä tarkasteltiin sukupuolen ja fenotyyppisen hajoavuuden perusteella, voitiin huomata, että luokitellun datan tarkkuus oli 8,1 % - 20,6 % heikompi naisilla kuin miehillä ja 11,8 % - 19,2 % heikompi tummaihoisilla kuin vaaleaihoisilla. Vielä tarkemmin tarkasteltaessa huomattiin, että korkein virhetodennäköisyys oli tummaihoisilla naisilla vaihdellen 20,8 % - 34,7 % välillä. Vaaleaihoisten miesten virhetodennäköisyysprosentti oli pienin lähennellen usein nollaa (Buolamwini ym., s. 10-11).

Algoritmien heikkoudet ovat yleisesti tiedossa. Automaattisen kasvojentunnistuksen tunnistustarkkuuteen vaikuttavat kuvan, henkilöiden tai kasvojen asento, valaistus, ilmeet, okkluusio ja tausta. Erityisesti valaistus on ihotyypin tunnistuksessa tärkeässä roolissa, yli- tai alivalaistujen kuvien datan tunnistettavuus voi olla haasteellista. Datan luokittelu ja kuvien laatu ovat myös erittäin tärkeitä tekijöitä tarkkuutta arvioitaessa. Algoritmien oikeudenmukaisuus perustuu asiayhteydellisiin päätelmiin ja optimointeihin, joiden lisätutkimuksia tarvitaan erilaisten vertailuanalyysien kanssa tekoälyn luotettavuuden ja läpinäkyvyyden lisäämiseksi. Tutkimukset itsessään kuitenkin lisäävät empiiristä tukea tekoälyn läpinäkyvyydelle ja luotettavuudelle (Buolamwini ym., s. 12).

Mitä tulee tunnistamisen tarkkuuteen, Proceedings of the National Academy of Sciences of United States of American suorittaman tutkimuksen mukaan ihmisen ja koneen kyky suorittaa kasvovertailua on hyvin pitkälle samaa tasoa. Tutkimuksessa tekoälyalgoritmeja verrattiin niin forensisen koulutuksen saaneisiin kasvotunnistusspesialisteihin kuin ns. supertunnistajiin, jotka ovat

luontaisesti parempia tunnistamaan ihmisten kasvonpiirteitä. Tutkimuksessa havaittiin myös, että ihmisen tunnistuksen taso parani, kun henkilö suorittu kasvojentunnistusta ryhmässä. Kasvontunnistukseen käytettävät tekoälyalgoritmit ovat kehittyneet merkittävästi viimeisten vuosien aikana. Tämä johtuu siitä, että niissä on alettu hyödyntämään syväoppimista ja neuroverkkoja, joita koulutetaan miljoonilla kasvokuvilla tuhansista eri ihmisistä. Tästä huolimatta forensisen kasvontunnistuskoulutuksen saanut ryhmä pärjäsi tunnistamisessa yhdenveroisesti kehittyneiden tekoälysovellusten kanssa. Tutkimuksen merkittävin tulos oli kuitenkin se, että yhdistettäessä ihmisen ja tekoälyn kasvontunnistuskyvykkyydet onnistuneiden tunnistusten määrä kasvoi merkittävästi (Philips, Yates, Hu, Hahn, Noyes, Jackson, Cavanos, Jeckln, Ranjan, Sankaranaraynan, Chen, Castillo, Chelappa, White & Toole, 2018, s. 3-4).

Suoritettaessa tekoälyalgoritmien toimintavarmuuteen liittyvää tarkastelua tulee myös huomioida, että tällä hetkellä niiden käyttö ei kameravalvonnan osalta pyrikään täydelliseen tunnistukseen. Tekoälyllä pyritään enemmänkin suorittamaan seulontaa ja helpottamaan tiedon käsittelijöiden mahdotonta tehtävää tilanteissa, joissa joudutaan aktiivisesti käymään läpi kymmenien tai satojen valvontakameroiden materiaalia. Lisäksi materiaalia voi joutua tarkastelemaan pitkältä ajanjaksolta, jolloin käsiteltävien henkilötietojen määrä on massiivinen. Isojen datamäärien huolellinen käsittely vie hyvin paljon aikaa ja resursseja. Lisäksi kameravalvonnassa käytettävät kamerat ja niiden sijoittelu sekä valaistuksen määrä eivät vastaa optimaalisissa ympäristössä toteutettavaa kasvokuvavertailua. Tämä vaikeuttaa niin ihmisen kuin tekoälyn tunnistusvarmuuteen. Tekoälyn tuoma etu onkin se, että sitä voidaan hyödyntää datan seulonnassa ja määrittää tunnistusarvoja siten, ettei ihmisen tarvitse käydä kaikkea materiaali läpi. Materiaalista voidaan nostaa esiin vai kasvonpiirteillään samankaltaisia henkilöitä, jotka voidaan nopeasti arvioida ihmisen toimesta positiiviseksi tai negatiiviseksi tunnistukseksi. Henkilöiden biometrisia tietoja ei tarvitse tallentaa kuin vain vertailukuvan osalta. Itse videomateriaalista riittää biometrinen laskenta ja tuotettujen materiaalista kaivettujen henkilöiden pelkkä kuva ilman biometrisia tietoja säilytetään. Näin ei tarvitse säilöä henkilöön kohdistuvia erityisiä henkilötietoja tarpeettoman paljon ja muutenkin henkilötietoihin kohdistuva käsittely vähentyy.

4.5.3 Automaattinen päätöksenteko

Automaattisella päätöksenteolla viitataan prosessiin, jossa tietojärjestelmä tekee itsenäisesti lopullisen päätöksen saamiensa tietojen perusteella. Tällaista prosessia kutsutaan itsenäiseksi automaattiseksi päätöksenteoksi. Automatisaatiota voidaan käyttää myös päätöksenteon apuna siten, että tietojärjestelmä valmistelee päätösluonnoksen, jota virkamies täydentää ja tekee lopullisen päätöksen. Tällöin kyseessä on avusteinen päätöksenteko prosessi. Tekoäly liitetään usein automaattisen päätöksenteon yhteyteen, kun kyseessä on loogista päättelyä, kielellistä ymmärrystä tai visuaalista havaitsemista parantavista järjestelmistä. Tekoälyn osalta kaksi keskeisintä tapaa toteuttaa ovat sääntöpohjaisilla tai op-

pivilla järjestelmillä. Sääntöpohjainen automaattinen päätöksenteko perustuu ihmisen määrittelemiin sääntöihin, joka edellyttää, että asiassa sovellettavat termit muutetaan kyllä/ei-tyyppisiksi säännöiksi, jotta ne voidaan toteuttaa koneellisesti. Vaihtoehtoisesti järjestelmä voidaan toteuttaa oppivan tekoälyn periaatteella. Tällä tarkoitetaan, että tekoäly löytää sille annetusta suuresta tietoaineistosta esimerkiksi säännönmukaisuuksia hakemusten ja päätösten välillä. Näitä säännönmukaisuuksia voidaan sitten soveltaa sille annettuihin uusiin hakemuksiin (Oikeusministeriö 2020, s. 3-4).

Automaattisiin päätöksentekojärjestelmiin liittyy virheellisen päättelyn riski. Teoriassa sääntöihin perustuva päätöksenteko on virheetöntä, mutta järjestelmä voi seuraavista syistä päätyä virheellisiin lopputuloksiin:

1. Päätöksentekosäännöt ovat virheellisiä, koska poikkeuksia ei ole huomioitu riittävästi
2. Päätöksentekosääntöjen ohjelmakoodi on virheellisesti toteutettu
3. Muu kuin päätöksentekosääntöjen poikkeus aiheuttaa virheellisen lopputuloksen, esimerkiksi sähkökatko

Tällaisten virheiden mahdollisuus on huomioitava otettaessa käyttöön automaattisia päätöksentekojärjestelmiä. Päätöksentekosäännöt on muodostettava luotettavasti kuten virkavastuulla, ohjelmakoodin luontiin on liitettävä asianmukainen testaus ja poikkeuksellisiin virhetilanteisiin on varauduttava asianmukaisesti järjestelmää suunniteltaessa (Oikeusministeriö 2020, s. 4).

Eduskunnan apulaisoikeusasiamies Maija Sakslin on joulukuussa 2019 antanut ratkaisun päätöksessä EOAK/3379/2018 Verohallinnon automatisoidun päätöksentekomenettelyn laillisuudesta. Ratkaisu koskee kahta kantelua, jossa Verohallinnon verotusmenettelyn automatisoinnista on kanneltu. Verohallinto on selvityksessään vastannut, että heidän automatisoidut menettelynsä ovat perustuneet lainsäädäntöön, jossa on huomioitu perustuslaki, tietosuoja-asetuksen 22 artikla ja muutoin menetelty hyvän hallinnon mukaisesti. Ratkaisussaan apulaisoikeusasiamies katsoo, että Verohallinnon automatisoitu verotus- ja päätöksentekomenettely ei perustu asianmukaiseen ja täsmälliseen lainsäätelyyn, jossa olisi otettu huomioon hyvän hallinnon ja oikeusturvan sekä virkavastuun asianmukainen toteutuminen. Apulaisoikeusasiamies piti menettelyä lainvastaisena. Lopuksi päätöksessä myös todetaan tietosuoja-asetuksen vaatimusten huomioonottamisesta automatisoidun päätöksenteon tarpeita selvitettäessä, jotka kuitenkin kuuluvat tietosuojavaltuutetulle eikä päätöksessä oteta siihen enempää kantaa.

Kameravalvonnan ja tekoälyn osalta automatisointi perustuu pitkälti vielä sääntöpohjaisiin järjestelmiin ja ohjelmistoihin. Kamerat tunnistavat ennalta määriteltyjä hahmoja, esineitä, olosuhteita tai muita ihmisen antamia sääntöjä. Näistä tunnistuksista tehdään hälytys, tilastointia tai tietoa, jonka perusteella henkilö käyttää näitä tietoja päätöksenteon tueksi ja tekee asiassa lopullisen ratkaisun. Kameravalvonta, tekoäly ja uuden teknologian luomat automatisoidut mahdollisuudet edellyttävät järjestelmän omistajalta, rekisterinpitäjältä ja tieto-

jen käsittelijältä suunnitelmallisuutta, riskien- ja vaikutustenarviointia, sovittuja käytäntöjä sekä tietojen elinkaaren hallintaa. Kameravalvonnan kokonaisuuden hallinnasta on kerrottu yksityiskohtaisesti tämän tutkimuksen tuloksissa luvussa 7.

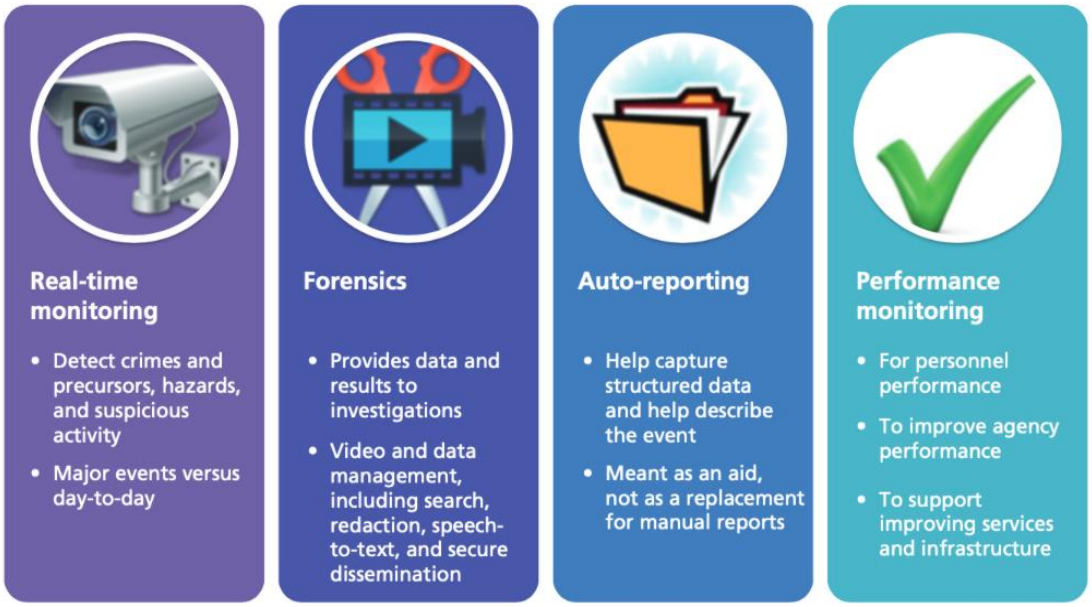
4.6 Kameravalvonnan tulevaisuudennäkymät

Tulevaisuudessa kameravalvonnan määrä tulee kasvamaan. IHS Markitin (2019) tekemän raportin mukaan, oletettavasti vuosi 2020 tulee olemaan videovalvontaan liittyvän teknologian myynnin kannalta tietynlainen vedenjakaja, koska vuosittainen myynti ylittää 20 miljardin rajan. Lisäksi valvontakameroita arvioidaan olevan maailmassa noin miljardin kappaleen verran. Western Digitalin (2018) tekemän analyysin perusteella Yhdysvalloissa enemmistö eli 52 % tunsi itsensä turvattomaksi. Lisäksi 45 % väestöstä pelkäsi joutuvansa joukkoammunnan kohteeksi. Tutkimus oli tehty vuosina 2015 ja 2017 ja siihen oli laskettu mukaan 23 kaupunkia. Analyysin perusteella arvioitiin, että turvallisuuden kehittämiseksi panostus valvontakameroihin kulkisi kolmessa syklissä (kuvio 20). Ensimmäisenä viranomaiset hyödyntäisivät omia kameraverkkoja, jonka tarkoituksena olisi selvittää rikoksia. Jälkijättöiseen selvittelyyn hyödynnettäisiin myös manuaalisesti muiden tahojen kameravalvontaa.

KUVIO 20 Kameravalvonnan kehityssyklit (Western Digital, 2018)

Vaiheessa kaksi, jonka Western Digital (2018) arvioi tapahtuvan 2025 mennessä, kameraverkkojen käyttöön valjastetaan tekoälyä. Näin datamassaa pystyttäisiin paremmin hyödyntämään, sillä tällä hetkellä arviolta vain 1 % videomateriaalista analysoidaan. Tekoälyn avulla kameravalvontaa voisi hyödyntää rikoksia ennalta estäen, mikä tulisi pelkästään Yhdysvalloissa vuoteen 2014 mennessä pelastamaan 76 000 ihmistä joukkoammuskeluilta. Älykaupunkien ja niiden asukkaiden mukaantulo ja yhteistyö viranomaisten kanssa laajentaisi massiivisesti kerättävän videoaineiston määrää. Yhdysvalloissa useissa kaupungeissa

kuten Chicagossa ja Baltimoressa poliisilla on suorakäyttöyhteys yritysten kuin yksityisten henkilöiden omiin valvontakameroihin. Tämän takia yksittäisten kaupunkien viranomaisverkkojen kameroiden lukumäärä on kasvanut eksponentiaalisesti, arviolta useisiin satoihin tuhansiin (Hollywood ym., 2018, s. 6). Kameravalvonnassa tekoälyä hyödynnettäisiin usealla osa-alueella. Niin reaaliaikaisesti tunnistamaan ja ennalta estämään rikoksia ja eri laatuisia tapahtumia, kuin takautuvasti käsittelemään ja indeksoimaan tuhansista lähteistä tuotettua videodataa. Lisäksi videovalvonnan avulla voitaisiin luoda automaattisesti raportteja ja tilastoja, joita voitaisiin hyödyntää niin toiminnan kehittämissä kuin datan rikastamisessa ja myymisessä. Kamerat voitaisiin valjastaa myös tehostamaan työpaikan prosesseja, kuten vähentämään työajan käyttöä tai parantamaan työntekijän työnlaatua (Hollywood ym., 2018, s. 8).

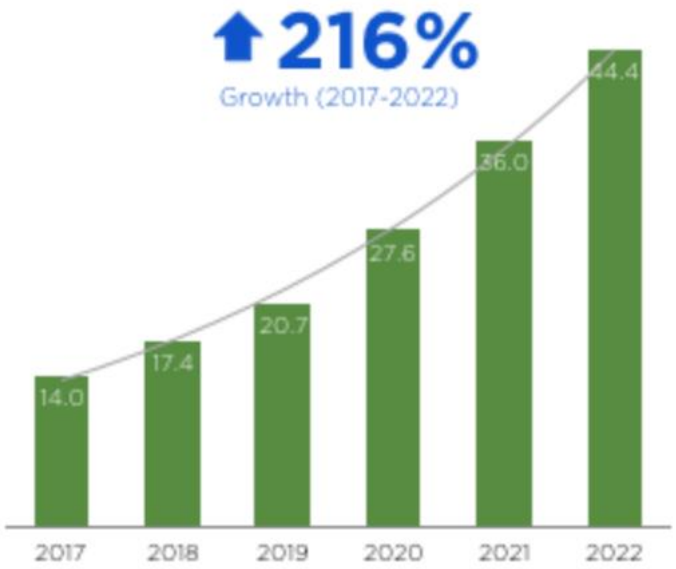


KUVIO 21 Videoanalytiikan ja sensorifuusion mahdollisuudet (Hollywood ym., 2018)

Vaiheessa 3 Western Digital (2018) raportti ennustaa, että lähes kaikki verkkoihin yhdistetyt laitteet toimivat datalähteinä, joita voidaan hyödyntää laajana kokonaisuutena niin yksityisten kuin viranomaisten erilaisiin tarpeisiin. Dataa ei itsessään enää muokata, vaan se luokittelee itsensä, jonka vuoksi datan analysointi on mahdollista toteuttaa suoraan ja täysin tarpeen mukaan. Datamassan kasvaessa tekoälyn tuottamat ennusteet ja arviot paranevat entisestään, joita voidaan hyödyntää proaktiivisesti esimerkiksi lukitsemalla automaattisesti tiloja tiettyjen uhkaindikaattorien toteutuessa. Langattomien verkkojen nopeuksien kasvaessa 5G:n myötä, isoa datavirtaa siirtävien teräväpiirtokameroiden käyttö laajenee myös ns. kertakäyttöiseksi. Esimerkiksi suurien tapahtumien tai rakennustyömaiden yhteyteen voidaan rakentaa tilapäisesti videovalvontakeskittymiä, joista data siirretään pilveen. Näin paikallisia kalliita VMS-ratkaisuja ei tarvitse rakentaa. Vuonna 2020 yli 73 operaattoria 41 maassa on tarjonnut yhden tai useamman 5G-palvelun (GSA, 2020). Kameroiden laskenta-

tehon noustessa niissä prosessoitavat toiminteet tehostuvat, jolloin data-analyysin latenssi palvelinpuolella vähenee. Etenkin kun tiedon siirtäminen 5G:stä johtuen ei ole enää toiminnan pullonkaula (ISH Markit, 2019).

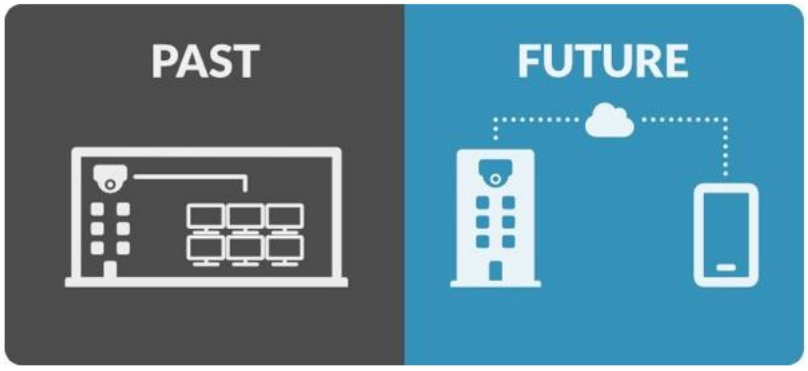
Tyypillisten valvontakameroiden määrä kasvaa (kuvio 22) tasaisesti tulevaisuudessa, mutta verkkoon liitettyjen videodataa tuottavien laitteiden määrä kasvaa räjähdysmäisesti. LDV Capitalin (2017) tekemän raportin mukaan videovirtaa tallentavia ja jakavia laitteita on vuonna 2020 45 miljardia.



KUVIO 22 Videota tuottavien laitteiden määrän kasvu (LDV Capital, 2017)

Teknologian suuntaus tulee vahvasti olemaan videokuvasta tehtävän analyysin, tallennuksen, suodattamisen ja havainnollistamisen ajamaa. Ilman konenäkö- ja tekoälypohjaisia ratkaisuja videovirran hyödyntäminen suuressa mittakaavassa reaaliaikaisesti olisi mahdotonta. Tämän vuoksi tekoälyn kehitys on avainasemassa tulevaisuudessa, eritoten robotiikan vallatessa alaa (LDV Capital, 2017).

Datamäärien kasvaessa luottamuksen tarve tulee olemaan yksi merkittävistä vaikuttimista kameravalvonnan käytön kuin sen myynnin osalta. Langattoman tiedonsiirron vaikutuksesta tietoa siirretään pitkälti pilviratkaisuihin (kuvio 23) sen halpuuden ja käytännöllisyyden vuoksi. Suljetut kameraverkot jäävät marginaaliratkaisuiksi.



KUVIO 23 Suljetuista verkoista pilviratkaisuihin (IPV CCTV, 2019)

Datan fyysisellä sijainnila pilviratkaisuissa on merkittävä rooli. Kansalliset ja kansainväliset sopimukset sekä lainsäädäntö antaa tai kieltää pääsyn palvelintiloihin. Dataa käsittelevän ja hyödyntävän tahon tulee pystyä takaaman tiedon niin pääsy käsiksi tietoon kuin sen eheys, luotettavuus (IPV CCTV, 2019). EU pyrkii regulaatiolla ja rahoituksella luomaan mahdollisuuksia innovoida ja toteuttaa luottamukseen pohjautuvia tekoälyratkaisuja. Vasta henkilön perusoikeuksien mukaisten käytäntöjen kautta tekoälyn koko potentiaalia voidaan hyödyntää ihmistä tukien eikä sitä vastaan.

5 YHTEENVETO KIRJALLISUUSKATSAUKSESTA

Tämän luvun tarkoituksena on koota yhteen tutkimuksen teoriaosuudesta esiin tulleet pääteemat. Tutkimuksen alussa varsinainen tutkimusongelma oli jaettu kolmeen syventävään alatutkimuskysymykseen. Näiden avulla alustavasti rajattiin tutkittavaa aluetta vastaamaan tutkimustilaajan tarpeita. Teoriaosuuden aikana tuli selväksi, että alatutkimuskysymysten avulla saatiin teoriaosuus selkeästi erotettaviin osiin, eli henkilötietoihin liittyvään regulaatioon, kameravalvontaan koskevaan kyberturvallisuuteen ja tekoälyn erilaisiin muotoihin, joita voidaan hyödyntää kameravalvonnassa. Ilmeistä on kuitenkin se, että kaikki pääkategoriat ovat toisiinsa vahvasti sidoksissa. Kirjallisuuskatsauksen avulla saatiin tutkimukseen kerättyä hyvin kattava otanta kameravalvontaan liittyvää regulaatiota, sekä eri instanssien päätöksiä ja ohjeistuksia. Lisäksi kameravalvonnassa tapahtuvaa tekoälyn kehitystä kuvattiin erilaisten esimerkkien avulla, joita tulkittiin tutkimuksen aikana kerätyn regulaation perusteella.

Tutkimuksessa käytettyä aineistoa avattiin tutkimusongelman näkökulmasta, pääsääntöisesti jokaisen kohdan yhteydessä. Toiminta helpottaa lukijaa löytämään vastauksia kysymyksiinsä nopeammin mutta antaa myös mahdollisuuden käsitellä yksittäisiä ja tärkeitä asioita hieman kattavammin sekä tarkemmin. Näin myös vältytään siltä, että tutkimuksen tulokset paisuvat siten, että tutkimuksen ydinongelmien tulkinta pilkkoutuu liian yksityiskohtaiseksi. Teorian yhteenvedon tarkoituksena on valittujen tutkimusmenetelmien mukaisesti jakaa ja järjestää havaitut sekä saturoituneet teemat pääkategorioihin. Pääkategorioiden osalta vasta tutkimuksen tuloksissa voidaan lopullisesti vastata kattavasti tutkimuskysymykseen ja sitä ohjaaviin alatutkimuskysymyksiin. Näin voidaan varmistua siitä, että tutkijoiden teoriaosuudessa esiintuomat ja tuloksissa vahvistetut johtopäätökset ovat valideja ja linjassa ulkopuolisten alansa erityisosaajien tulkintojen kanssa.

Teoreettisen viitekehyksen kasaamisen yhteydessä tutkijat huomasivat, että aihealueesta ei ollut enää saatavilla uutta materiaalia. Tämä tarkoitti myös sitä, että tiettyihin asioihin ei löytynyt suoria vastauksia. Tämän luvun tarkoituksena onkin osaltaan havainnollistaa ydinkategorioihin liittyvät vielä lisäselvitystä vaativia kysymyksiä. Hyvin varhaisessa vaiheessa tutkimusta oli ilmeis-

tä, että tutkimuksen kannalta on oleellista saada lausuntoja kirjallisuuskatsauksen tueksi aihealueen asiantuntijoilta. Kirjallisuuskatsauksen jäljiltä olevien ratkaisemattomien kysymysten teemahaastattelujen runkona käytettiin teorian pohjalta luotuja tutkijoiden omia tulkintoja. Kirjallisuuskatseuksessa havaittiin myös se, että suoran kameravalvontaa koskevan regulaation puute muodosti ongelman. Etenkin silloin kun toimintaa piti arvioida Suomen perspektiivistä. Euroopan sisäinen regulaatio oli tuoretta, eikä siitä ollut vielä keritty tehdä tarpeeksi paljon linjauksia valvovien viranomaisten toimesta. Tämä korostui tekoälyohjelmistojen käytöstä tehtyjen päätösten osalta, joita oli kokonaisuudessaan vain muutamia. Euroopan unionin yleinen tietosuoja-asetus ja tästä johdettu kansallinen tietosuojalaki loivat ylätason kameravalvonnan regulaatiolle. Näistä johdettua yksityiskohtaisempaa kameravalvontaan liittyvää ohjeistusta oli julkaistu Euroopan tietosuojaneuvoston (EDPB) kautta. Ohjeistuksessa oli tuotu esille jopa käytäntöön asti vietyjä esimerkkejä. Tästä huolimatta tekoälyn käyttö kameravalvonnassa jätti aukkoja mentäessä yksityiskohtaisempiin käyttötapauksiin. Vaikka kyseessä olikin hyvinkin yksittäisiä tilanteita, niistä johdettavat ongelmat toivat esille laajempia tulkintakysymyksiä, joihin ei kirjallisuuskatsauksessa löytynyt vastauksia. Eritoten henkilötiedon ja biometrisen tiedon eli erityisen henkilötietoluokkien rajanveto oli hahmontunnistuksen osalta vailla kunnollista laintulkintaa. Esimerkiksi käyttötapaus, jossa henkilön kuvaa käytetään laskennallisen mallin pohjana, jota vasten tekoäly suorittaa videomateriaalista vertailua, on hyvin haasteellinen. Käytettäessä tekoälyohjelmistoja tulisi rekisterinpitäjän olla hyvin perillä järjestelmän kaikista ominaisuuksista ja niissä muodostuvista henkilötiedoista.

Kameravalvontajärjestelmiin liittyvän kyberturvallisuuden osalta, niin ikään GDPR ja tiedonhallintalain mukaan tuomat uudistukset vaikuttavat merkittävästi. Linjausten myötä näitä koskevat ohjeistukset olivat kuitenkin selkeitä ja toimintaa ohjaavia ohjeistuksia esimerkkeineen löytyi reilusti. Äärimmäisen hyvinä malleina toimivat tiedonhallintalaista luodut tarkastuskortit, joissa yksityiskohtaisesti käytiin läpi pykälistä johdetut tarpeet tiedonhallintalain täyttymiseksi. Mitä pidemmälle kirjallisuuskatsaus eteni, tuli myös selkeä tarve haastatella tutkimuksen tilaajan tiedonhallinnasta ja kameravalvonnasta vastaavia tahoja. Haastattelujen avulla pystytään rakentamaan selkeä kuva siitä, miten uudistunutta lakia julkisen hallinnon tiedonhallinnasta on keretty implementoida käytäntöön. Teoriaosuudessa havaittiin ainakin, että kameravalvontaan liittyvät tietosuojaselosteet ovat niin Tampereella kuin useassa muussakin kaupungissa vanhan lain puolella tehtyjä. Lisäksi etenkin poliisin kanssa tehdyt rekisterinpidolliset käytänteet olivat kaupungeittain hyvin hajanaisia. Tietosuojavaltuutettu olikin tuoreessa päätöksessään (TSS 6610/182/18 2019) puuttunut poliisin ja Oulun kaupungin kameravalvontaa koskevaan sopimukseen ja rekisterinpitoon.

Kameravalvonnassa hyödynnettävien tekoälysovellusten määrä on kasvanut räjähdysmäisesti ja tulevaisuutta ennustavien raporttien pohjalta kuluva vuosikymmenen alku on alan läpimurron aikaa. Videokuvasta tehtävä konepohjainen laskenta ja analyysi ovat tulevaisuudessa niin robotiikan kuin tiedol-

la johtamisen kulmakiviä. Kirjallisuuskatsauksessa käsiteltiin tekoälysovellusten osalta perinteiseen videovalvontaan liittyviä sovelluksia ja kameroiden hyödyntämistä yhtenä sensorina paremman tilannekuvan luomiseksi. Rajaus tehtiin vastaamaan tilaajan tarpeita ja heidän tavoitteitaan SURE-projektin osalta. Esitellyt sovellukset olivat kameravalvontaa käyttävän henkilön työtä helpottavia sovelluksia. Teorian regulaatio-osuudessa havaittiin, että ohjelmistot, jotka käsittelevät erityisiä henkilötietoluokkia vaatisivat kokonaisuudessaan oman tutkimuksen. Näin korkean riskin aiheuttavaa tietojenkäsittelyä sivuttiin tekoälyä koskevassa teoriaisuudessa vain eettisyyden ja tekoälyn tehokkuuden kannalta. Kasvojentunnistuksen saralla on tehty paljon tutkimusta tekoälyn toimintaa tehostavasta vaikutuksesta. Tekoälyn onkin havaittu hyödyntävän merkittävästi niin materiaalin läpikäyntiä. Lisäksi tekoäly tehostaa selvästi ihmisen tekemää tunnistusta videovalvonnasta taltioidun henkilöllisyyden selvittämisessä. Havainto tukee tilaajan tavoitteita kehittää tekoälysovelluksia, jotta videomateriaalista tehtyjä havaintoja voitaisiin automatisoida tai tehdä materiaalista nopeammin käsiteltävää.

Kaikkia teorian puolelta esiinnousseita pääteemoja koskettava ja tilaajan erityisesti tutkimuksen aikana esiintuoma kokonaisuus oli kameravalvontajärjestelmän monipuolisen käytön mahdollisuus. Tällä tarkoitetaan sitä, että nykyisellään kaupungin yleisvalvontaan käytettäviä kameroita ja järjestelmään mahdollisesti liitoksissa olevia muita kameroita, voitaisiin hyödyntää monen tahon toimesta. Tahoina erikseen tuotiin esiin kaupungin omat tarpeet tapahtumaturvallisuuden, yleisen turvallisuuden ja kaupunkikehityksen saralla. Lisäksi järjestelmää pitäisi pystyä käyttämään niin poliisin kuin pelastuslaitoksen puolesta. Kirjallisuuskatsauksessa ratkaisuksi nousi yhteisrekisterinpito etenkin niiden tahojen osalta, joilla voi tulla tarve päästä käsiksi järjestelmän reaaliaikaiseen kuvavirtaan. Takautuvan materiaalin osalta toiminta voitaisiin järjestää rekisterinpidollisesti tietojenluovutuskäytännöin. Yhteisrekisterinpidossa jokainen taho vastaisi itse oman toimintansa vastuista ja velvollisuuksista. Nämä kirjattaisiin selkeästi tietosuojaselosteeseen ja käyttö perustuisi kunkin osapuolinen lailliseen käyttöperusteeseen. Kyseistä tutkimuksen osa-aluetta syvennetään vielä eri osapuolien kuin laillisuusvalvontaviranomaisen haastatteluilla.

6 TUTKIMUKSEN TOTEUTUS

Tässä luvussa käydään läpi tutkimuksessa käytetyt tutkimus- ja analyysimenetelmät. Tutkimuksessa hyödynnetään kolmea eri tutkimusmenetelmää: fenomenografia, grounded theory ja toimintatutkimus. Aineisto hankinnan metodeina hyödynnetään kirjallisuuskatsausta ja haastatteluita. Aluksi luvussa käydään läpi tutkimusstrategia ja tutkimuksen tavoite. Tämän jälkeen esitellään tutkimusmenetelmät sekä tutkimuksen metodologia, jossa avataan aineiston käsittelyyn ja analysoitiin käytetyt menetelmät. Lopuksi luvussa arvioidaan tutkimuksen luotettavuutta ja eettisyyttä.

6.1 Tutkimusstrategia

Tutkimuksen tarkoituksena on pyrkiä selvittämään regulaation pohjalta, millä tavoin Suomessa tekoälyä voidaan hyödyntää kameravalvonnassa. Koska kyseessä on todellisen elämän ongelman ratkaiseminen, toteutettiin tutkimus laadullisena eli kvalitatiivisena tutkimuksena. Kvalitatiivisen tutkimistyypin valinta on siltäkin osin perusteltua, että aihealuetta pyritään tutkimaan mahdollisimman laaja-alaisesti. Induktiivinen eli ongelman monitahoinen tutkimus, joka tässä tutkimuksessa toteutettiin erilaisina haastatteluina ja laaja-alaisena aineiston keruuna, mahdollistaa monen suuntaisten suhteiden löytymisen (Hirsjärvi, Remes & Sajavaara, 2009, s. 161-164).

Tutkimukseen osallistuu kaksi tutkijaa, jotka oman ammattitaitonsa ja työnsä puolesta tuntevat paljon kameravalvontaan liittyviä aihealueita. Tutkimuksessa hyödynnetään näin tutkijatriangulaatiota, jossa samaa ilmiötä tutkitaan useamman tahon toimesta. Molemmat tutkijat osallistuvat tutkimukseen koko prosessin ajan, mutta tutkimustyön osa-alueita kohdennetaan tutkijoiden oman ammattitaidon ja halun mukaisesti (Eskola & Suoranta, 1998, s. 69-70). Tutkijatriangulaatioon päädyttiin, koska yhteistyön uskotaan parantavan tutkimuksen onnistumisen mahdollisuutta. Tutkijoiden erilaiset näkökulmat ja yhteistyö mahdollistaa aiheen laajempialaisen asian tarkastelun, tutkimuksen

tilaajan määrittämässä tiiviissä aikataulussa. Lisäksi tutkijoiden ammatilliset yhteydet parantavat haastateltavien tahojen hankkimista ja kahden tutkijan avulla haastatteluja pystytään suorittamaan enemmän. Tämä edelleen rikastuttaa tutkimusta (Jokinen & Juhila, 2002, s. 109-118).

Tutkimuksen teoreettinen viitekehys jaetaan kolmeen laajaan aihealueeseen ja niiden alateemoihin. Teoreettista viitekehystä rajataan siten, että kameravalvonnan regulaatio jaetaan henkilötietoja käsittelevään ja kyberturvallisuuteen syventyvään osaa. Näiden lukujen osalta käsitellään ainoastaan Suomeen sidoksissa olevia instansseja. Suomessa lainsäädäntö ja valvontaviranomaisten toimintaan vaikuttavat kuitenkin myös Euroopan tasolla tehtävät asetukset ja päätökset. Näin ollen myös muualla Euroopan unionin jäsenvaltioissa käsiteltyjä tapauksia, mietintöjä kuin linjauksia sisällytetään teoreettiseen viitekehykseen. Kolmannessa aihealueessa tuodaan esille tekoälyn määritelmää ja sen mahdollisuuksia kameravalvonnassa. Tekoälyn eettinen käyttö sisällytetään myös yhtenä käsiteltävän alateemana tutkimukseen, koska sen vaikutus kameravalvontaan ja datan automaattiseen hyödyntämiseen herättää merkittävää julkista debattia (Koivisto, Leikas, Auvinen, Vakkuri, Saariluoma, Hakkarainen & Koulu, 2019, s. 17-18). Tämän vuoksi ohjelmistoja käyttävän tahon on pyrittävä toimimaan mahdollisimman läpinäkyvästi. Kirjallisuuskatsauksessa hyödynnetään lähteinä niin painettuja kuin sähköisiä teoksia ja artikkeleita.

Kirjallisuuskatsauksen jälkeen esiin tulleita asioita syvennetään haastatteluilla. Haastatteluissa hyödynnetään teoriapohjalta muotoiltua puolistrukturoitua teemahaastattelua (ks. liite 1-2) Teemahaastattelut jaotellaan haastateltavan asiantuntemuksen mukaisesti eri tutkimusalueisiin, keskittyen teoriaosuudessa käsiteltyjen aiheisiin. Teemahaastattelun etuna on mielipiteiden syventäminen ja selventäminen (Hirsjärvi ym., 2009, s. 205). Tutkimuksessa haastatteluilla halutaan saada tarkennuksia mm. kameravalvonnan regulaatioon sekä niistä tehtyihin tulkintoihin. Haastatteluihin valitaan oman alansa erityisasiantuntijoita, joiden asiantuntemus oli keskittynyt kameravalvontaa koskeville yksittäisille osa-alueille. Haastattelut toteutetaan yksilöhaastatteluina.

Alansa erityisasiantuntijoiden haastattelujen avulla pystytään tulkitsemaan kameravalvonnassa hyödynnettävän tekoälyn käytön rajoituksia ja mahdollisuuksia. Haastattelujen merkitys tutkimuksen luotettavuuden kannalta on merkittävä. Regulaation hajanaisuus ja siihen kohdistuvat uudet linjaukset aiheuttavat tutkimukselle tietynlaisen tutkimusteoreettisen puutostilan. Tämän vuoksi haastateltaviksi valittiin aihealueeseen sidoksissa olevia päättäviä viranomaisia sekä muita asiantuntijoita.

6.2 Metodologia ja tutkimusmenetelmät

Tutkimuksen tilaajan haluna on saada selvitys siitä, millainen regulaatio ohjaa kameravalvonnan käyttöä ja kuinka tämä ohjaa oikeellista toimintaa. Oikeus suorittaa kameravalvontaa ei ole sama asia kuin siitä määritetty laki tai asetus, koska lakia hyödynnetään tulkitsemisessa mitä saa ja ei saa tehdä. Lain kirjain

ei siis ole absoluuttinen tosi vaan pikemminkin ohjenuora siitä millä tavoin eri tilanteissa kuuluisi toimia. Lain kirjaimen tulkinnaksi tarvitseekin käsitellä voimassa olevia oikeuslähteitä ja pyrkiä perustelemaan niiden varassa toiminnan oikeellisuutta (Määttä, Tolvanen, Väätänen, Kolehmainen, Myrsky & Keinänen, 2012, s. 7). Kameravalvontaa ohjaa osaltaan sellaiset lait, joiden tulkinnasta on paljon tuomioistuimien ohjaavia päätöksiä. Tällaisia ovat esimerkkisi rikoslaki ja henkilötietolaki. Tästä huolimatta osa lainsäädännöstä on vanhaa ja epäkuranttia, koska uuden teknologian myötä mahdollisuudet ovat muuttuneet. Uudet lait ja linjaukset taas ovat vailla oikeusasteiden tulkintaa. Tämä aiheuttaa haasteita tulkita toimintaa ohjaavia määreitä siten, että toiminta olisi oikeellista. Uudet lait ja teknologia tekee kameravalvonnassa käytettävästä tekoälystä uuden vähän tutkitun ilmiön.

Toimintatutkimuksella pyritään ratkaisemaan todellisessa maailmassa esiintyviä käytännön ongelmia ja se vaatii yleisesti yhteistyötä tutkimuksen tilaajan kanssa. Toimintatutkimuksen avulla voidaan esimerkiksi ratkaista työyhteisössä esiintyviä ongelmia. Tutkimuksessa alkuvaiheessa toimittajan kanssa käytiin keskustelu, jossa tutkittavaa ongelmaa käytiin läpi. Keskustelussa tuli ilmi, että tilaajan oman hankkeen edistäminen on haasteellista, koska aiheeseen liittyvä säännöspohja on hajanainen. Keskustelun avulla tutkijat laativat tutkimuskysymyksen ja rajasivat tutkittavaa aihetta siten, että ongelmaan voidaan löytää ratkaisu. Tutkimuksen aikana tutkijat osallistuvat tilaajan järjestämiin tapahtumiin, jossa ensimmäisessä vaiheessa muotoiltuja ongelmia ja näkökulmia muokataan, mikäli se on tutkimuksen kannalta tarpeellista. Osallistuva yhteistyö on toimintatutkimukselle tyypillistä (Metsämuuronen, 2000, s. 28-31).

Grounded theory (myöhemmin GT) on menetelmällinen lähestymistapa, jonka avulla tutkimuksessa pyritään selvittämään kameravalvontaa koskevan vanhemman regulaation ja uusien lakien suhdetta käytännön tulkintaan ja todellisuuteen. Lisäksi tekoäly ilmiönä sidotaan kiinni tutkimuksen viitekehykseen (Hirsjärvi & Hurme, 2000, s. 164). GT alkaa aineiston keruulla, johon molempien tutkijoiden aihetta sivuava ammattitaito sidotaan mukaan. Näin voidaan tehokkaammin rajata laajaa ja hajanaista aineistoa tutkimustehtävän kannalta välttämättömäksi. Teoreettisen viitekehyksen kasaamiseksi käytetäänkin saturaation periaatetta, jolloin materiaalia kerätään siten, ettei kameravalvontaan liittyvää ja tutkimuskysymyksessä rajattuun alueeseen löydy enää uutta ainesta (Eskola & Suoranta, 1998, s. 62-63). Tutkimuksen eettisyyttä tarkasteltaessa on kuitenkin otettava huomioon tutkijoiden taustan vaikutus analyysin tuloksiin.

GT:n rakenteen mukaisesti aineiston kokoamisen jälkeen teoriaosuudessa havaitut teemat koodataan kategorioihin, joista ilmenee aineistoon liittyviä pääkäsitteitä tai ydinkategorioita. Relevantit ydinkategoriat ovat niitä, jotka selittävät isoimman osan tutkittavan aiheen vaihtelusta. Kun uusia luokkia ei enää löydy ja ydinkategoriat ovat saturoituneet, luodaan niiden pohjalta teemahaastatteluringot (Metsämuuronen, 2000, s. 24-25).

Fenomenografiaa hyödynnetään aineiston keruussa yhtenä tutkimusmenetelmänä, koska tutkimuksessa halutaan selvittää ihmisten erilaisia tulkintoja

kameravalvontaan liittyvästä regulaatiosta. Lain soveltajien tulee käyttää lain tulkinnassaan hyödyksi myös muita oikeuslähteitä. Tällaisia lähteitä ovat esimerkiksi lain valmisteluaineistot kuten hallituksen esitykset ja eri valiokuntien mietinnöt. Esitöiden lisäksi lain tulkintaa linjaa siitä tehdyt eri oikeusasteiden päätökset. Korkeimman oikeuden ennakkoratkaisut toimivat lain tulkinnassa, mutta nekin ovat itsessään tulkintaa (Määttä ym., 2012, s. 9). Fenomenograafisella analyysilla ilmiöön liittyvät hajanaiset tulkinnat ja käsitykset pyritään jalostamaan yhdeksi selkeäksi kokonaisuudeksi. Tutkimuksessa fenomenografista analyysia ei voida käyttää suorien vastausten antamiseen, mutta sen avulla ilmiön monihaaraiset tulkinnat ja lain merkitys voidaan tuoda esiin. Tutkijan tarkoituksena onkin onnistua tuomaan esiin ilmiön konteksti, jota haastateltavat erityisasiantuntijat tulkitsevat omasta käsityksestään (Metsämuuronen, 2000, s. 22).

6.3 Aiempi aihealueeseen liittyvä tutkimus

Uuden tutkimuksen toteuttamisessa on hyvä huomioida aiheeseen liittyvä aiemmin tuotettu tutkimus sekä muut aihealueeseen liittyvät analyysit. Valmiin aineiston käyttöä hyödynnetään tässä tutkimuksessa niin tutkimuksen viitekehyksen määrityksen ja tutkimuskysymysten hahmottamisen yhteydessä. Lisäksi tutkimusprosessin aikana valmiita aineistoja käytetään epäsuorasti siten, että niitä peilataan nykypäivään sekä uuden tutkimuksen tutkimusongelman ratkaisemiseksi (Hirsjärvi ym., 2004, s. 175).

Suoraan kameravalvontaan liittyviä alemman korkeakoulututkinnon opinnäytteenä tehtyjä hyvinkin rajattuja tutkimuksia löytyi useita. Näissä käsiteltiin pääosin tiettyyn yritykseen tai sijaintiin kohdistuvia kamera-asennuksia sekä kameravalvonnan hyödyntämistä rikostorjunnassa. Lisäksi hieman laajempia kameravalvonnan lainsäädäntöön liittyviä pro gradu töitä löytyi yksi kappale, joka on 10 vuotta vanha. Tämä tutkimus on osaltaan ollut pohjana myös yksityiselle puolelle toteutetussa kameravalvontaoppaassa. Tietyiltä osin tutkimuksiin liittyvät lakiosiot eivät esimerkiksi rikoslain puolelta ole muuttuneet. Uuden teknologisen kehityksen myötä lainvalmistelijoiden alkuperäinen lain näkemys ei kuitenkaan vastaa tämänhetkistä tilaa ja tarkoitusta.

Euroopan tasolla uusi tietosuoja-asetus (2016/679) on merkittävästi muovannut yksilöiden oikeuksia ja näin ohjaa myös osaltaan kameravalvontaa. Lisäksi julkiselle ja yksityiselle puolelle teetetty Euroopan komission mietintö henkilötietojen käsittelystä videolaitteiden kautta (EDPB 3/2019) linjaa osaltaan kameravalvontaa ja datan säilyttämistä.

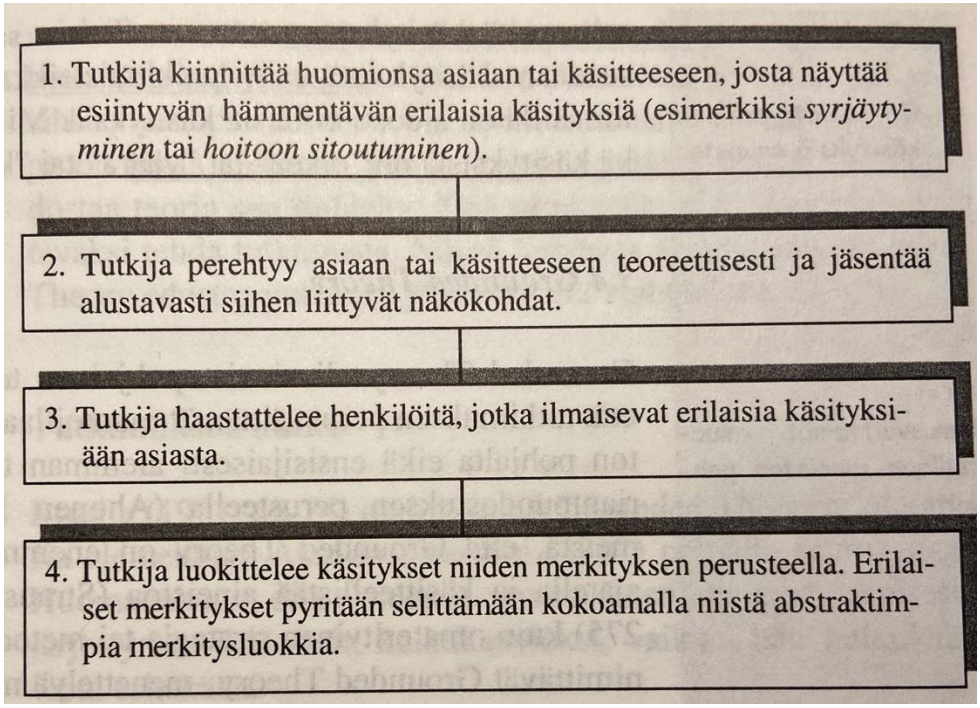
Suomessa tietosuoja-asetuksen soveltamisesta vastaa tietosuojavaltuutettu, joka on kannanotoissaan linjannut valvontakameroiden käyttöä ja niiden datan suhdetta tietosuojalakiin (1050/2018). Tietosuojalakia kuin tietosuojavaltuutetun kannanottoja käsitellään tutkimuksessa tutkimuskysymyksiin peilaten. Lisäksi aihetta tutkivaa kirjallisuutta kuten ”Henkilötietojen käsittely - EU-tietosuoja-asetuksen vaatimukset” (Hanninen ym., 2017) tarkastellaan syvälli-

sesti tutkimuksessa. Lapin yliopistossa tehty väitöskirja (Korja, 2016) biometristen tietojen hyödyntämisestä on laaja kokonaisuus, joka kuvaa hyvin biometristentietojen tietojen käsittelyn laillisuutta sekä näiden tietojen eri tyyppejä.

Tekoälyn osalta löytyy kohtuullisen paljon hyvinkin yksityiskohtaista tutkimusta siitä miten erilaisen algoritmit toimivat. Näiden käyttökelpoisuus on kuitenkin rajallista, koska tämän tutkimuksen päätarkoituksena ei ole tekoälysovellusten toimintaperiaatteiden perinpohjainen läpikäynti matemaattisella tasolla. Tutkimuksen fokus on enemmänkin selvittää perusteita tekoälysovellusten hyödyntämiseksi, jonka vuoksi algoritmien toimintaperiaatetta on avattu enemmän henkilötietojen näkökulmasta.

6.4 Haastattelujen runko ja eteneminen

Tutkimuksen suunnitteluvaiheessa oli jo selvää, että kirjallisuuskatsauksen avulla ei pystytä hankkimaan kaikkia tutkimuksen tavoitteeksi asetettuja tavoitteita. Kameravalvonnan osalta regulaatio ja siitä tehdyt tulkinnat olivat hajanaisia tai jopa suorastaan puutteellisia. Teemahaastattelujen käyttö olikin tutkimuksen osalta luontainen vaihtoehto, joka täydensi aineistonkeruussa tehtyjä havaintoja (kuvio 24). Kameravalvonnassa käytetystä tekoälystä tehtyjen tulkintojen erilaisuus ja puute myös tuki selkeästi sitä, että yhdeksi tutkimusmenetelmäksi valittiin fenomenografia (Metsämuuronen, 2000, s. 23).



KUVIO 24 Fenomenografisen tutkimuksen kulku (Metsämuuronen, 2000, s. 23)

Haastatteluihin valmistautuminen vaatii tutkijoilta huolellista esiselvitystyötä ja perehtymistä aiheeseen. Lisäksi haastattelijan pitää olla varovainen, ettei omat tulkinnat vaikuta haastateltavaan (Alastalo & Åkerman, 2010, s. 377). Kirjallisuuskatsauksessa kerätyn ja analysoidun materiaalin pohjalta luotiin liitteiden 1-2 mukaiset teemahaastattelurungot. Osaltaan kysymykset olivat suuntaa antavia, mutta tietyistä keskeisistä asioista, kuten henkilötietojen luokittelusta erityisiin henkilötietoihin, kysymykset olivat tarkoituksella hyvin yksityiskohtaisia. Osaltaan kysymykset olivat sidottuja tutkijoiden omiin tulkintoihin teorian pohjalta esiinnousseista asioista. Tämä tarkoitti sitä, että haastattelija esitti haastateltavalle eräänlaisen tapahtumakuvauksen, jonka pohjalta haastateltava tulkitsi ja teki päätelmän oman asiantuntemuksensa nojalla. Vaikka haastattelunkulku syntyy aina vuorovaikutustilanteessa, tutkijan on oltava tarkka, ettei kysymykset ole johdattelevia ja näin tutkija tarkoituksella saa haluamiaan vastauksia (Alastalo & Åkerman, 2010, s. 377-381). Kysymysten osalta tutkijat tarkkaan harkitusti jättivät haastateltavalle mahdollisuuden tehdä asiasta oman tulkinnan tapahtumankuvauksen perusteella. Kysymyksiin ei liitetty omaa näkökulmaa vaan, ne oli rakennettu vastaamaan tilaajan reaalimaailman ongelmaa. Vastausten jälkeen haastateltavan kanssa käytiin vuoropuhelua tulkinnan perusteista kuin siitä millä tapaa haastattelija oli tulkinnut asiaa. Asiantuntijahaastattelussa yhteistyön avulla on mahdollista tarkastella tutkittavaa aihetta ja yksittäisiä seikkoja kriittisesti (Alastalo & Åkerman, 2010, s. 389-392). Tutkimuksen lähtökohtana oli, ettei tietyistä aihealueista ollut olemassakaan suoria vastauksia, jonka vuoksi vuorovaikutteista haastattelutapaa oli käytettävä.

Haastateltavaksi valittiin kaikkien kolmen pääteemojen mukaisesti, niin henkilötietojen käsittelyn, tietosuojan kuin tekoälyn saralla päätyönään toimivia erityisasiantuntijoita. Yhteensä tutkimuksessa haastateltiin 10 asiantuntijaa. Haastateltaviin oltiin henkilökohtaisesti yhteydessä, jonka yhteydessä heille kerrottiin haastattelun tarkoitus ja eettiset pelisäännöt. Lisäksi heti haastattelun sopimisen jälkeen haastateltaville toimitettiin sähköpostilla haastatelurunko ennakkotutustumista varten. Haastattelut toteutettiin 23.4. - 10.5.2020 ja ne olivat kestoltaan 35min - 1h15min. Haastattelut jouduttiin suorittamaan täysin etänä videon välityksellä vallitsevan poikkeustilan takia. Ennen haastattelun aloittamista kerrattiin tutkimuksen eettisen pelisäännöt ja kysyttiin suostumus ammatin hyödyntämiseksi. Haastateltavien anonymiteetin suojelemiseksi tutkimuksessa heistä käytetään koodinimiä H1-H10 (taulukko 1).

TAULUKKO 1 Haastatellut asiantuntijat ja heidän tittelinsä

Tunnus	Titteli
H1	Ylitarkastaja
H2	Apulaistietosuojavaltuutettu
H3	Tietosuojavastaava
H4	Poliisitarkastaja
H5	Projektipäällikkö

H6	Lakimies
H7	Myyntipäällikkö
H8	Tietosuojapäällikkö
H9	Riskienhallintapäällikkö
H10	Tietosuojavastaava + Turvallisuuspäällikkö

Teemahaastattelut nauhoitettiin ja toimitettiin tutkijoille salattuun pilvipalveluun, joka oli Jyväskylän yliopiston tarjoama OneDrive alusta. Haastattelut olivat jaettu puoliksi siten, että kumpikin tutkija haastatteli viisi henkilöä. Teemahaastatteluja ei kokonaisuudessaan tarvitse litteroida, vaan haastattelun osia voidaan tuoda esille tutkimuksessa (Hirsjärvi & Hurme, 2000, s. 138). Haastatteluja ei litteroitu, mutta molemmat tutkijat kävivät nauhat läpi ja niiden tuloksia käsiteltiin tutkijoiden kesken yhteisissä palavereissa. Haastatteluista fenomenografian avulla tulkitut päätelmät tuotiin osaksi tutkimusten tuloksia. Haastatteluiden tulkinnat erotettiin toisistaan tunnuksilla H1-H10.

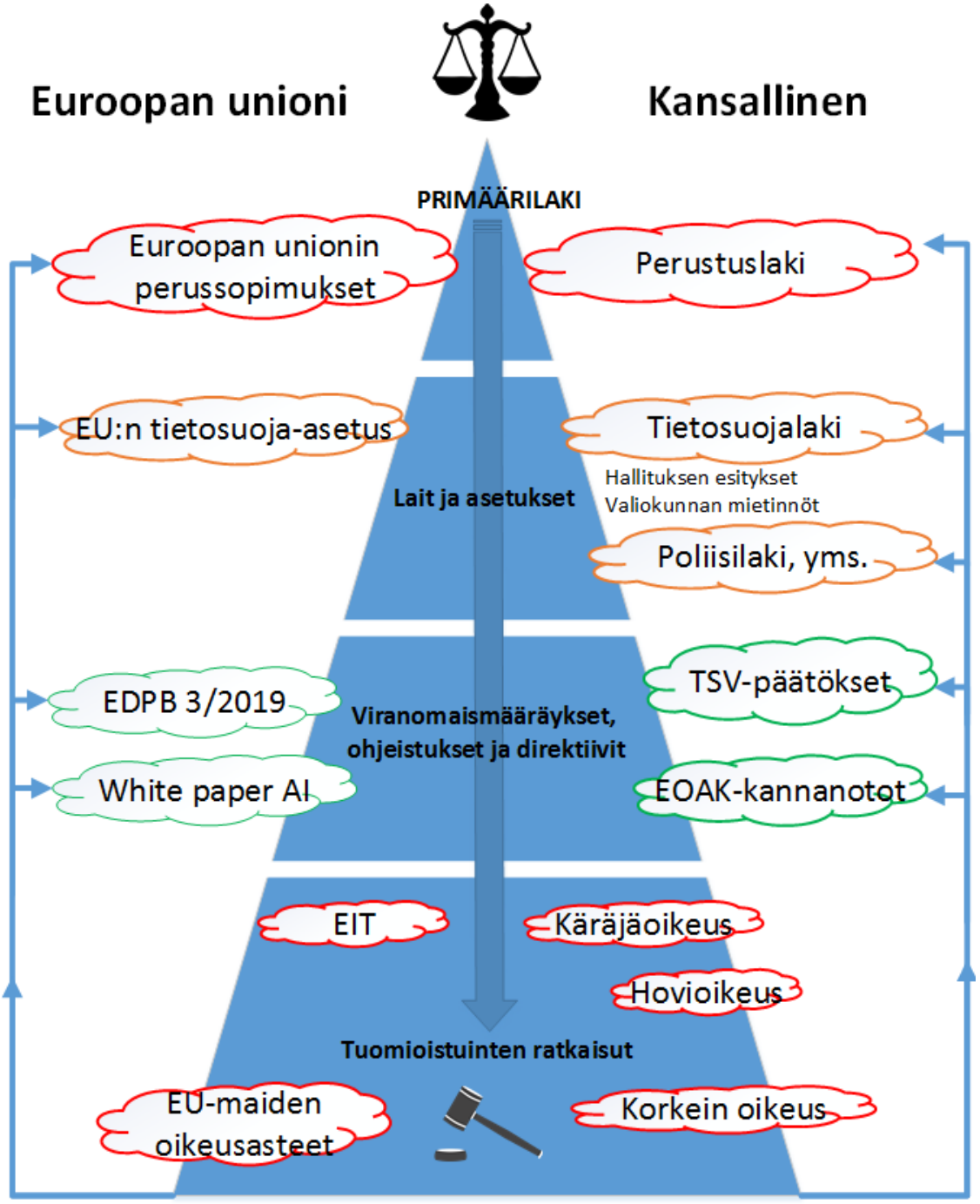
Tutkimuksen tilaajan toivomuksena oli saada yhteenveto kameravalvonnassa käytettävän tekoälyyn liittyvästä regulaatiosta ja miten se vaikuttaa järjestelmään käyttäviin tahoihin. Tutkimuksessa hyödynnetyn teorian ja siitä jatkettujen haastattelujen avulla luotiin kolmen pääkategorian osalta tuloksia tukevat visuaaliset hahmotelmat. Näiden avulla tilaajalle tuodaan helposti ja tiivistetysti esille tutkimuksessa havaitut kameravalvontaan ja tekoälyyn liittyvät merkitykselliset seikat. Lisäksi tuloksissa avataan tarkemmin haastatteluiden analysointia. Tutkimuksen pohjalta luodaan myös tilaajalle tekoälyä koskeva kameravalvontaopas. Tätä osuutta ei liitetä tämän tutkimuksen yhteyteen, koska oppaaseen liittyy salassapitoa koskevia asioita.

7 TUTKIMUKSEN TULOKSET

7.1 Kameravalvontaan liittyvä regulaatio

Kameravalvonta ei ole vuosien varrella muuttanut luonnettaan, vaan se on edelleen luontainen osa kokonaisturvallisuutta yhä useammassa yrityksessä tai organisaatiossa. Lisäksi sitä hyödynnetään yleisesti esimerkiksi toiminnan ohjauksessa tai erityyppisten suunnitelmien tukena. Järjestelmien ylläpito ja huolto on usein yksityisen sektorin toimijoiden kuten vartiointiliikkeiden vastuulla, kun loppukäyttäjänä voi olla esimerkiksi julkisen sektorin viranomainen tai jokin muu taho. Kameravalvontajärjestelmistä sekä niiden käyttäjistä tai käyttäjäyhdistelmistä on monenlaisia variaatioita. Suomessa yksityisellä ja julkisella sektorilla regulaatio hieman poikkeaa, kun puhutaan lainsäädännöllisistä vaatimuksista liittyen kameravalvontajärjestelmiin. Viranomaisilla on vielä tämän lisäksi omia erityislainsäädäntöjään, jotka ohjaavat viranomaistoimintaa toimivaltaperusteisesti. Kameravalvonnasta ei oikeastaan voi puhua ilman, että siihen liittyy tietosuoja ja henkilötiedot tavalla tai toisella. Kuva tai ääni, josta henkilö on tunnistettavissa täyttävät henkilötiedon määritelmän. Vasta anonymisoimalla tiedot, niitä ei käsitellä enää henkilötietoina. Henkilötietojen käsittelyyn kantaa ottava lainsäädäntö on tällä hetkellä erittäin hajallaan, sillä tietosuojasta säädellään yli 600 laissa. Käytännön tasolla Suomessa tietosuojan soveltamista ovat ohjanneet tietosuojavaltuutetun kannanotot, lausunnot ja päätökset, muut viranomaiset sekä tuomioistuimien ratkaisut. Tietosuojavaltuutettu onkin ollut tärkeässä roolissa, sillä tuomioistuimien päätöksiä erilaisiin tilanteiseen löytyy niukasti. Euroopan Unionin jäsenvaltiona Suomen lainsäädäntöä ohjaa myös EU:n yhteisölainsäädäntö. Euroopassa henkilötietojen käsittelystä on säädelty GDPR:ssä, joka onkin lähes kaikkea tietosuojalainsäädäntöä ohjaava asetus, johon monet kansalliset lainsäädännöt nojaavat tietosuojan osalta. Regulaatiolla pyritään auttamaan yrityksiä ja organisaatioita toimimaan ny-

kyaikaisessa digitaalisessa ympäristössä. Sillä edistetään myös henkilötietojen turvallista käsittelyä ja kansalaisten luottamusta digitaaliseen maailmaan. Kuvassa (kuvio 25) hahmotellaan Euroopan unionin ja suomen kansallisen tason regulaation hierarkiaa.



KUVIO 25 Kameravalvontaan liittyvän regulaation visualisointi

Tämän tutkimuksen yhtenä alatutkimuskysymyksenä oli tutkia mitä regulaatiota liittyy Suomessa suoritettavaan kameravalvontaan. Tutkimuksessa on keskitytty olennaisimpaan kansalliseen ja kansainväliseen lainsäädäntöön kamera-

valvonnan näkökulmasta. Suomessa regulaatio jakautuu kolmeen osaan toimijoiden kesken. On olemassa yksityis-, julkis- ja viranomaissektorin toimijoita. Tähän lukuun on lisätty asiantuntijoiden teemahaastatteluista kommentteja tukemaan kirjallisuuskatsauksesta tehtyjä havaintoja. Lainaukset näkyvät tutkimuksen tekstissä sisennettynä ja pienemmällä fontilla sekä taulukon 1 mukaisin haastatellun tunnuksella.

> H8: Henkilötietojen käsittelyyn sovelletaan sekä yksityisen, julkisen että viranomaisten toiminnassa Europan unionin tietosuoja-asetusta ja se tulee kaikkien toimialojen henkilötietojen käsittelyyn sovellettavaksi. Sieltä löytyy periaatteet mitä tulee noudattaa. Asetus on väline- ja teknologianeutraali eli se soveltuu siitä huolimatta millä tavalla henkilötietoja kerätään.

> H6: Regulaatio ei ehkä ole riittävän selkeätä tällä hetkellä, siten toki, että liittyy henkilötietokokonaisuuteen. On kuitenkin olemassa myös osa-alueita kuten esimerkiksi IoT, jossa se ei välttämättä ole kristallisen kirkasta, siellä tulee kuitenkin myös ottaa huomioon, että sovelletaanko tähän samoja säädöksiä. Jossain välissä tulee kohta, missä rajaa näiden välillä vedetään. Suoraviivaista sapluunaa on vaikea tehdä, vaan tapaukset on arvioitava tapauskohtaisesti. En kuitenkaan näe tarvetta laintasoiselle sääntelylle, koska nykylainsäädännöstä löytyy kyllä vastauksia mutta jonkinlainen toimeenpano-ohjaus voisi olla paikallaan.

Yksityisen sektorin toimijoiden toimintaa tietosuojan parissa säädellään GDPR:n ja kansallisen perustus- sekä tietosuojalain mukaisesti. Henkilötietojen käsittelyperusteet pohjautuvat GDPR:n 5. artiklaan, joka sisältää periaatteita, laillisen käsittelyn perusteita ja yleisesti käsittelyn oikeuksista sekä velvollisuuksista. Tietoturvallisuuden osalta rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava GDPR:n 32 artiklan asianmukaiset tekniset ja organisatoriset toimenpiteet:

- Henkilötietojen pseydonymisointi ja salaus
- Kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus
- Kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa
- Menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi

Yksityisiä ja muita julkisia toimijoita kuin viranomaisia, ei rajoita toimivaltaperusteet, vaan heidän toimintansa pohjautuu tarkoitusperusteeseen ja siihen missä sekä minkä vuoksi henkilötietoja käsitellään. Turvallisuuspalveluita ostetaan julkisten toimijoiden tarpeita täyttämään monesti yksityisen puolen toimijoilta, kuten esimerkiksi vartiointiliikkeiltä. Vartiointiliikkeet voivat tuottaa kaupungeille monenlaisia palveluita. He voivat toimia suorittajina esimerkiksi tila-, henkilöstö- tai tapahtumaturvallisuuteen liittyvissä tapauksissa. Julkis- tai viranomaissektorin toimijalle palveluita tuottaessaan yksityisen sektorin toimi-

joiden tulee noudattaa julkisen ja viranomaissektorin toimijoiden regulaatioon perustuvia vaatimuksia, mikäli järjestelmän ja tietojen omistaja on joku muu kuin yksityisen sektorin toimija. Tällaisesta palvelun tuottamisesta sovitaan toimijoiden kesken usein kirjallisella sopimuksella tai vastaavalla tavalla muun muassa henkilötietojen käsittelystä. Sopimuksessa on oltava yksityiskohtaisesti kuvattu mistä asioista sopimuksessa sovitaan.

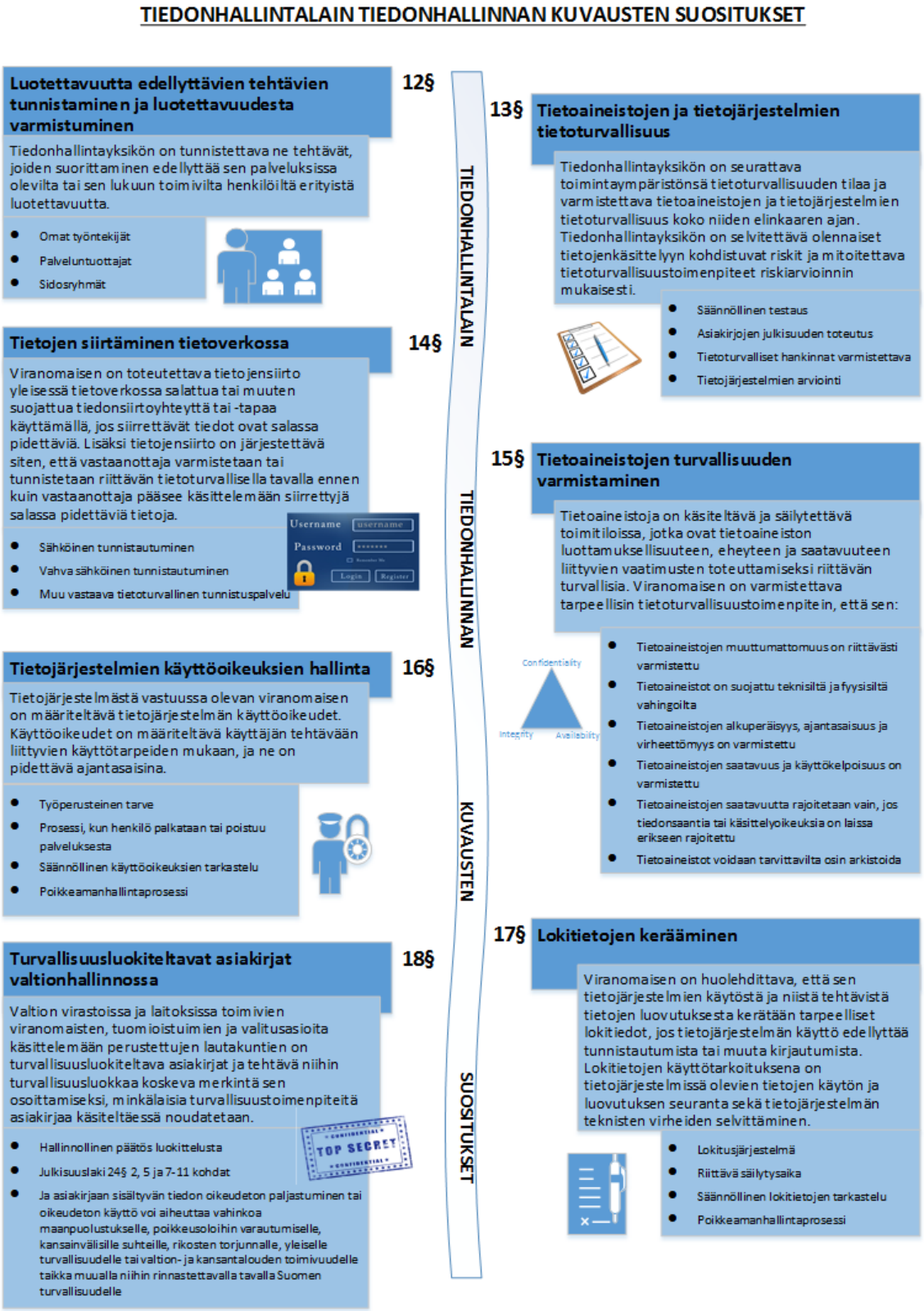
Julkisen sektorin toimijoita sitoo yksityisen sektorin tavoin kansallisen lainsäädännön puolelta perustuslaki ja tietosuojalaki sekä kansainvälisesti EU:n tietosuoja-asetus GDPR. Henkilötietojen käsittelyä koskevien periaatteiden, turvallisuuden ja käsittelyn lainmukaisuuden lisäksi julkisen sektorin toimijoiden osalta sovellettavaksi tulee laki julkisen hallinnon tiedonhallinnasta ja neljännen luvun pykälät 12§ - 18§ tietoturvallisuudesta (kuvio 26), jotka edellyttävät:

- Luotettavuutta edellyttävien tehtävien tunnistamista ja luotettavuudesta varmistumista
- Tietoaineistojen ja tietojärjestelmien tietoturvallisuuden varmistamista
- Tietojen siirtämistä tietoverkoissa salaamalla tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä
- Tietoaineistojen turvallisuuden varmistamista
- Tietojärjestelmien käyttöoikeuksien hallintaa
- Lokitietojen keräämistä
- Turvallisuusluokittelun suorittamista ja merkinnän tekemistä

> H10: Varsinkin ns. Smart City-teemassa on tärkeä määritellä, kuka on rekisterinpitäjä ja kuka oikeasti omistaa tiedon. Ne ovat todella oleellisia kysymyksiä, eikä mitään helppoja sellaisia.

Toimialasta huolimatta, erityisen tärkeäksi koetaan, että heti kameravalvontajärjestelmän suunnittelu- ja hankintavaiheesta alkaen osataan ottaa riittävästi huomioon tietosuojan lisäksi myös tietoturvallisuus. Lainsäädännön ja muun regulaation vaikutukset ovat laajat. Ne myös tuovat mukanaan eritasoisia riskejä sekä laajoja vaikutuksia, jotka pitää kyetä hahmottamaan järjestelmän tarkoituksenmukaisen käytön tukemiseksi. Näiden lisäksi vielä toimittajat tarjoavat yleensä niitä tuotteita, mitä on nopeasti saatavilla ja valmiina varastossa. Hankintavaiheeseen on syytä kiinnittää erityistä huomiota. Tämä on valitettavan monella toimijalla vaihe, joka jää välistä.

> H10: Hankintavaihetta ennen ja oikeastaan hankinnan suunnitteluvaiheessa pitäisi tehdä ns. tarkoituksenmukaisuusmäärittely, jolla otetaan kantaa huomioon otettaviin asioihin. Määrittelyssä otetaan kantaa mm. millä tekniikalla, minkälaisilla rajoitteilla ja mitä ylipäänsä järjestelmältä halutaan. Lisäksi siinä kuvataan mitä järjestelmällä valvotaan ja millä tavalla.



KUVIO 26 Hahmotelma kameravalvontajärjestelmän tiedonhallinnasta lakiperusteisesti

Viranomaissektorin toimijoilla julkisen sektorin vaatimusten lisäksi tulee toimivaltaperusteet ja erityislainsäädäntö, jotka ohjaavat toimintaa perustuslain, tie-

tosuojalain ja EU:n tietosuoja-asetuksen lisäksi. Esimerkiksi poliisin toimintaa edellä mainitun lainsäädännön lisäksi henkilötietojen käsittelyssä ohjaa laki henkilötietojen käsittelystä poliisitoimessa ja laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä. Kameravalvontajärjestelmän yhteisrekisterinpidon osalta on syytä pohtia voivatko osapuolet käyttää viranomaisen käyttöperusteita ja tarvesidonnaisuutta tietojen käsittelyyn. Yhteisrekisterinpidon vastuista ja velvoitteista tulee sopia GDPR:n 26. artiklan mukaisesti läpinäkyvästi ja yksityiskohtaisesti. Järjestelyistä on käytävä asianmukaisesti ilmi todelliset roolit ja suhteet rekisteröityihin nähden.

> H8: Koen, että pitää olla henkilötietojen käsittelyyn liittyvää asiantuntemusta, kykyä tunnistaa mikä on konteksti ja tilanne, minkä äärellä ollaan. Tämä avulla osataan ottaa käyttöön oikeat työkalut, lähteä etsimään esimerkiksi erityislainsäädäntöä ja huomioida tietosuoja-asetuksen periaatteet. Välttämättä ei ole yhtä eksaktia lakia ja pykälää minkä nojalla mennä, vaan pitää ymmärtää lainsäädännön viitekehys ympärillä ja sovittaa toimintatapa siten, että kaikki edellytykset täyttyvät.

> H10: Jos ajatellaan että järjestelmä on moniviranomaiskäytössä, jossa eri viranomaisilla on eri toimivaltuuksia. Järjestelmän osalta pitää tarkkaan kuvata, että mihin tarkoitukseen kukin viranomainen sitä käyttää ja kuinka sitä valvotaan. Tässä muodossa järjestelmän käyttö voi sisältää merkittäviä riskejä. Rekisterinpitäjällä pitää olla tiedossa kamerakohtaisesti järjestelmäkuvaus.

Eettiset kysymykset hyödynnettävyydestä ja kyvyistä nousevat aika ajoin esille. Ihmisten suhtautuminen kameravalvontaan ja tekoälyyn on yleisesti ottaen varovaisen positiivista ja terveen kriittistä. Kameravalvontaa ja tietosuojaa säätelevän lainsäädännön tarkoituksena on muun muassa herättää ihmisten luottamus käytettävään uuteen teknologiaan. Sitä nykylainsäädäntö, useamman sadan lain myötä, ei valitettavasti edesauta. Voidaankin ihan asiallisesti esittää kysymys siitä, että pitäisikö kameravalvonnalle ja tekoälylle olla oma spesifinen lainsäädäntönsä. Tällä nimenomaan voitaisiin lisätä ymmärrettävyyttä ja läpinäkyvyyttä käytettävistä kyvyistä kansalaisten silmissä.

Ei siis ole mikään ihme, että suhtautuminen on ristiriitaista jopa globaalisti. Viimeisin vedenjakaja kameravalvonnan osalta on ollut kasvojentunnistusteknologian käyttäminen. Biometrisia tietoja pidetään arvossa arvaamattomassa, kun pohditaan mihin tulevaisuuden laskentakyky, koneoppiminen ja tekoäly muiden ominaisuuksiensa avulla voivat kyetä. Osa valtioista, kuten esimerkiksi Iso-Britannia sallii teknologian käytön oman lainsäädäntönsä puitteissa, kun taas esimerkiksi Yhdysvalloissa teknologia on jo kielletty osissa osavaltioita. Suomessa kasvojentunnistukseen liittyvä tietosuoja on tiukasti säädelty, eikä sen valvovan viranomaisen tietosuojavaltuutetun tulkinnan mukaan kasvojentunnistusteknologian käyttö ole mahdollista kuin tiukasti rajatuissa ympäristöissä ja tietyillä käyttöperusteilla. Tuomioistuinten päätöksiä erilaisista tapauksista ei myöskään ole riittävästi saatavilla tällä hetkellä, jolla toimintaa voitaisiin ohjata oikeaan suuntaan. Yritykset ja toimijat eivät uskalla käyttää kaikkia toiminnallisuuksia esimerkiksi kameravalvonnassa, koska sanktiot väärinkäytöksistä ovat suuria.

Valvonta on äänteeltään ja tulkinnallisesti ehkä hieman negatiivinen sana, joka kognitiivisesti aiheuttaa ihmisessä luontaisen vastareaktion. Päättäjien olisi kuitenkin aiheellista tarkastella myös, miten uusia kykyjä voitaisiin parhaalla mahdollisella tavalla hyödyntää. Sen avulla voidaan saavuttaa uusia vallankumouksellisia kykyjä usealla eri alalla. Tämä edellyttäisi avoimia ja läpinäkyviä sekä samalla tiukasti ja yksityiskohtaisesti kuvattuja dokumentteja teknologian käytöstä sekä muita lakisääteisiä toimenpiteitä. Pääsy tietoihin pitäisi hallinnollisesti, fyysisesti ja teknisesti rajata työtehtäväperusteisesti ja siten, ettei sen väärinkäyttö olisi mahdollista tai ainakin se olisi erittäin vaikeaa. Varautuminen on suomalaisessa yhteiskunnassa luontaista ottaen huomioon historiamme. Onko se tarpeellista vai yliarvioidaanko teknologian kykyjä tässä tilanteessa, on toinen kysymys. Voimmeko saavuttaa teknologisen potentiaalin nykylainsäädännöllä on yhtä aiheellinen kysymys kuin se, että tarvitaanko tekoälyyn perustuvaa teknologiaa lainkaan. Oikein säädeltynä teknologialla voisi olla usealla toimijalla valtavia vaikutuksia. Toiminnanohjauksessa, suunnittelussa, tilastoinnissa, jatkuvuudenhallinnassa sekä varautumisessa hyödynnetään nyt jo tekoälyä. Viranomaisille tekoälyllä avustettu kameravalvonta voisi osoittautua erittäin hyödylliseksi. Nähtäväksi jää, kuinka tulevaisuudessa tekoälyn ja kameravalvonnan potentiaalia hyödynnetään Suomessa eri aloilla.

H5: Tällä hetkellä kameravalvontaan kohdistuva regulaatio on äärimmäisen sekavaa. Tämä johtaa helposti siihen, että enemmin jätetään asia tekemättä, koska pelätään rikkovan säädöksiä. Kameravalvonnalla on kaupunkiympäristössä merkittävä turvallisuutta lisäävä vaikutus etenkin rikosten selvittämisen kannalta.

H8: Lainsäädännön riittävä selkeys on hankala kysymys. Mitään yksiselitteistä vastausta ei voi antaa. Tapaukset pitää arvioida aina case by case, että mitä ollaan tekemässä ja mihin tarkoitukseen tai kuka ylipäätään toteuttaa kameravalvontaa. Onko se esimerkiksi viranomainen. Suhteutetaanko kameravalvonta viranomaisen toteuttamana työntekijöihin vai onko se viranomaisen omaisuuden valvontaan. Nämä määrittelevät sen mikä on käsittelyn oikeusperusta eli mikä oikeuttaa keräämään kameravalvonnan avulla tietoja.

7.2 Kameravalvonnasta muodostuvat henkilötiedot

Lähtökohtaisesti kameravalvonnan tuottamat tiedot ovat aina henkilötietoja, jos henkilö on niistä kuvan tai äänen perusteella tunnistettavissa joko suoraan tai välillisesti.

H4: Esimerkiksi tieliikennekameroita ei välttämättä tällä hetkellä pidetä henkilörekisterinä, koska sieltä ei muodostu sellaista kuvamateriaalia, josta henkilöä tai rekisterikilpeä ei voida tunnistaa. Kameravalvonnasta ei näin tarvitse ilmoittaa, jolloin henkilö ei tiedä joutuvansa kameravalvonnan kohteeksi. Jos kameroiden tarkennusominaisuutta käytetään tai niihin yhdistetään muita esimerkiksi viranomaisen tietoja, voi niistä helposti muodostua henkilötietoja. Mielestäni myös näistä kameroista olisi hy-

> vä ilmoittaa kyltein aivan samaan tapaan kuin muista kaupungin yleisvalvontaan tarkoitetuista kameroista.

Videovalvonnan yleinen tarkoitus on tunnistaa tai selvittää tapahtunut teko tai tapahtuma. Tekoälyn avulla järjestelmistä pyritään tekemään vielä entisestään proaktiivisempaa, jolloin tapahtumiin reagointi olisi nopeampaan. Etenkin valvontakamerajärjestelmien osalta, joissa tietojen luovutuksen tai rekisterinpidon puolelta poliisi toimii kumppanina, järjestelmän perimmäinen tarkoitus on henkilön tunnistaminen. Poliisi voi vielä erityislainsäädäntönsä nojalla rikastaa kameravalvonnasta saatuja tietoja muilla tiedoilla, mikä entisestään vahvistaa tunnistamistarkoitusta järjestelmän käytön perusteena. Henkilötietojen käsittely vaatii aina rekisterinpidollisia toimia. Poikkeustapauksissa tietosuojaselostetta ei tarvita, jos kameran kuvauksesta ei muodostu henkilötietoja. Esimerkiksi tehtaan linjastolla kuvattavien esineiden laadunvalvonta ei ole henkilötietoja muodostavaa kameravalvontaa. Mikäli samaan järjestelmään on liitetty tehtaan yleisille paikoille sijoitettuja, kulunvalvontaan tai fyysiseen turvallisuuteen tarkoitettuja kameroita, järjestelmässä käsitellään henkilötietoja. Toki käyttötapausten ja teknisten rajausten avulla voidaan jakaa käyttöä siten, että järjestelmää voi käyttää taho, joka ei työssään saa henkilötietoja käsitellä.

> H4: GDPR on tuonut asetuksena alalle toivottua säätelyä, mutta edelleen omaa erityislakia ja säätelyä olisi paikallaan. Tekoälyn osalta lainsäädäntö ei kuitenkaan saattaisi pysyä perässä ja aiheuttaisi enemmän ongelmia kuin antaisi ratkaisua. Kuitenkin jotkut raamit olisi hyvä antaa, jotta toiminta ei olisi niin hajanaista etenkin yksityisellä sektorilla. Materiaalin käytöstä pitäisi myös säädellä tarkemmin, jotta myös rikoksen uhrin oikeudet toteutuisivat. Näin liike voisi myös itse hyödyntää materiaalia esim. sarjanäpistelijöiden estämiseksi, joihin poliisi ei voi resurssien vuoksi reagoida.

> H1: Kameravalvonnan osalta toivoisin enemmän pehmeitä normeja ja toimialasäännöstöjä sekä eettisiä ohjeita, kuin kankeaa erityistä lainsäädäntöä. Itsesääntelyn kautta pystyttäisiin paljon tehokkaammin saamaan ratkaisuja hyvinkin yksityiskohtaisiin ongelmiin. Se loisi alalle vallitsee toimialasäännöstöä, johon voisi tukeutua myös oikeuskäsittelyissä.

Tekoälyn tuottamat laskennalliset mallit (hash) eivät itsessään ole varsinaisesti henkilötietoja. Normaalisti niitä kuitenkin käytetään tunnistustarkoituksessa kameravalvonnan yhteydessä ja niitä hyödynnetään videodatan käsittelyyn. Näin laskennalliset mallit perivät videodatan henkilötietomääritelmän, etenkin jos videodata on sellaista, mistä henkilön tai siihen liittyviä asioita voi tunnistaa. Henkilötiedot ovat GDPR:ssä määritetty ns. tavallisiin henkilötietoihin ja erityisiin henkilötietoluokkiin. Tärkeää on huomioida, että videovalvonta itsessään ei muodosta erityisiä henkilötietoluokkia. Tällä tarkoitetaan sitä, että järjestelmään taltioitu videovirta tai tunnistettava kuva ei muodosta biometrista tietoa. Vasta siinä vaiheessa, kun esimerkiksi tekoälyn keinoin videodata muutetaan laskennalliseen muotoon, siitä tietyissä tapauksissa muodostuu GDPR:n artikla 9 mukaisesti erityisiä henkilötietoja. Yleisenä linjauksena voidaan pitää sitä, että jos henkilöä yksilöiviä fysiologisia piirteitä muutetaan matemaattisesti haettavaan

muotoon, syntyy erityinen henkilötieto. Tiedon muodolla ei ole merkitystä eli jos tieto ei ole ihmisen ymmärrettävissä se on silti biometrinen tieto, koska se on tietyn algoritmin avulla kohdistettavissa yksilöityyn henkilöön.

> H2: Kameravalvonnassa hyödynnettävät tarkoitetut tekoälyntuottamat laskennalliset mallit eivät itsessään ole henkilötietoja, silloin jos niiden tarkoituksena ei ole yksilöllisesti tunnistaa henkilöä. Kasvontunnistus on erityisten henkilötietoluokkien käsittelyä, mutta hahmontunnistus ei sitä ole, jos laskennalliset mallit luodaan henkilön vaatetuksen, sukupuolen tai jonkin muun vastaavan tiedon pohjalta eikä niiden avulla voida tunnistaa henkilöä.

Nykyisten tekoälysovellusten hahmontunnistukseen tarkoitetut toiminteet kuitenkin aiheuttavat vielä tulkinnannanvaraisen ongelman. Tämä johtuu siitä, että järjestelmää käyttävän tulee tarkasti selvittää mihin tietoon perustuen hahmontunnistusta tehdään. Sovelluksen toimintalogiikka pitää vaikutustenarvioinnissa avata äärimmäisen selkeästi. Ihmishahmosta voidaan luoda hahmontunnistuksessa sellaisia matemaattisia vektoreita, jotka hyödyntävät henkilöä yksilöiviä ominaisuuksia. Esimerkiksi henkilön vartalon mitat, kasvonmuodot tai kaikkien tietojen yhteen sovitettu malli voidaan tulkita joko biometriseksi tai ei biometriseksi. Hyvin avatun esiselvityksen nojalla hahmontunnistuksen käyttö on mahdollista. Toki asiasta on suotava hakea kannanotto myös tietosuojavaltuutetulta. Oikeassa maailmassa henkilön vartalon mittojen mukaan tehtävä hahmontunnistus ei periaatteessa tuottaisi henkilö yksilöivää biometrista tietoa missään olosuhteissa. Kameroiden kulmat, henkilön vaatetus ja sääolosuhteet vaikuttaisivat vertailukuvaan niin vahvasti, että täysin yksilöivän laskennallisen mallin luominen olisi mahdotonta. Tästä huolimatta tulee selvittää tarkasti, mitä järjestelmä hahmontunnistuksessa hyödyntää ja mihin seikkoihin algoritmin tekemä tunnistus perustuu. Mikäli tunnistuksessa hyödynnetään perinteisiä henkilötietoja, kuten sukupuolta, ihon- tai tukanväriä, vaatetusta tai tällaisten tietojen yhteissummaa laskennalliset mallit eivät ole biometrisia erityisiä henkilötietoja.

> H7: Modernit kameravalvonnan analysointityökalut ovat osittain ongelmallisia. Vaikkei järjestelmässä olisikaan kasvorekisteriä, niin pystyt silti tiettyä yhtä henkilöä hakemaan tallennushistoriasta. Sitten punnitaan, onko se biometrista tietoa vai ei.

> H1: Jos hakeminen tapahtuu yleisillä hakukriteereillä, kuten vaatetuksella tai sukupuolella, millä henkilöä ei suoraan pysty identifioimaan, niin silloin ei tehdä biometriseen tietoon pohjautuvaa tietojenkäsittelyä.

Tekoälysovelluksissa on myös mahdollista tehdä hakuja järjestelmään syötetyn kuvan perusteella tai videonauhalta taltioidusta kuvakaappauksesta. Tätä toiminnetta hyödynnettäessä tulee jälleen kerran pystyä tarkoin perustelemaan mihin tietoon pohjautuen laskennallinen malli luodaan. Jos siinä käytetään henkilön yksilöiviä fysiologisia piirteitä, käsitellään erityisiä henkilötietoluokkia. Mikäli kuvasta hyödynnetään normaalisti samoissa ohjelmissa käytettyjä

suodatusominaisuuksia kuten, objektien väriin tai vaatetukseen liittyviä attribuutteja, kuvalla hakeminen pysyy perinteisten henkilötietojen käsittelynä.

Eräänlaisena poikkeuksena henkilötietoluokittelussa kameravalvonnan osalta toimii poliittiset mielipiteet, ammattiliiton jäsenyyteen liittyvät tiedot, rotu tai etniset tiedot. Kameravalvonnassa, etenkin kaupunkien yleisvalvontaan tarkoitettujen, julkisille paikalle sijoitettujen kameroiden osalta, tällaisia tietoja voi päätyä valvontatallenteisiin. Kameran omistajan puolelta on kuitenkin periaatteessa mahdotonta estää tietojen päätymistä tietokantaan. Osaltaan siksi, että kaupunkien yleisvalvontakameroiden käytöstä on erikseen yleisesti ilmoitettu ja toiseksi tallenteeseen päätyy kaikki kuva-alan ohittavat henkilöt ja kyseisen tiedon suodattaminen on kuvausvaiheessa mahdotonta. Lisäksi henkilö itse tietoisesti saapuu kuvattavalle alueelle, josta on erikseen ilmoitettu kohteelle. Toiminta on siis rekisteröidyn itsensä puolelta aktiivista ja tarkoituksellista. EDPB:n (3/2019) tulkinnan mukaan henkilön itsensä aktiivinen toiminta ei katsota olevan tiedon julkaisemista. Tulkinta aiheuttaa selkeän vaaratekijän, jos sen vuoksi julkisella paikalla ei voitaisi suorittaa yleistä valvontaa lakisääteisin perustein. Näin tahot voisivat tarkoituksella pukeutua esimerkiksi poliittisiin asusteisiin ja suorittaa niin julkisella paikalla rikoksia. Viranomaisella ei olisi valtuuksia tallentaa kyseistä materiaali puhtaasti sen vuoksi, että henkilöt hyödyntäisivät GDPR:n tulkintaa. Kaupunkikamerat ovat pysyvästi sijoitettuna kohteisiin, eikä niiden käyttöperusteena toimi erityisten henkilötietojen kerääminen. Videomateriaali on raakadataa, jota säilötään ns. tilapäisesti kameravalvontajärjestelmässä. Vasta tiedon esiselvitysvaiheessa, kuten rikoksen tapahtuessa, tieto luokitellaan. Esimerkiksi poliisin käydessä läpi poliittisessa mielenilmauksessa tapahtunutta rikosta ja tallentaa videoleikkeen rikosasian mukaan. Siirron yhteydessä videoleike luokitellaan erityiseksi henkilötiedoksi ja se liitetään osaksi poliisin esitutkinta-aineistoa. Vasta sen jälkeen videoleikkeeseen tarvitsee kohdistaa sen luokittelun määrittämiä toimenpiteitä. Samalla tavalla on tulkittu Poliisin pilvipalvelu Poudan osalta, jonne kansalaiset voivat toimittaa periaatteessa mitä tahansa aineistoa, mutta vasta poliisin esiselvityksen yhteydessä materiaalille määritetään materiaalin salassa pidettävyyden taso. GDPR:n artikla 6 c mahdollistaa käsittelyn lainmukaisuuden, mikäli henkilötietojen käsittely on tarpeen rekisterin pitäjän lakisääteisen velvoitteen noudattamiseksi. GDPR:n artikla 6 e mahdollistaa henkilötietojen käsittelyn, kun se on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Näiden molempien kohtien osalta kansallisessa lainsäädännössä tulisi olla omaa erityistä lainsäädäntöä, jossa tarkemmin selvennettäisiin henkilötietojen käsittelystä. Poliisilain oman kansallisen erityislainsäädännön kautta määrittään poliisin toimivaltaa teknisen valvonnan osalta, jolloin poliisi saa suorittaa valvontaa yleisellä paikalla tai yleisellä tiellä, kunhan siitä on etukäteisesti ilmoitettu. Lisäksi GDPR:n artikloja tarkentavassa kohdassa 51 mainitaan: ”Valokuvien käsittelyä ei olisi automaattisesti katsottava henkilötietojen erityisryhmien käsittelyksi, koska valokuvat kuuluvat biometristen tietojen määritelmän piiriin ainoastaan siinä tapauksessa, että niitä käsitellään erityisin teknisin menetelmin, jotka mahdollistavat luon-

nollisen henkilön yksilöllisen tunnistamisen tai todentamisen.". Kameravalvonta voidaan rinnastaa yksittäisiä valokuvaan, koska se on oikeastaan iso otos kuvia, johon ei voida edes kohdistaa minkäänlaista hakua.

> H4: Kun videomateriaalia ei tallenneta erityisen henkilötiedon perusteella, videomateriaali häviää normaalin kierron mukaisesti. Tällöin tämä on vain poliisin yleistä valvontaa, jota poliisi suorittaa yleisen valvonnan ja turvallisuuden perusteella. Näitä tietoja ei muutenkaan tallenneta minnekään poliisin omiin järjestelmiin tai kasvogallerioihin. Tieto on vain kameravalvontapalvelimelta haettavissa manuaalisesti eikä siihen voi kohdistaa hakuja esimerkiksi henkilön nimellä tai sosiaaliturvatunnuksella.
>
> H2: Itseasiassa esittämänne huomio erityisten henkilötietojen muodostumisesta kameravalvonnan yhteydessä on äärimmäisen hyvä, eikä tätä todennäköisesti ole tarpeeksi mietitty edes EU-tasolla. Lähtökohtaisesti tällaisten tietojen päätyminen videomateriaaliin on jo alkuvaiheessa erityisten henkilötietojen käsittelyä. Tämä on kuitenkin sellainen asia mikä pitää viedä eteenpäin EDPB:hen. Osaltaan olisi varmasti hyvä pohtia asiaa myös tiedon luokittelun suunnalta, jolloin materiaalin tarkastelun yhteydessä havaittu tieto luokitellaan erityiseksi henkilötiedoksi.
>
> H1: Mikään hakukriteereistä ei saa olla syrjivä. Kameravalvonta on neutraalia, koska se kuvaa kaikki ketkä kuvaan sattuu tulemaan, eikä erottele henkilöä esimerkiksi ihonvärin mukaan. Jos järjestelmään luodaan etsimään vain tietyn ihonvärisiä henkilöitä silloin siitä, tulee syrjivä. Ihonvärillä suodattaminen ei kuitenkaan ole syrjivä, jos järjestelmässä voidaan etsiä kaikkien ihonvärien pohjalta. Toki ihonväri on ylipäätään hyvin vaikea tulkita tekoälynavulla, mutta se toimii hyvänä esimerkkinä.

Kameravalvontajärjestelmän on mahdollista käyttää kuvahakuominaisuutta, jossa hakua kohdistetaan henkilön vaatetuksen mukaan, etsien esimerkiksi samankaltaisia henkilöitä. Tällöinkään ei kyseessä ole erityisten henkilötietojen käyttöä, koska hahmontunnistusohjelmiston tarkoituksena ei ole yksilöidä henkilöä vaan suodattaa niitä tiettyjen attribuuttien nojalla. Tekoälysovellukseen ei kuitenkaan saa rakentaa poliittisten mielipiteiden etsimiseksi työkaluja, esimerkiksi valkoisen ylivallan hihamerkkiä etsivää hakuominaisuutta. Samoin hakujen kohdistaminen henkilön rodun tai etnisen alkuperän mukaisesti aiheuttaa erityisten henkilötietoluokkien käsittelyä. Tärkeänä huomiona on myös, että tekoälyalgoritmi automaattisesti on indeksoinut kyseisen vaatetuksen tietyllä laskennallisella kaavalla. Se tosin on ohjelmakohtaista, taltioidaanko laskennalliseen malliin vain vaatetuksen värin, jossa hihamerkki on mukana vaiko hihamerkin yksilöllisenä attribuuttina. Kuvan (kuvio 27) tarkoituksena on tuoda visuaalisesti esille henkilötietojen jakautuminen edellä avattujen perusteiden mukaisesti.

KUVIO 27 Henkilötietojen jakautuminen käsiteltäessä videomateriaalia

7.3 Kameravalvontajärjestelmien suunnittelu ja käyttö

Lähdettäessä rakentamaan uutta kameravalvontajärjestelmää tai luodessa järjestelmään uusia tekoälymahdollisuuksia, on aina hyvä aloittaa koko toiminnan perusteista. Parhaiten tämä onnistuu luomalla dokumentoitu järjestelmäkuvaus, johon tuodaan järjestelmään liittyvät osat ja tahot. Kuvauksesta tulee myös osa koko järjestelmän dokumentaatiota, jonka avulla toiminnasta muodostuu havainnollistava ja selkeä prosessi. Tätä toimintaa ohjaavaa prosessia voidaan hyödyntää kaikkien siihen kytkeytyvien henkilöiden tai organisaatioiden kanssa. Yleinen ongelma järjestelmien kehityksessä ja ylläpidossa on juuri dokumentaation puute ja toiminteiden henkilöityminen yksittäisten tahojen vastuulle, jolloin tietoa ei välttämättä ole säilötty kuin vain tietyille vastuuhenkilöille. Henkilön poistuessa muihin tehtäviin, päivitettäessä järjestelmää tai sen osia, hyvän dokumentaation turvin vältytään työläiltä lisätöiltä. GDPR:n ja siitä johdetun EDPB:n ohjeen (3/2019) sekä kansallisen tietosuojalain (1050/2018) ja tiedonhallintalain (906/2019) myötä dokumentaation vaatimukset ovat kaikilla kameravalvontaan liittyvillä osa-alueilla nousseet.

> H3: Tietosuojan osalta on tärkeää, että toiminta muodostuu prosessin omaiseksi. Aluksi asiat on voitu miettiä todella hyvin. Vastuuhenkilön vaihtuessa tai vuosien päästä järjestelmän päivityksen yhteydessä halutaan tehdä kuitenkin muutoksia, jolloin dokumentoinnin tarve korostuu.

> H9: Kameravalvonnan suunnittelutiimissä tulisi olla riittävästi läsnä etiikan ja lainsäädännön raamien tuntemusta. Ennen kaikkea etiikan ja yrityksen arvopohjan ymmärtäminen on yksi tärkeimmistä asioista. Kaikki mitä voi tehdä ei välttämättä ole yrityksen edun mukaista.

> H3: Valvontakameroiden osalta kaupunkialue voi muuttua, jolloin kameran kuva-alaan saattaa nousta esimerkiksi uusi rakennus. Kamera voikin vahingossa kuvata uuden rakennuksen huoneistoihin ja näin väärää materiaalia päätyy tietokantaan. Kameravalvontajärjestelmän osalta seurannasta ja valvonnasta on syytä huolehtia.

Järjestelmää onkin hyvä tarkastella kolmesta eri suunnasta eli hallinnollisesta, fyysisestä ja teknisestä näkökulmasta. Hallinnollisilla toteutuksilla luodaan perusta kameravalvontajärjestelmälle ja varmistutaan organisaation valmiudesta ja kyvykkyydestä. Fyysisillä toteutuksilla taas huolehditaan laitteiden, tilojen ja tietojen eheydestä. Lopuksi teknisillä toteutuksilla varmistutaan tietojen luotettavuudesta. Järjestelmän ehkä tärkeimpänä yksittäisenä vaatimuksena on kuitenkin määrittää ne tahot, jotka järjestelmää tulevat käyttämään ja miten heidän lakisääteiset perusteensa vaikuttavat järjestelmän käyttöön. Tällä on myös merkittäviä vaikutuksia siihen, onko järjestelmän rekisterinpito järkevää tai käytännöllistä hoitaa yhteisesti vai erikseen. Mikäli järjestelmän hallinnolliset toteutukset on hoidettu puutteellisesti, järjestelmää on mahdotonta toteuttaa fyysisesti ja teknisesti oikein. Pahimmassa tapauksessa tämä voi johtaa siihen, ettei

järjestelmää ole mahdollista hyödyntää yhteiskäyttöisesti tai siinä mahdollisesti käytettäviä ominaisuuksia on rajattava.

Järjestelmän tietojen elinkaaren hallinta on myös toteutettava ja dokumentoitava alusta loppuun. Tällä tarkoitetaan siis dokumentoitua prosessikuvausta järjestelmän suunnittelusta alkaen ja päättyen siihen pisteeseen, kunnes tarve tietojen käsittelylle päättyy ja ne on hävitettävä asianmukaisesti. Kameravalvonnan kuvauksesta tulisi siis löytyä järjestelmän käyttöön ja sen käyttöoikeuksiin liittyvät selvitykset. Visualisoidusta tai luetteloidusta kuvauksesta on helpompi hahmottaa ne tahot, joilla on oikeus käsitellä järjestelmää ja millä tavoin ne on rajattu. Tahojen vastuut ja roolit tulee selkeästi avata dokumentaatiossa. EDPB:n ohjeistuksessa (3/2019) esimerkiksi käyttöroolien kuvaus tulee olla selkeä ja käyttöoikeuden kamerakohtaiset näkyvyydet tulee olla selvitettävissä. Mikäli valvontakamerajärjestelmään liitetään paljon erityyppisiä kameroita, kuten liikennekameroita, yleisvalvontaan tarkoitettuja kameroita ja kaupungin omien tilojen kameroita, näkyvyyksien rooli entisestään korostuu. Esimerkiksi poliisilla on hyvin laaja käyttöoikeusperuste yleisen turvallisuuden nojalla hyödyntää julkiselle paikoille asennettuja yleisvalvontakameroita. Tämän vuoksi jo suunnittelun alkuvaiheessa kameroiden käyttötarkoituksen perusteleminen, ryhmittämisen ja niiden kuvasektorin määrittämisen merkitys korostuu. Olennaista on myös huomioida, että vaikka jotkut järjestelmän kamerat eivät itsessään keräisi henkilötietoja, yhteisrekisterinpidossa olevien kameroiden osalta tietoja yhdistelemällä nämäkin tiedot saatetaan luokitella henkilötiedoiksi. Tällaisia kameroita voivat esimerkiksi olla tieliikennekamerat, joista henkilöä tai auton rekisterinumeroa ei ole tunnistettavissa, mutta yhdistettynä järjestelmän muihin tietoihin tai kameroihin, parkkipaikalle pysähtyneen auton kuljettajasta voidaan saada tunnistettava kuva. Tällöin ilmoitusvelvollisuus kameravalvonnasta tulisi järjestää myös näiden kameroiden osalta.

Kun kameravalvonnassa käsitellään henkilötietoja siitä, tulee laatia tietosuojaseloste. Selosteessa on perusteltava jokaisen eri käyttäjäroolin käyttöperuste. Tietosuojavaltuutettu on yhteiskäyttöisen kameravalvonnan osalta tuonut päätöksessään (TSS 6610/182/18 2019) esille, että olisi suotavaa tukea yhteiskäyttörekistereitä. Näin jokainen taho määrittäisi omat vastuualueensa kameravalvontajärjestelmän käytöstä. Lähtökohtaisesti olisi järkevää, että järjestelmän ylläpidosta, kuten huollosta ja teknisistä ratkaisuista vastaa järjestelmän rakentaja eli kaupunki. Yhteisrekisterinpidollisista syistä järjestelmän olisi hyvä täyttää tiedonhallintalain mukaiset suositukset turvallisuudesta. Tämä tukisi viranomaisten liittymistä järjestelmän yhteisrekisterinpitäjäksi. Tiedonhallintalain minimivaatimukset salassa pidettävän tiedon osalta ovat hyvin pitkälti samassa tasossa viranomaisen alimman turvallisuusluokitellun (TL IV) tason kanssa. Näin ollen esimerkiksi turvallisuusviranomaisten kanssa tehtävien, kameravalvontaa koskevien, sopimusten tekeminen helpottuisi. Yhteisrekisterinpidossa erityisesti järjestelmän hallinnolliset ja tekniset toteutukset korostuvat.

> H1: Yhteisrekisterinpidon kautta pystytään hälventämään epäselvyyksiä aivan rekisterinpidosta lähtien. Näin voidaan määrittää käsittelytarkoituksia ja rajapintoja mihin ja mitäkin tietoja missä tilanteissa voidaan käyttää. Isoin ongelma yhteisrekiste-

rinpidossa on vastuiden selkeä määrittäminen ja nämä pitää huomioida ja jakaa selkeästi heti alkuvaiheessa. Kaupunki voi paljon vapaammin sijoittaa kameroita eikä niitä tarvitse edes niin yksityiskohtaisesti perustella rekisteriselosteessa. Turvallisuusviranomaisten toimivalta on säädelty paljon tarkemmin kuin kaupungin, jolloin perusteet jokaisen taltioivan kameran osalta pitää olla selvät.

H2: Yhteisrekisterinpito ei ole täysin yksiselitteinen asia. Yhteisrekisterinpidossa olevat järjestelmät, joissa on paljon erilaisia toiminallisuuksia ja niihin on liitetty useita erityyppisiä kameroita, voi aiheuttaa lakiteknisen ongelman. Lähtökohtaisesti jokaisella rekisterinpitäjällä tulisi olla koko rekisterin kannalta laillinen käsittelyperuste. Erittäin tarkalla teknisellä ja hallinnollisella toteutuksella kameroiden tietokannat ja käyttöoikeudet voidaan jakaa niin, että järjestelmää voidaan oikeasti käyttää yhteisrekisterinpidollisesti.

Kaupungin rekisterinpidon alla toteutetusta järjestelmästä voidaan jakaa teknisiä yhteyksiä tietojen luovuttamiseksi. Tahot eivät kuitenkaan voi täysin itsenäisesti noutaa dataa, vaan järjestelmään tulee tehdä siihen tekninen ratkaisu, jotta rekisterinpitäjä pystyy määrittämään tapauskohtaisesti tietojen luovutuksen. Tietojenluovutuksen nojalla esim. poliisin ja pelastustoimen kyky päästä reaaliaikaiseen materiaaliin vaikeutuu. Ratkaisuksi järjestelmään pitäisi luoda tapauskohtainen toiminne, jotta rekisterinpitäjä voisi tilanteessa arvioida ja luovuttaa mahdollisuuden reaaliaikaiseen näkyvyyteen. Tämä ei käytännön tasolla olisi kuitenkaan järkevästi toteutettavissa kellon ympäri.

Yhteisrekisterinpidon kautta ongelma poistuu ja vastuu toimista siirtyy rekisterinpitäjille. GDPR:n artikloja tarkentavassa kohdassa 50 tuodaan esille, että henkilötietojen käsittely muita tarkoituksia varten kuin mitä varten ne on kerätty, olisi sallittavaa ainoastaan silloin kuin se on yhdenmukaista alkuperäisen tarkoituksen mukaisesti. Kamerat tulee jakaa selvästi omiin varantoihin. Yleisen järjestyksen ja turvallisuuden (lyhenne YJT) ylläpitämiseksi tarkoitetut kamerat tulevat järjestelmässä jakaa ainoastaan poliisin käyttöön nojaten poliisilain (872/2011) 4-luvun 1§ tekniseen valvontaan. Näiden käyttötarkoitus on lähtökohtaisesti myös rikosten paljastaminen ja ennalta ehkäisy, jonka vuoksi niitä käytetään tunnistamistarkoituksessa. Tapauskohtaisesti esimerkiksi tapahtumaturvallisuuden osalta vartijat, jotka toimivat tapahtumajärjestäjän palkkaamina suorittamassa poliisin tukena tapahtuman turvallisuutta, voivat saada tilapäisen käyttöoikeuden järjestelmään. Laki yksityisistä turvallisuuspalveluista (1085/2015) 2-luvun 4 § määrittää vartijan laillisen käyttöperusteen samanlaiseksi kuin poliisilla. Tarkoituksena olisi siis henkilön koskemattomuuden suojaaminen ja rikosten paljastaminen. Teknisesti YJT-kameroiden rekisterinpito olisi rajattu yhteisrekisterinpidossa poliisille, jolloin tapahtumien osalta sopimus järjestelmän käytöstä tehtäisiin poliisin kanssa. Vastuut käyttäjien toimista tulee kuitenkin olla hallinnollisesti kuin teknisestikin todella selkeästi valvotut ja rajatut, etenkin yksittäisten tapahtumien osalta.

Kaupungin puolelta järjestelmän rekisterinpidollinen vastuu olisi jaettu poliisin ja pelastustoimen kanssa ainoastaan liikennekameroihin ja muihin vastaaviin kameroihin, joiden pääasiallinen tarkoitus ei ole ihmisten tunnistaminen. Tällaisten kameroiden osalta ei edes yleisesti ole mahdollista saada tunnistetta-

vaa kuvaa henkilöstä tai ajoneuvosta, jolloin tietovarantoihin ei alustavasti sovelleta GDPR:ää. Koska niitä kuitenkin hyödynnettäisiin yhdessä ja niitä mahdollisesti voitaisiin poliisin puolelta yhdistää muihin järjestelmässä oleviin henkilötietoihin, niitä tulisi käsitellä myös henkilötietoina. Henkilötietoina pidettävän materiaalin myötä, järjestelmässä hyödynnettävän tekoälyohjelmiston käyttö mahdollistuisi. Tällöin materiaalin tehokkaampaa käsittelyä voisi toteuttaa koko materiaalin osalta, eikä olisi pelkoa siitä, että tekoälyn tuottamat tiedot muuttaisivat materiaalin tunnistamattomasta tiedosta henkilötiedoksi. Huomioitavaa olisi kuitenkin se, että tekoälyohjelmisto ei missään nimessä saisi käsitellä tai luoda biometrisia tai muita erityisiä henkilötietoluokkia. Teknisten rajausta avulla tekoälyohjelmistollakaan ei saisi käsitellä kuin sitä tietoa mihin taholla on lakiperusteinen käyttöperuste. Poliisin YJT-kameroita ei siis saisi edelleenkään käsitellä kuin poliisi ja erillistapauksissa vartija.

> H4: Niin poliisilla kuin kaupungilla tulee olla laillinen käyttöperuste kameravalvonnan suorittamiseksi ja tallenteiden katselemiseksi. Poliisilla on hyvin selkeä lakiperuste yleisillä paikoilla tapahtuvaan tekniseen kameravalvontaan. Kaupungin puolelta voi olla ongelmallista suorittaa valvontaa. Toki kunnalla on oikeus suojella omaisuutta, tehdä väenlaskentaa tai tapahtumaturvallisuuden osalta käyttää valvontakameroita yleisötapahtumissa, mutta käyttöperuste tulee olla hyvin selkeästi avattu ja kamerakohtaisesti mietitty.

> H2: Rekisterinpitäjän tehtävänä on suunnitella järjestelmän tarkoituksenmukainen ja lainmukainen käyttö. Vaihtoehtoja tulee arvioida. Yhteisrekisterinpidon osalta tulee miettiä tosiasiallista toimintaa. Mikä on varsinainen käyttötarkoitus ja kuka määrittää henkilötietojen käsittelyn keinot. Jos se eroaa toisistaan tai liittyy vain löyhästi toisiinsa, niin on vaikea nähdä yhteisrekisterinpidon mahdollisuutta ja tarkoituksenmukaisuutta. Tulee arvioida myös mitä nykylainsäädäntö mahdollistaa ja riittääkö se, vai tarvitaanko säädösmuutoksia. Tässä yhteydessä tulee myös huomioida, että henkilötietojen käsittelyä tehtäisiin osin eri oikeusperusteilla (asetus ja rikosasioiden tietosuojalaki). Tietoja voidaan luovuttaa (tietoluvat) jos käyttötarkoitus on sama tai oikeus käsitellä ko. tarkoitukseen, tai tiedonsaannista säädetään laissa.

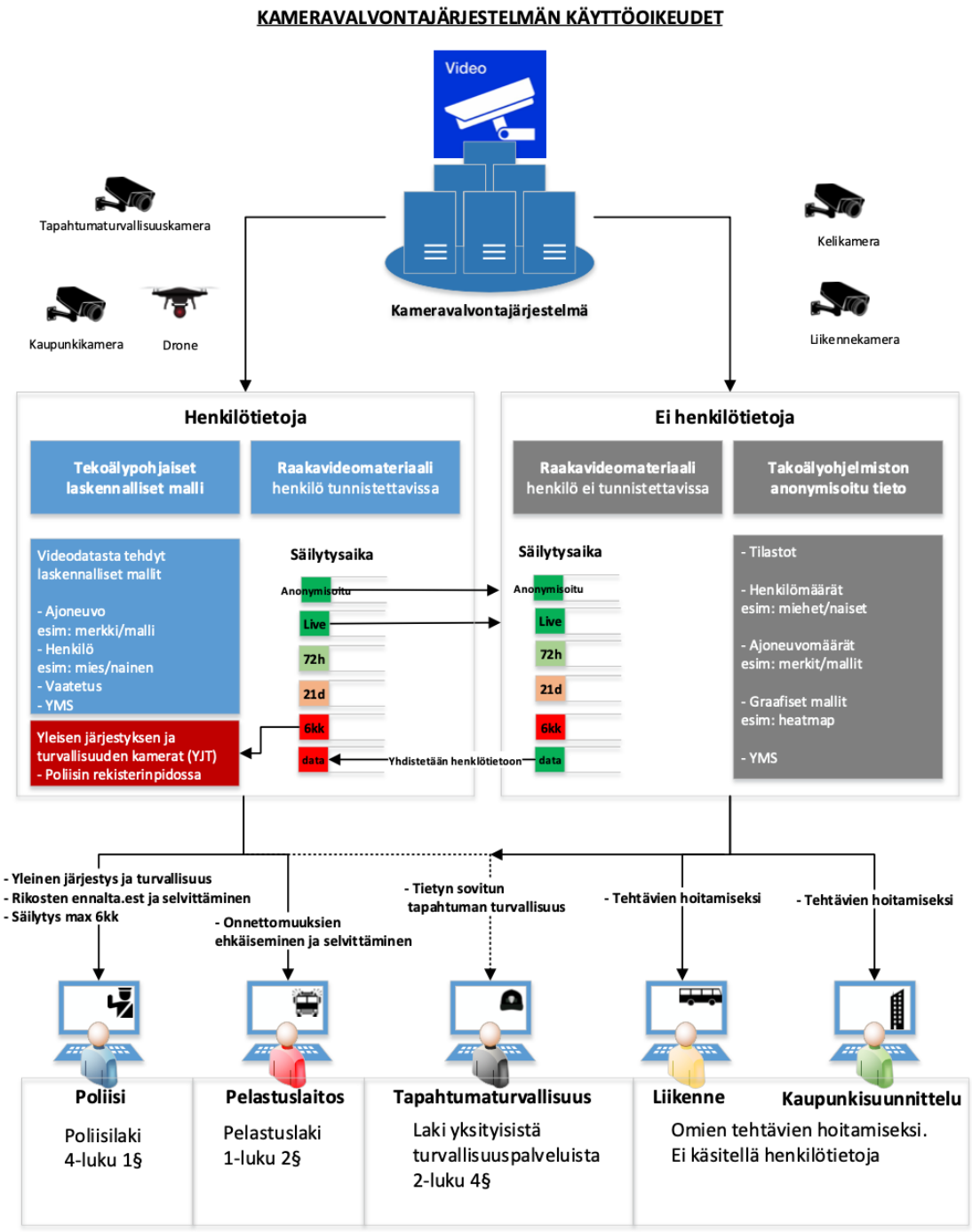
> H2: Yhteisrekisterinpito ei ole täysin yksiselitteinen asia. Yhteisrekisterinpidossa olevat järjestelmät, joissa on paljon erilaisia toiminallisuuksia ja järjestelmään on liitetty useita erityyppisiä kameroita, voi aiheuttaa lakiteknisen ongelman. Lähtökohtaisesti jokaisella rekisterinpitäjällä tulisi olla koko rekisterin kannalta laillinen käyttöperuste. Erittäin tarkalla teknisellä ja hallinnollisella toteutuksella kameroiden tietokannat ja käyttöoikeudet voidaan jakaa niin, että järjestelmää voidaan oikeasti käyttää yhteisrekisterinpidollisesti.

Mikäli järjestelmästä hyödynnetään esimerkiksi tekoälyohjelmiston avulla luotua tilastotietoa, kyseistä tehtävää tekevällä järjestelmän käyttäjällä ei tarvitse olla laillista käyttöperustetta henkilötietojen ja sitä myöten koko valvontakamerajärjestelmän käyttöön. Tällöin pitää huolehtia, että käyttöoikeudet ovat rajattu siten, että käyttäjä voi ainoastaan käsitellä sellaista osaa järjestelmässä, jossa ei ole esillä henkilötietoja, eikä näitä tietoja yhdistelemällä ole mahdollista luoda yhteyttä takaisin henkilötietoihin. Tiedot ja niiden yksilöön liittyvä alkuperä on siis täysin anonymisoitu.

H2: Jos tiedot ovat aidosti anonymisoituna (ei tunnistettavissa), ei GDPR sovellu. Tietojen kautta ei kuitenkaan tule olla mitään epäsuoraakaan keinoa tunnistaa rekisteröityä. Jos esimerkiksi tiedot rajataan pelkästään laskettuun ihmismäärään tai ihmisryhmien erottamiseen toisistaan (esim. sukupuoli ja ikä), tietoja ei saa luoda käyttäen biometrisiä tunnisteita tai tiedoista ei saa muodostua sellaisia.

H7: Siinä vaiheessa, kun hahmon kasvojen metadataa käytetään parametrinä, mennään ns. harmaalle alueelle. Onko se sama hahmo, joka löytyy, vaikka sillä olisi vihreä paita, kun viimeksi sillä oli keltainen paita? Ei voida käsi sydämellä sanoa, että järjestelmä on ehdottanut asioita, vaan se kyllä tietää. Mennään enemmän siihen, että miten järjestelmät rakennetaan ja suunnitellaan. Inhimillisen tekijän rooli korostuu ja sen on oltava aina niin vahva, että lopullinen päätöksentekijä asiassa on ihminen.

Alla olevassa kuvassa (kuvio 28) on tuotu esille kaupunkikamerajärjestelmän yleisiä käyttötahoja. Näiden kohdalta on avattu järjestelmän lakisääteisiä käyttöperusteita suhteutettuna niihin tietoihin, joihin tahoilla työtehtävien hoitamiseksi olisi tarpeellista päästä. Lisäksi sen alla olevassa toisessa kuvassa (kuvio 29) on tuotu esille tahojen lailliset käsittelyperusteet.



KUVIO 28 Hahmotelma kameravalvontajärjestelmän käyttöoikeuksista

KÄSITTELYPERUSTEIDEN LAINSÄÄDÄNNÖLLINEN POHJA

POLIISI

Poliisilaki (872/2011) 4-luku 1 §: Tekninen valvonta ja tiedonsaantioikeudet
Teknisellä valvonnalla tarkoitetaan jatkuvaa tai toistuvaa ajoneuvoihin, ajoneuvojen kuljettajiin, jalankulkijoihin tai yleisöön kohdistuvaa teknisellä laitteella tapahtuvaa katselua tai kuuntelua sekä äänen tai kuvan automaattista tallentamista.
Poliisi saa siitä ennalta ilmoitettuaan suorittaa yleisellä paikalla tai yleisellä tiellä teknistä valvontaa yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, rikosten ennalta estämiseksi, rikoksesta epäillyn tunnistamiseksi sekä erityisten valvontakohteiden vartioimiseksi.

Laki henkilötietojen käsittelystä poliisitoimessa (616/2019)
2-luku 5§ Henkilötietojen käsittely tutkinta- ja valvontatehtävissä
Poliisi saa käsitellä henkilötietoja esitutkinnan, poliisitutkinnan tai muun rikoksen selvittämiseen tai syyteharkintaan saattamiseen liittyvän tehtävän, yleisen järjestyksen ja turvallisuuden ylläpitämiseen liittyvän tehtävän ja muun poliisille säädetyn valvontatehtävän suorittamiseksi.
2-luku 7§ Henkilötietojen käsittely rikosten ennalta estämiseksi tai paljastamiseksi
Poliisi saa käsitellä henkilötietoja rikosten ennalta estämiseen tai paljastamiseen liittyvän tehtävän suorittamiseksi.

PELASTUS

Pelastuslaki (379/2011) 1-luku 2§
1) ehkäistä tulipaloja ja muita onnettomuuksia;
2) varautua onnettomuuksiin sekä toimintaan onnettomuuksien uhatessa ja sattuessa;
3) rajoittaa onnettomuuksien seurauksia;.

42§ Yhteistyö onnettomuuksien ehkäisemisessä
Pelastuslaitoksen tulee onnettomuuksien ehkäisemiseksi ja turvallisuuden ylläpitämiseksi toimia yhteistyössä muiden viranomaisten sekä alueella olevien yhteisöjen ja asukkaiden kanssa sekä osallistua paikalliseen ja alueelliseen turvallisuussuunnittelutyöhön.
88 §Tiedonsaantioikeus palon- ja onnettomuuden tutkinnassa
Tämän lain 41 §:n mukaista palontutkintaa suorittavalla alueen pelastusviranomaisella ja 107 §:n mukaista onnettomuuden tutkintaa suorittamaan määrätyllä tutkintalautakunnan jäsenellä ja asiantuntijalla on oikeus päästä onnettomuuskohteeseen ja ottaa näytteitä sekä saada salassapitosäännösten estämättä maksutta tutkinnassa välttämättömiä tietoja ja asiakirjoja onnettomuuskohteen edustajalta ja viranomaisilta.
89 § Tiedonsaantioikeus pelastustoimintaa ja valvontatehtäviä varten
Pelastusviranomaisella on sille tässä laissa säädettyjen tehtävien suorittamiseksi oikeus salassapitosäännösten estämättä saada maksutta pelastustoiminnan suunnittelussa ja toteutuksessa sekä pelastustoimelle säädettyjen valvontatehtävien hoitamisessa tarpeellisia tietoja.
Pykälien 88§ ja 89& osalta:
Tarkoitetut tiedot on oikeus saada myös rajapinnan kautta tai muutoin sähköisesti.

VARTIJAT

Laki yksityisistä turvallisuuspalveluista (1085/2015) 2-luku 4§
Vartijan tehtävänä on suorittaa vartioimistehtäviä vartioimisalueella.
Erillisen omaisuuden vartiointia, henkilön koskemattomuuden suojaamista tai rikoksen paljastamista koskevaa vartioimistehtävää vartija voi suorittaa myös muualla kuin vartioimisalueella.

KAUPUNKI

EU:n yleinen tietosuoja-asetus (2016/679) Artikla 6. Käsittelyn lainmukaisuus
e)käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;
Tietosuojalaki (1050/2018) 4§
Henkilötietoja saa käsitellä tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdan mukaisesti, jos:
1) kysymys on henkilön asemaa, tehtäviä sekä niiden hoitoa julkisyhteisössä, elinkeinoelämässä, järjestötoiminnassa tai muussa vastaavassa toiminnassa kuvaavista tiedoista siltä osin kuin käsittelyn tavoite on yleisen edun mukainen ja käsittely on oikeasuhtaista sillä tavoiteltuun oikeutettuun päämäärään nähden;
2) käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi;
Laki julkisen hallinnon tiedonhallinnasta (906/2019) 23§ Katseluyhteyden avaaminen viranomaiselle
Viranomainen voi avata katseluyhteyden toiselle viranomaiselle tietovarannon sellaisiin tietoihin, joihin katseluoikeuden saavalla viranomaisella on tiedonsaantioikeus. Sen lisäksi, mitä 4 luvussa säädetään, edellytyksenä katseluyhteyden avaamiselle on, että:
1) katselumahdollisuus on rajattu vain yksittäisiin hakuihin, jotka voivat kohdistua tiedonsaantioikeuden mukaisesti tarpeellisiin tai välttämättömiin tietoihin; sekä
2) tietojen hakemisen yhteydessä selvitetään tietojen käyttötarkoitus.
Viranomaisen on toteutettava katseluyhteys siten, että katseluyhteyden mahdollistava tietojärjestelmä tunnistaa automaattisesti poikkeavan tietojen hakemisen.

KUVIO 29 Käsittelyperusteiden lainsäädännöllinen pohja

Kameravalvontajärjestelmä edellyttää säännöllistä riskienarviointia mutta erityisesti suunniteltaessa se on otettava huomioon. Etenkin kun järjestelmässä käsitellään henkilötietoja uusien teknologien avulla, on tästä tehtävä vaikutustenarvioinnin liitteeksi riskiarvio. Riskien arviointiin on syytä osallistua kaikki järjestelmän rekisterinpitotahot sekä kommentteja tulisi ottaa myös tahoilta kenelle tietoja järjestelmästä luovutetaan. Riskiarvioissa tulisi havaita henkilötietojen käsittelystä syntyviä riskejä, keinoja niiden minimoimiseksi ja hallintatavat riskien toteutuessa. Riskien suhteen tulisi olla avarakatseinen ja pyrkiä arvioimaan myös mahdollisesti tulevaisuudessa syntyviä riskejä. Esimerkiksi mahdollisten uusien teknologien myötä järjestelmästä saatavien henkilötietojen käyttöperusteen muutokset. Järjestelmän käyttöperuste ei saisi muuttua kesken kaiken, vaan järjestelmää saa käyttää ja siitä tietoa luovuttaa vain tietosuojaselosteessa mainituin perustein. Järjestelmän hallinnan puolelta olisi hyvä huomioida seuraavia seikkoja:

> H4: Poliisissa ollaan valmistelemassa vaikutustenarviointia siitä, miten poliisi voi teknisesti liittyä mm. kaupunkien videovalvontajärjestelmiin. Tämän myötä nykyisiä hyvin hajanaisia järjestelmiä voitaisiin helpommin ja järkevämmin sitoa yhteen, joka osaltaan parantaisi niiden valvontaa ja yhdenmukaistaisi henkilötietojen käsittelyä.

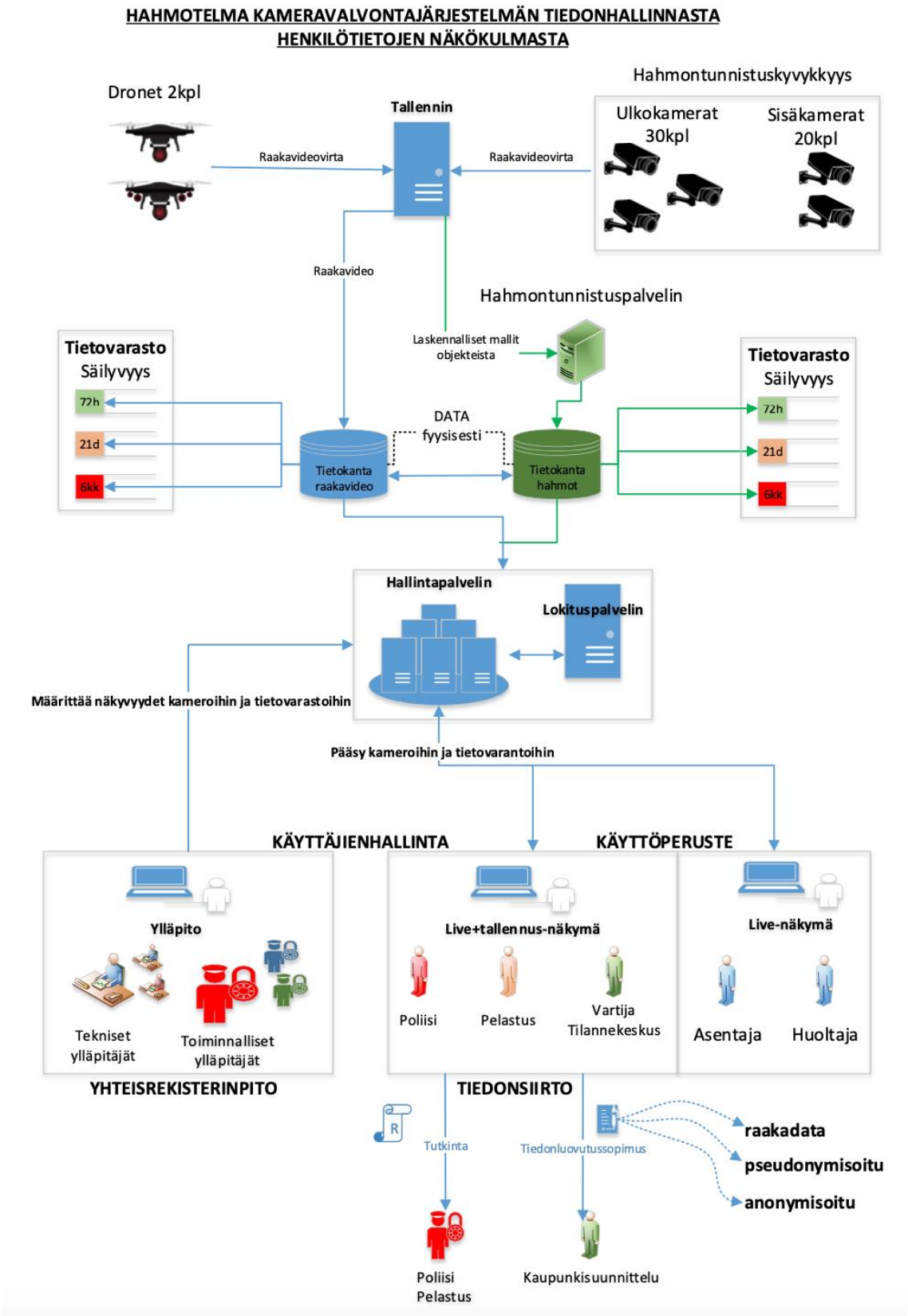
Monen rekisterinpitäjän järjestelmä vaatii jo suunnitteluvaiheessa paljon huomiota, jotta siihen on rakennettu tarpeeksi kyvykkyyksiä rajata järjestelmän ominaisuuksia. Rajaamisen merkitys järjestelmän käytön kannalta on yksi kriittisimmistä asioista, koska sen avulla mahdollistetaan järjestelmän mahdollisimman laaja hyödyntäminen. Erilaisilla ja helposti muokattavilla käyttöoikeuksilla sekä tiedon tallentamisen lohkoilla voidaan määrittää hyvinkin yksilöllinen käyttö. Tämä on yleisesti isoin puutos ns. avaimet käteen hankittavien järjestelmien kanssa. Tämä johtuu siitä, että GDPR:n ja Suomen kansallisen lainsäädännön tuoreutta ei ole pysytty ottamaan huomioon Euroopan ulkopuolisissa maissa, joista iso osa tekoälyohjelmistoja on tullut markkinoille. Käyttäjien lakiperusteiset käyttöoikeudet kameravalvontajärjestelmän käsitellylle ovat hyvin hajanaisia, eivätkä ne ole linjassa keskenään. Tämän vuoksi järjestelmän tulisi olla hyvin muokattavissa, jotta jokaiselle taholle voidaan rakentaa omat pääroolit ja jopa käyttäjäkohtaiset näkymät. Tämä tukee sitä, että järjestelmään voidaan tallentaa yhteiseen tietovarantoon henkilötietoja, jotka ovat esimerkiksi säilyvyydeltään automaattisesti rajattu siten, että tietyn ajan sisällä vain tietyt käyttäjät pääsevät materiaaliin käsiksi. Toisena esimerkkejä toimii se, että osa käyttäjistä näkee vain osan verkon kameroiden tuottamasta datasta ja näkyvyys pohjautuu henkilön lakisääteiseen käyttöperusteeseen. Roolien ja näitä koskevien riskien miettimien pitää aloittaa jo järjestelmän rakennusvaiheessa, jotta järjestelmä on kykenevä yhteiskäyttöiseksi järjestelmäksi. Alla olevan kuvan (kuvio 30) tarkoituksena on visualisoida kameravalvontajärjestelmän käyttöoikeuksien jakautumista yhteiskäyttöisessä henkilötietorekisterissä.

> H4: Varsinkin liikkuvan rikollisuuden ja järjestäytyneen rikollisuuden tutkinnassa näitä asioita selvitellään usean kuukauden päästä asian todellisesta tapahtuma-

ajankohdista. Sen takia on tärkeää, että poliisi voi saada kuudenkin kuukauden päästä tallennettua materiaalia käsittelyyn, mikäli se on tapauskohtaisesti tärkeää. Kuusi kuukautta on poliisin teknisen valvonnan osalta pisin mahdollinen tallennusaika kameravalvontamateriaalille.

H2: Kameravalvonnan ylläpidon osalta on hyvin tärkeää miettiä myös pääkäyttäjien jakautumista niin hallinnollisiin kuin teknisiin ylläpitäjiin.

H2: EDPB:n 72 h määre ei ole ehdoton valvontakameramateriaalin säilytykselle. Tämä tosin vaatii selkeän perustelun tarkoituksesta ja tarpeellisuudesta, mikäli materiaalia säilytetään pidempään. Jos on eri käsittelyn tarkoituksia, niin tiedot tulee eritellä loogisesti, joka on mahdollista tehdä myös käyttöoikeuksin. Järjestelmässä voi olla myös mahdollisuus hyödyntää ns. black box periaatetta. Tällöin tallenteisiin pääsee käsiksi vain yksittäisissä tapauksissa, kun laillinen käyttöperuste ilmaantuu.



KUVIO 30 Hahmotelma kameravalvontajärjestelmän tiedonhallinnasta käytännössä

Kameravalvontajärjestelmän suunnittelun ja käytön tueksi on mahdollista hyödyntää seuraavia kysymyksiä. Kysymykset tukevat mm. järjestelmän tietosuojaselosteen laatimista, vaikutustenarviointia ja muuta dokumentointia. Aluksi huomioidaan järjestelmän osalta olennaisimmat yleiset kysymykset, jonka jälkeen ne jaetaan kappaleen alussa mainitun turvallisuuden kolmijaon mukaisesti hallinnolliseen, fyysiseen ja tekniseen osioon. Näillä kysymyksillä pyritään helpottamaan järjestelmän dokumentaation laatimista ja kokonaisturvallisuuden hallintaa.

Yleisesti huomioitavia asioita kameravalvontajärjestelmän suunnittelussa ja käytössä:

- Visuaalinen järjestelmäkuvaus kameravalvontajärjestelmästä
- Vaikutustenarviointi
- Riskienarviointi, tietojen elinkaaren hallinta kokonaisuudessaan
- Tietosuojaseloste
- Laadukas dokumentointi

Hallinnollisten toteutusten näkökulmasta tulisi huomioida seuraavia asioita:

- Millaisia rooleja ja näkyvyyksiä järjestelmään luodaan?
    - Reaaliaikainen näkyvyys, pääsy tallenteisiin tai molemmat
    - Tallenteiden säilyvyyden eri tasot ja niiden jakautuminen laillisen käyttöperusteen mukaan: esim. 72h/1kk/6kk
    - Tekoälysovelluksesta muodostuvat henkilötiedot ja niiden käyttö sekä toimiminen eri tallenteiden säilyvyysluokkien kanssa.
    - Tiettyjen kameroiden rajaaminen käyttöperusteisesti
- Järjestelmästä siirrettävät henkilötiedot ja niiden elinkaaren sekä käsittelyperusteen hallinta?
    - Henkilötietojen käsittelystä (ml. koko elinkaaren huomiointi) on sovittava kirjallisella sopimuksella
    - Käsittelyssä huomioitava vastaanottavan tahon laillinen käyttöperuste
- Miten riskienarviointi on toteutettu ja kuinka sekä kenen vastuulla on toimia, jos riskit toteutuvat?
    - Dokumentoitu riskienarviointi, selkeä riskienhallintaprosessi
    - Riskin omistaja, hallintakeinot, merkityksen arviointi
    - Tarvittavien tahojen osallistaminen organisaatiotasolla
    - Sidosryhmien huomiointi riskienarvioinnissa
    - Toipumis- tai jatkuvuussuunnitelma

- Miten yhteiset ohjeistukset on rakennettu?

    - Dokumentoidut yhteiset ohjeet järjestelmässä
    - Kunkin tahon on huomioitava oma lakisääteisen toimivaltaperuste ja ohjeistuksen eroavaisuudet

- Mitä kameroita järjestelmään kytketty ja kuinka paljon niitä on yhteensä?

    - Kameroiden sijoittaminen karttapohjalle. Toiminnolla tuetaan käyttäjiä ja kameroiden huoltoa sekä ylläpitoa.
    - Dokumentoinnin päivittäminen osoitettava henkilölle

- Millä tavoin kamerat eroavat toisistaan?

    - Voidaanko kameralla tuottaa tunnistettava kuva?
    - Käytetäänkö kameraa tunnistustarkoitukseen?
    - Kerätäänkö kameralla henkilötietoja?
    - Onko kyseessä kiinteä kamera, tarkentava kamera, drone, sisä- tai ulkokamera yms.?
    - Mihin kameroihin on kytketty tekoälyominaisuuksia?
    - Kameroiden muut ominaisuudet kuten kuvatahti ja resoluutio

Fyysisten toteutusten näkökulmasta tulisi huomioida seuraavia asioita:

- Millä tavoin kameroiden ja järjestelmän fyysisestä turvallisuudesta on huolehdittu?

    - Murtosuojaukset, sääsuojaukset yms.
    - Kaapeloinnit, jakamot, tallentimet, palvelimet
    - Lukitukset, kulkuoikeudet, hälytykset

- Millä tavoin kameran suuntaus on huomioitu suhteessa henkilötietojen keräämiseen?

    - Esimerkiksi vuodenaikojen, infrastruktuurin tai kameran suuntauksen vaikutukset, siten ettei kamera kuvaa asuntoihin sisälle tai muuten kerää sellaista tietoa mikä ei ole sallittua

Teknisten toteutusten näkökulmasta tulisi huomioida seuraavia asioita:

- Missä kameroiden tuottamaa dataa säilytetään ja millaisessa muodossa data on?

  - Mitä eri tietokantoja tai kamerakokonaisuuksia järjestelmään on integroitu?
  - Voidaanko ja käytetäänkö näitä yhdessä käyttää henkilön tunnistamistarkoitukseen, mikä voi johtaa siihen, että kokonaisuutena kameroiden dataa voidaan käsitellä henkilötietoina?
  - Tärkeää on huomioida, että tekoälyohjelmistot tuottava kameravalvonnan raakadatan lisäksi erillisiä laskennallisia malleja, jotka itsessään voivat olla myös henkilötietoja, etenkin jos niitä käytetään raakavideodatan kanssa.

- Millä tavoin tiedon säilyvyys on järjestetty ja mihin osiin tietovarannot on jaettu?

  - Sirpaloituuko tiedot eri tietokantoihin ja kuinka kauan niissä säilytetään tietoa?
  - Miten tiedon poistaminen tapahtuu?
  - Millä eri perusteilla tietoa voidaan säilyttää yli EDPB:n suosittelema 72 tuntia?

- Ketkä käyttävät järjestelmää ja mihin lailliseen käyttöperusteeseen se pohjautuu?

  - Miten ja kuka vastaa oman vastuualueensa seurannasta ja käyttäjistä
  - Miten vastuutaho raportoi asiasta järjestelmän ylläpitäjälle/rekisterinpitäjälle

- Kuka vastaa järjestelmän teknisestä ylläpitämisestä ja huoltamisesta

  - Miten sopimukset luodaan yksityisten yritysten kanssa?
  - Dokumentoinnin tärkeys järjestelmän nykyisen tekniikan ja toteutuksen suhteen
  - Miten muutokset dokumentoidaan?
  - Kamera- ja järjestelmälisenssit ja niiden voimassaoloaika
  - Elinkaarikustannukset

- Miten määritetään kameravalvontajärjestelmän lokitus?

  - Laillisen perusteen kirjaaminen jo käyttövaiheessa, jolloin lokiin jää perusteet tallenteiden tarkastelusta tai siirtämisestä esimerkiksi esitutkintaan.

8 JOHTOPÄÄTÖKSET JA POHDINTA

Kameravalvontaan ja tekoälyyn liittyvä julkinen keskustelu on selvästi negatiivissävytteinen. Tämä tuli esille tutkimuksen aikana niin kirjallisuuskatsauksessa läpikäytyjen lukuisten artikkelien, tulevaisuutta kuvaavien raporttien kuin lainsäätäjien teksteissä tuotujen riskien puolelta. Lisäksi tätä tuki asiaan vihkiytyneiden asiantuntijoiden haastattelut, joissa useissa toistettiin, että asian ympäriltä on tehty liian vähän tutkimusta. Suomea ja Eurooppa koskevan faktapohjaisen tutkimuksen puute ja median saama huomio, on johtanut hyvinkin populistiseen uutisointiin ja muokannut ihmisten mielipiteitä tekoälystä. Tällöin keskiöön on noussut Euroopan ulkopuolella tapahtuneet asiat. Median repostelemat esimerkit totalitarismisesta diktatuurista ovat saaneet paljon palstatilaa demokratian puolesta puhuvissa maissa, etenkin kun toimia on automatisoitu tekoälylle ja viety pidemmälle kuin George Orwell uskalsi edes kuvitella. Suomi on kuitenkin jopa Euroopan mittapuulla mitattuna poikkeuksellinen oikeusvaltio. Ihmisten luottamus virkamiehiin, kuten poliisiin on säilynyt ällistyttävän korkealla tasolla. Tähän ei ole juuri vaikuttanut edes lähivuosien aikana massiiviset mediamylläkät, johtuen korkean tason rikostutkinnoista. Tämä herättääkin kysymyksen miksi tuntuu siltä, että tekoäly, jonka tarkoituksena on parantaa ihmisten elämänlaatua, mutta myös tehostaa virkamiesten tekemien päätösten oikeellisuutta koetaan uhkana.

Kameravalvonta on itsessään myös saman tematiikan uhri kuin tekoälykin. Oletuksena on, että satojentuhansien kameroiden kuvavirtaa tarkkaillaan valvovan tahon toimesta 24/7. Tutkimuksessa kuitenkin tuli esille, että ainoastaan 1 % kaikesta tallennetusta videosta päättyy tarkastettavaksi ja analysoitavaksi. Tästä herää yhtä lailla kysymys, että miksi ihmiset kokevat kameravalvonnan uhkakuvaksi, koska pääosin sitä käytetään jokaisen henkilön oikeusturvan takeena. Videotallenne poliisitoiminnassa on periaatteessa lähes ainut sellaisenaan hyvin varteenotettavan näyttöarvon antava todiste. Verratessa sitä silminnäkijähavaintoon tai paikalta taltioituun biometriseen DNA-tunnisteeseen, on videotallenne ainut mistä voidaan lähes varmuudella todeta tapahtumien todellinen tilanne. Olettaen tietenkin, että tallenne on tarpeeksi hyvälaatuinen ja sen

luotettavuudesta ja eheydestä on huolehdittu riittävästi siten, että sitä ei ole esimerkiksi manipuloitu leikkaamalla tai käsitelty digitaalisesti.

Uhkakuva viranomaisen tarkkailusta tuntuu myös erikoiselta, kun tarkastelee sitä tiedon määrää mitä ihmiset luovuttavat vapaaehtoisesti suuryrityksille. Ottaen huomioon vielä sen, että lähestulkoon kaikkien henkilöiden taskussa oleva älypuhelin ei ole enää suomalaista tekoa, vaan se on kasattu Kiinassa ja verkotettu Yhdysvaltoihin. Kahden maailman suurimman tiedusteluviranomaisen vastuulle, joilla on Edward Snowdenin paljastusten ja Kiinan totalitarismin myötä suora pääsy oman maansa sisällä tallennettuun dataan. Näitä tahoja vastaan on Euroopassa reagoitu vahvasti siten, että eurooppalaisia ihmisten perusoikeuksien vaalimiseksi on säädetty lakeja kuten GDPR. Kaikki Euroopan unionin jäsenmaat ovat ottaneet ne käyttöön ja jalkauttaneet niitä jopa osittain hyvällä menestyksellä aivan käytännön tasolle. Onkin tärkeää huomioida, että Euroopan unionissa panostetaan niin rahallisesti kuin regulaation pohjalta todella laajasti siihen, että voidaan kehittää ja käyttää luotettavia tekoälyohjelmistoja. Näiden tuominen valvontakameroihin entisestään vaatii käyttäjiä kiinnittämään huomiota säädettyyn tieto- ja henkilönsuoja kysymyksiin.

Suomi, joka on maailman onnellisin ja yksi vähiten korruptoituneista valtioista, mainostaa myös itseään yhtenä kyberturvallisuuden mallimaana. Täällä kameravalvonnalle ja siinä hyödynnettävälle tekoälylle ei kuitenkaan ole suoraa omaa lainsäädäntöä. Kysyttäessä ensimmäiseltä vastaantulevalta henkilöltä kuvailemaan omin sanoin mitä Euroopan unionin yleinen tietosuoja-asetus koskettaa häntä. Olisi vastauksena varmaankin ainoastaan hämmästynyt ilme. Tarkennettaessa kyselyä mainitsemalla GDPR, voisi henkilö ehkäpä jopa osata sanoa, että se liittyy jollain tapaan yritysten tapaan käsitellä hänen antamiaan tietoja. Tästä voi vetää hyvin johtopäätöksen siitä, että ihmisten yleinen tuntemus lainsäädännöstä on heikolla tasolla. GDPR:n yhtenä tavoitteena ja kulmakivenä on, että säädetyt ohjeistukset ovat normaalin kansalaisen ymmärrettävissä ja tarvittaessa hän saisi näistä lisätietoa. Tutkimuksen myötä on tullut ilmi, että kameravalvontaan ja etenkin henkilötietojen käsittelyyn liittyy useita satoja eri lakeja. Mikäli kameravalvontaa kohden luotaisi oma lainsäädäntönsä se olisi kuitenkin riippuvainen kymmenistä muista laeista. Tämä tekisi siitä edelleen hyvin vaikeasti tulkittavan ja äärimmäisen kankean toteuttaa ja uudistaa. GDPR:n myötä uusien ohjelmiston hyödyntäminen pakottaa toimijat avaamaan henkilötietojen käsittelyä. Lisäksi viranomaistahot kuten poliisi ovat äärimmäisen sidottuja toimivaltapykäliinsä, milloin heillä on oikeus suorittaa valvontaa. Tämä toiminta on jatkuvan laillisuusvalvonnan alaisuudessa ja etenkin erityisten henkilötietoryhmien käyttöön kohdistetaan suuren riskitason takia toistuvaa valvontaa. Lisäksi nykyinen tiedonhallintalaki pakottaa julkiset tahot ilmoittamaan, kun ne käyttävät henkilötietojen käsittelyyn uusia teknologioita. Onkin tärkeää, että teknologian kehittyessä suurin harppauksin tulee valvovan viranomaisen ohjata ketterästi teknologian käytön rajoja. Tämä mahdollistuu ainoastaan toimintaa ohjaavalla kevyellä säätelyllä ja ohjeistuksella. Laillisuusvalvontaviranomaisen tulee pystyä tuomaan regulaation tulkintaan kansankielelle, jotta sitä voidaan paremmin jalkauttaa käytäntöön yritysten ja viranomais-

ten toimesta. Aktiivinen ja läpinäkyvä vuoropuhelu korostuu, koska silloin voidaan nopeasti reagoida ja oppia välttämään virheellisiä tulkintoja ja teknologian väärää käyttöä. Kaiken toiminnan taustalla tulee aina olla ihmisen eli rekisteröidyn oikeudet. Ei pidä kuitenkaan unohtaa sitä, että yksilöoikeuksia käytetään tarkoituksella väärin rikoksentekijän toimesta ja niitä rikottaessa piiloudutaan niiden oikeuksien taakse, joita rikoksentekijä itse tarkoituksella yrittää loukata.

8.1 Varautuminen ja tulevaisuus

Kameravalvonnan rooli rikosten selvittämisessä, ennalta estämisessä ja paljastamisessa on merkittävä. Kameravalvontaa hyödynnetään sellaisenaan myös tilannekuvan muodostamisen tukena. Tekoälyn myötä kameravalvonta on saamassa merkittävää jalansijaa myös tiedolla johtamisen saralla. Datan ja siitä tehtävän analyysitiedon voidaan hyvin todeta olevan nykyajan öljyä. Kameravalvonnasta datavirtaa kertyy äärettömän paljon ja tulevaisuudessa siitä voidaan hyödyntää monikymmenkertainen määrä. Kameravalvonnan osalta elämme kuitenkin vielä hyvin vanhankaltaisessa toimintaympäristössä. Vaikka verkkoon kytketyt IP-kamerat ovat vallanneet markkinat, iso osa valvontakameraverkoista toimii suljetussa ympäristössä. Tämä toki johtuu osaltaan tietoturvakysymyksestä, vaikka tulevaisuus näyttääkin pilviseltä. Tällä tarkoitetaan sitä, että verkkojen nopeutuessa, etenkin 5G:n myötä, halusimme tai emme pilviratkaisut ovat kustannuksiltaan ja skaalautuvuudeltaan ainoa järjellinen ratkaisu.

Tarkasteltaessa kameravalvonnasta julkisesti esillä olevia tietosuojaselosteita huomaa, että jotakuinkin jokaisessa henkilötietoja sisältävässä kameravalvontarekisterissä tietojenluovutuksen kohteena on mainittu poliisi. Maamme sisäisestä turvallisuudesta vastaava taho, perustaa isolta osin rikosten jälkijättöisen tutkinnan julkisten ja yksityisten tahojen kameravalvonnan varaan. Yhdysvalloissa tietyissä kaupungeissa on mahdollista kytkeä oma kameransa viranomaisen luomaan verkkoon, jonka kautta poliisilla on laillisen perusteen myötä mahdollista päästä tarkastelemaan materiaalia. Myös Suomessa kehitetään poliisin kykyä hyödyntää ja kytkeytyä julkisiin kameraverkkoihin. Isojen älykaupunkien rooli tässäkin suhteessa on merkittävä. Turvallisuuden kannalta onkin järkevää tulevaisuudessa luoda tekninen mahdollisuus hyödyntää jo olemassa olevaa kameravalvontaa kansalaisten turvallisuuden parantamiseksi. Tekoäly tuo mahdollisuuden aivan oikeasti jopa ennalta estää rikoksia ilman ihmisen reagointia. Kameran analysoima tappelu voi pahimmassa tapauksessa johtaa ihmisen kuolemaan tai hieman syrjäisempään sijaintiin talviyönä sairaskohtauksen saanut henkilö voi paleltua hengiltä. Tekoälyn keinoin tilanteisiin voidaan reagoida niiden tapahtuessa. Ei myöskään pidä unohtaa Euroopassa muuttunutta turvallisuustilannetta, jossa erilaisista isommista väkivallanteoista on tullut osa suomalaistakin arkipäivää. Viranomaisella tulee olla kyky reagoida näihin tilanteisiin ja teknisesti tarjota mahdollisuus hyödyntää uutta tekno-

logiaa. Esimerkiksi kohteeseen kuvaavilla tekoälyä hyödyntävillä kameroilla. Toiminta pitää kuitenkin olla läpinäkyvää ja myös jälkijättöisesti tarkastellen perusteltua sekä selvitettävissä.

Tekoälyn hyödynnettävyys pitää myös pystyä konkretisoimaan äärimmäisissäkin tilanteissa. Tutkimuksen aikana jyllännyt koronaviruspandemia todisti sen, että osaltaan hyvin yksilön oikeuskeskeinen ajattelutapa on kankea reagoimaan pandemian kaltaisissa poikkeusoloissa. Esimerkiksi kasvojentunnistuksen ja siitä johdetun tartuntalaskelman keinoin, olisi todennäköisesti pystytty paremmin selvittämään koronatartunnan saaneita ihmisiä. Myös näiden ihmisten lähipiirissä tarpeeksi pitkään oleskelleet olisi voitu tunnistaa ja saattaa sairaalaan tarkastettavaksi. Nyt etenkin Eurooppa yllätettiin ja vapaan liikkuvuuden vuoksi pandemia levisi nopeasti kaikkiin Euroopan maihin. Tämä johti laajaan terveydenhoidolliseen katastrofiin. Tekoälyä on pystyttävä hyödyntämään tehokkaammin, silloin kun siihen tulee laillinen peruste, esimerkiksi tässä tapauksessa poikkeuslakien nojalla. Tällöin teknisiä esteitä on purettava, jotta toiminta on ylipäätään toteutettavissa. Euroopan tietosuojaneuvosto laati kohtuullisen nopealla aikataululla GDPR:n pohjautuvia ohjeistuksia siitä miten poikkeusoloissa koronapandemian aikana toimia. Esimerkiksi viranomaisille mahdollistettiin televalvontatietojen käyttö tartunnan saaneiden tavoittamiseksi (EDPB COVID-19, 2020). Nopealla reagoinnilla säästetään ihmishenkiä. On kuitenkin myös tärkeää, että tekoälyn käyttö on tarkoin säädelty ja valvottu. Pandemian kaltaisten poikkeusolojen loputtua, käytön peruste lakkaa ja rakennetut järjestelmät on laitettava pois päältä tai purettava. Esimerkkinä Yhdysvalloissa tapahtuneen terrorismihyökkäyksen jälkeen säädetyt poikkeuslait ovat edelleen voimassa. Tämä osoittaa, että lait ovat liian kankeita reagoimaan nopeasti tapahtuviin tilanteisiin ja ne jopa voivat kääntyä itseään vastaan, etenkin teknologian nopean kehittymisen vuoksi.

8.2 Tutkimuksen luotettavuus ja eettisyys

Tutkimuksen luotettavuuden määrittely ja tutkijoiden omat vaikutukset tutkimuksen objektiivisuuteen, on huomioitava jo suunnitteluvaiheessa. Hyvää tutkimusta ohjaa strukturoitu tyyli ja tutkimusmenetelmät. Materiaalin läpinäkyvyys ja eettiset tavat tiedonkeruulle ovat laadukkaan tutkimuksen mittareita. Myös eettisiin ongelmiin tulee varautua jo luodessa tutkimusstrategiaa (Kuula, 2006, s. 11-13). Tutkittavan aiheen määrittäminen sekä rajaaminen on tutkijan ensimmäinen eettinen valinta. Tähän toki vaikuttaa vahvasti tutkijan oman halu ryhtyä tutkimaan aihetta, mutta myös tutkijan eletty elämä ohjaa hänen tulevia päätöksiään. Tämän vuoksi onkin tärkeää ymmärtää oman valinnan perusteet ja kohdella tutkimuksessa mukana olevia tahoja eettisesti. Omaa työskentelyä tulee arvioida koko tutkimuksen aikana (Hirsjärvi ym. 26-27). Laadullisessa tutkimuksessa käsitellyt henkilöt, paikat ja näihin kytkeytyvät tapahtumat, kuten haastattelut tulee käsitellä tutkimuksessa läpinäkyvästi ja tarkasti. Tämä

turvaa tutkimuksen tuottamien tulosten paikkansapitävyyttä (Hirsjärvi ym., 2004, s. 216-217).

Laadukkaaseen tutkimukseen sitoutuu vahvasti tutkimuksen reliabiliteetti, josta käytetään myös nimiä luotettavuus tai validiteetti. Näitä termejä voidaan käyttää kvalitatiivisessa tutkimuksessa vaikkakin se ei ole niin yleistä kuin kvantitatiivisen tutkimuksen puolella (Hirsjärvi ym., 2004, s. 216-217). Tutkimuksen kattavuus vahvistaa sen reliabiliteettia, joten aineiston kyllääntyminen on otettava tutkimuksessa teoriaosuudessa huomioon. Tarpeeksi laaja tiedon keruun ja sen monipuolinen käyttö avaa uusia näkökulmia tutkimukseen. Kuitenkin liian laajan alueen käsittely voi viedä tutkimusta väärille urille, kun taas liian suppea aineisto ei tuota tarpeeksi luotettavaa lopputulosta. Tiedonkeruun aikana saturaatiopisteen löytymistä voidaan hyödyntää aineiston riittävyyden mittaamisessa. Tällöin tutkija havaitsee, että aihealueesta kerätty tieto alkaa toistaa itseään, eikä se tuota enää tutkimusongelman kannalta uutta tietoa (Hirsjärvi ym., 2004, s. 171).

Tutkijatriangulaation avulla tutkimuksessa pyritään varmistamaan tarpeeksi laaja aineiston keruu, jota tarkastellaan tutkimuksen aikana säännöllisesti tutkijoiden välisessä vuorovaikutuksessa. Kyllääntymisen havaitseminen on tukijakohtaista ja vasta molempien havaittua aineiston saturaatiopiste, voidaan aineiston määrää alkaa rajoittaa. Koska tutkimuksen tekijöitä on kaksi tutkimuksessa säilytettävä materiaali ja lähteet säilötään pilvipalveluun. Näin molemmilla tutkijoilla on mahdollisuus tarkastella kaikkia tutkimuksessa löydettyjä lähteitä. Toiminnalla mahdollistetaan hyvin läpinäkyvä aineiston käsittely ja vahvistetaan tutkimuksen reliabiliteettia.

Tutkimusprosessin alussa sen valmisteluun käytetään molempien tutkijoiden asiantuntemusta. Lisäksi käydään läpi paljon aiheesta jo tehtyä tutkimusta sekä selvitystä. Aiemman tutkimuksen avulla tutkimuskysymysten selkeämpi määrittäminen ja linjaaminen takaa oikeiden asioiden tutkimisen. Lisäksi vuoropuhelu tutkimuksen tilaajan kanssa vahvistaa valintojen validiteettia. Tutkijatriangulaation lisäksi tilaajan kanssa käydään vuoropuhelua koko tutkimuksen ajan, jolloin voidaan varmistua tutkimuksen tuottavan tietoa heidän käytännön ongelman kontekstissa. Tutkijat pystyvät näin ollen hyödyntämään tiedonkeruussa juuri oikeita tilaajaan liittyviä yksityiskohtia. Tutkijoiden tulee kuitenkin huomioida, että tutkimustyö ja tulos on objektiivinen, sekä tilaajan kanssa tehty yhteistyö on eettisesti ja moraalisesti tutkimusetiikan mukaista.

8.2.1 Luotettavuuden ja eettisyyden arviointi

Tutkijoiden välinen kommunikaatio ja tiedonvaihto sujui todella hyvin, mikä vahvisti tutkijatriangulaation toteuttamista. Yliopiston tekniset toteutukset kuten pilvipalvelu ja etäpalaverisovellus mahdollistivat niin tutkijoiden välisen kommunikaation kuin tilaajan kanssa tehdyn tiedonvaihdon. Poikkeusoloissa läpiviety tutkimus ei olisi onnistunut ilman kunnollisia etätyömahdollisuuksia. Tosin tutkimuksen ajoitus onnistui kohtuullisin hyvin, koska kirjastojen sulkeutuessa tutkijat olivat ehtineet lainata suurimman osan tutkimuksessa käytettä-

västä kirjallisesta materiaalista. Myös osa kirjallisuuskatsauksen lähteistä pystyttiin hankkimaan verkon kautta, esimerkiksi lukuiset hallitusten esitykset ja muut lakilähteet.

Tutkimuksen pätevyyttä arvioidaan tutkimusmenetelmien sopivuudella selvitettävän aiheen tutkimiseen. Tapauksen kompleksisuuden ja kohtuullisen laajan tutkimuskokonaisuuden vuoksi tutkimusmenetelmiä valittiin useampi. Tutkimuksen kulku oli siis tietyllä tavalla monitahoinen, mutta se ei sekoittanut tutkimuksen kulkua vaan päin vaistoin helpotti tutkimuksen jäsentelyä. Toimintatutkimukselle tyypillistä kommunikaatiota tilaajan kanssa jatkettiin säännöllisesti koko tutkimuksen ajan. Tutkijat myös osallistuivat tilaajan järjestämään työpajaan, jossa osaltaan tuotiin esille tutkimuksen aikana esiin tulleita näkemyksiä ja tulkintoja. Työpajan avulla tutkimuksen suuntaan pystyttiin vielä entisestään tarkentamaan.

Tutkimuksen teoreettisen viitekehyksen valmistettua kerättiin aineisto yhteen, jonka avulla pystytiin havaitsemaan tutkimuksen ydinkategoriat. Tässä vaiheessa tutkijat toimittivat teoriaosuuden materiaalin ja alustavat teemahaastattelurungot tilaajalle kommenteille. Saadun palautteen avulla tutkimuksen fokusta tarkennettiin entisestään. Yhteistyö tilaajan kanssa auttoi merkittävästi tutkijoita tunnistamaan tilaajalle kriittisiä, jopa yksittäisiä tekoälyn käyttötapauksia. Näin teemahaastatteluihin onnistuttiin valitsemaan juuri oikeat tahot ja kysymysten asettelulla pystyttiin vastaamaan tilaajan arjessa eteen tulleeseen ongelmaan.

Arvioitaessa kvalitatiivisen tutkimuksen luotettavuutta ei pidä unohtaa tutkijoiden objektiivisuuden arviointia. Eritoten tämä korostuu fenomenografisessa tutkimusmenetelmässä. Tutkijoiden oma asiantuntemus ja työkokemus koettiin kuitenkin enemmänkin positiiviseksi asiaksi, koska sen avulla tutkimusta osattiin kohdentaa jo alkuvaiheessa. Lisäksi haastateltavien puolelta saatu palaute asiantuntevasta ja hyvin kohdistetuista ja alustetuista kysymyksistä korosti tutkimuksen luotettavuutta. Tutkijat myös kokivat äärimmäisen tärkeäksi sen, että teoriavaiheessa syntyneitä johtopäätöksiä voitiin vertaisarvioida tutkijoiden välillä. Teemahaastattelujen myötä johtopäätöksiä haastettiin eri asiantuntijoiden kesken, jolloin tukijoiden kuin tutkimuksen tulosten objektivisuus ja paikkansapitävyys pystyttiin paremmin varmistamaan.

8.3 Jatkotutkimusmahdollisuudet

Tämänkin tutkimuksen yhtenä perusteena oli aiheeseen liittyvän tutkimuksen puute ja kameravalvontaan sekä tekoälyyn kohdistuvan ohjeistuksen sekä linjausten vähäisyys. Mitä syvemmälle aihepiiriin tarkastelu eteni, sitä selkeämmin tuli esille, että kameravalvonnassa käytettävän tekoälyn perusteellista linjanvetoa ja käsitteiden avaamista ei ole kunnolla toteutettu. Tämä johtuu osaltaan siitä, että lainsäädäntö on uutta ja vasta lähivuosien aikana teknologian kehitys on mahdollistanut tekoälyn laajemman käytön juuri kameravalvonnassa.

Aiheeseen liittyviä jatkotutkimusmahdollisuuksia on laajasti ja tutkimusta tehdäänkin monella rintamalla. Kaupalliset toimijat kehittävät omia tekoälyalgoritmeja ja vievät teknologista kehitystä eteenpäin. Tekoälytutkimus onkin monen kaupallisen tahon markkinointivaltti. Myös akateemisessa maailmassa tutkimusta toteutetaan, sillä myös Suomessa useampi yliopisto ja korkeakoulu on ottanut opintotarjontaansa tekoälyä, kyberturvallisuutta ja robotiikkaa.

Tämän tutkimuksen osalta nousi selkeästi esille se, että yleisellä tasolla tehtävä tekoälyn ja kameravalvontaan kohdistuvien mielipiteiden perustaksi pitäisi tehdä faktapohjaista tutkimusta. Mielipiteet vaikuttavat vahvasti myös poliittiseen päätöksentekoon, mikä ohjaa budjetointia ja ylipäätään mahdollisuuksia. Tekoälyn uhkakuvien sijaan pitäisi pystyä keskustelemaan mahdollisuuksista ja ratkaisuista, millä tavoin kehitystä voidaan rakentaa luottamusta ja läpinäkyvyyttä tukien.

Kameravalvonnan ja tekoälyn käyttäjinä toimii vielä periaatteessa kolme erityyppistä instanssia eli yksityinen ja julkinen puoli sekä viranomaispuoli. Näitä koskeva regulaatio kuin valvontakin on hyvin erityyppistä. Kameravalvonnan osalta tiedon käyttö ja hyödynnettävyys kulkevat kuitenkin isoilta osin käsikädessä. Ihmisiin kohdistuva valvonta etenkin valtiotasolta on GDPR:ssä määritetty korkea tason uhkaksi. Ilman valvontaan yhteiskunta luisuisi kuitenkin anarkiaksi. Usein myös huomio kiinnittyy lakia rikkovan tahon oikeuksiin, ja vahinkoa kärsineen tuska hukkuu oikeustaisteluun. Jatkotutkimuksen kannalta olisikin hyvä pohtia ja vertailla tarkemmin niin yksityisen ja julkisen sektorin kuin viranomaisten suorittaman valvonnan menetelmiä, niihin kohdistuvaa valvontaa sekä toiminnan tarkoitusperiä. Suomessa viranomaisten toimivalta on täysin sidottu lakiin. Tämä tekee toiminnasta hyvinkin läpinäkyvää. Tärkeää olisikin tuoda esille käytännön tasolla niitä tarpeita mitä viranomaisella olisi ja mitä varten sen tulisi pystyä tehokkaammin suoriutumaan tehtävistään. Olisi myös hyvä tutkia millä tavoin yhteistoimintaa voitaisiin tehostaa yksityisen tahon puolelta. Avaamalla toimintaa käytännön tasolla faktoihin ja tilastoihin vedoten, olisi kansalaistenkin helpompi ymmärtää siitä mihin tekoälyä ja kameravalvontaa viranomaistasolla hyödynnetään. Tämän tutkimuksen myötä tuli hyvin selväksi, ettei viranomaisella kuin muullakaan julkisella puolella ole mahdollisuuksia, resursseja, saati halua kohdistaa kansalaisiin Kiinan valtion tyylistä diktatuurimaista valvontaa. Suomalaisessa demokratiassa rehellisyys ja läpinäkyvyys ovat tärkeimpiä arvoja, ja lainkuuliaisuus on sen yksi ilmenevä muoto. Ohjeiden ja säännösten noudattamisessa olemme hyviä niin yksittäisinä kansalaisina kuin viranomais- ja valtiotasolla. Se, että oikeusasteisiin ja mediaan päätyy tietoja väärinkäytöksistä ja ne herättävät runsasta julkista keskustelua, kuvastaa valtiomme läpinäkyvyyttä. Tämä on kansamme vahvuus ja jonka tukemiseksi alueeseen kohdistuva faktoihin pohjautuva tutkimus on äärimmäisen tärkeää.

LÄHTEET

Aamulehti. (2018). Tampere lisää rajusti kameravalvontaa. Haettu 9.2.2020 osoitteesta https://www.aamulehti.fi/a/201291658

Aithority. (2019). Top Countries and Cities by number of CCTV Cameras. Haettu 10.2.2020 osoitteesta https://www.aithority.com/news/top-10-countries-and-cities-by-number-of-cctv-cameras/

Alastalo, M., & Åkerman, M. 2010. Asiantuntijahaastattelun analyysi: faktojen jäljillä. Teoksessa Ruusuvuori J. Nikander P. & Hyvärinen, M. (toim.) Haastattelun analyysi. Tampere: Vastapaino.

Allied Market Research. (2017). Video Surveillance Market Outlook 2025. Haettu 20.1.2020 osoitteesta https://www.alliedmarketresearch.com/Video-Surveillance-market

Automated Detection of Firearms and Knives in a CCTV image. (2016). Haettu 31.3.2020 osoitteesta https://www.mdpi.com/1424-8220/16/1/47/htm

Axis. (2019). What are the cybersecurity issues in video surveillance. Haettu 1.3.2020 osoitteesta https://www.axis.com/blog/secure-insights/what-are-the-cybersecurity-issues-in-video-surveillance/

BBC. (2019). South Wales Police use of facial recognition ruled lawful. Haettu 7.4.2020 osoitteesta https://www.bbc.com/news/uk-wales-49565287

Central Intelligence Agency. The Enigma of Alan Turing. Haettu 11.3.2020 osoitteesta https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/the-enigma-of-alan-turing.html

Cheng, K., Lubamba, E., Tahir, R. & Maozhen, L. (2020). Capsule recurrent neural network with weight update using dynamic routing by agreement: A unified model for action recognition in videos. Springer Nature Switzerland AG.

CNN. (2019). Move over TSA PreCheck. Long live Clear. Haettu 6.4.2020 osoitteesta https://edition.cnn.com/travel/article/clear-airport-security/index.html

Edilex. (2019). Hovioikeus : Polttoaineen anastamisesta epäillyn henkilön nimen ja kuvan julkaiseminen Facebookissa loukkasi tämän yksityisyyttä.

EDPB 3/2019. (2020). Guidlines on processing of personal data through video devices. European Data Protection Board.

EDPB. (2020). European Data Protection Board. Haettu 1.4.2020 osoitteesta https://edpb.europa.eu/edpb_fi

EDPB COVID-19. (2020). Statement on the processing of personal data in the context of the COVID-19 outbreak. Haettu 25.5.2020 osoitteesta https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

Elements of AI. 2020. Miten tekoäly määritellään. Haettu 11.3.2020 osoitteesta https://course.elementsofai.com/fi/1/1

Elmenreich, W. Recsearch Report 47/2001. An Introduction to Sensor Fusion

Erillisverkot. (2019). Drone on nykypäivän tähystystorni rajalla. Haettu 3.4.2020 osoitteesta https://erveuutiset.erillisverkot.fi/drone-on-nykypaivan-tahystystorni-rajalla/

EOAK. Eduskunnan oikeusasiamiehen kanslian päätös EOAK/3379/2018.

Esteva, A., Kuprel, B., Novoa, R., Ko, J., Swetter, S., Blau, H., Thrun, S. (2017) Dermatologist-level-classification of skin cancer with deep neural networks. Yhdysvallat: Stanford University

Euractiv. (2020). LEAK. Comission considers facial recognition ban in AI white paper. Haettu 15.5.2020 osoitteesta https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/

Euroopan parlamentin ja nevoston asetus (EU) 2016/679.

Eskola, J. & Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

ESRC. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. London: Economic & Social Research Council

Euroopan komissio - Horisontti. (2014). Euroopan unionin tutkimuksen ja innovoinnin puiteohjelma. Luxemburg: Euroopan unionin julkaisutoimisto. 2014

Euroopan komissio. (2019). Luotettavaa tekoälyä koskevat eettiset ohjeet. Brysseli: Euroopan komissio

Euroopan komissio. (2020). Tekoäly - huippuosaamista ja luottamusta. Haettu 15.4.2020 osoitteesta https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_fi

Euroopan komissio - COM (2020). White paper on Artificial Intelligence - A European approach to execellence and trust. COM(2020) 65 Final.

Finanssiala. (2010a). Kameravalvontaopas. Haettu 14.2.2020 osoitteesta https://www.finanssiala.fi/vahingontorjunta/dokumentit/Kameravalvontaopas.pdf

Finanssiala. (2010b). Kameravalvonnan suunnitteluohje. Helsinki: Finanssiala ry.

Finavia. (2019). Konenäön avulla voidaan tehostaa lentokentän toimintoja. Haettu 3.4.2020 osoitteesta https://www.finavia.fi/fi/uutishuone/2019/konenaon-avulla-voidaan-tehostaa-lentokentan-toimintoja

Galar, D. & Kumar, U. (2017). eMaintenance - Essential Elextronic Tools for Efficiency. Academic Press.

GSA. (2020). LTE & 5G Market statistics - April 2020. Haettu 20.4.2020 osoitteesta https://gsacom.com/technology/5g/

HA 39/2018 vp Valiokunnan mietintö vp HE 242/2018

HE 9/2018 vp Hallituksen esitys Eduskunnalle EU:n yleisestä tietosuoja-asetusta täydentäväksi lainsäädännöksi

HE 57/1994 vp Hallituksen esitys Eduskunnalle poliisilaiksi ja eräiski siihen liittyviksi laeiksi.

HE 184/1999 vp Hallituksen esitys Eduskunnalle yksityisyyden, rauhan ja kunnian loukkaamista koskevien säännösten uudistamiseksi.

HE 75/2000 vp Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi.

HE 59/2002 vp Hallituksen esitys Eduskunnalle työturvallisuuslaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 162/2003 vp Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta.

HE 257/2010 Hallituksen esitys Eduskunnalle pelastuslaiksi ja laiksi meripelastuslain 23§:n muuttamisesta

HE 22/2014 vp Hallituksen esitys Eduskunnalle laiksi yksityisistä turvallisuuspalveluista sekä eräiksi siihen liittyviksi laeiksi

HE 18/2018 Hallituksen esitys Eduskunnalle laeiksi pelastuslain muuttamisesta ja väliaikaisesta muuttamisesta sekä eräiksi muiksi laeiksi

HE 284/2018 vp Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.

Helsinki. (2019). YJT-kameroiden hankinnan valmistelun käynnistyminen. Haettu 5.3.2020 osoitteesta http://dev.hel.fi/paatokset/asia/hel-2019-003997/u02100vh2-2019-132/

Helsingin hovioikeuden ratkaisu diaarinumero R 18/2685, tuomion antamispäivä 4.12.2019

Helsingin sanomat. (2020). Julkisilla paikoilla tapahtuva kasvojentunnistus aiotaan kieltää väliaikaisesti – sääntely liian vaikeaa, liikaa riskejä. Haettu 3.4.2020 osoitteesta https://www.hs.fi/politiikka/art-2000006380255.html

Hikvision. (2019). 2018 environmental, social and governance report. Hangzhou: Hikvision

Hirsjärvi, S. & Hurme, H. (2000). Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirjärvi, S., Remes, P. & Sajavaara, P. (2009). Tutki ja kirjoita. Tammi. Kariston kirjapaino Oy. Hämeenlinna.

Hollywood, J. Vermeer, M. Woods, D. Goodison, B & Jackson A. (2018). Using video analytics and sensor fusion in law enforcement. RAND Corporation.

Hyacinth, B. (2017). The Future of Leadership. Rise of automation, Robotics and Artificial Intelligence. USA.

Hänninen, M. Laine, E. Rantala, K. Rusi, M & Varhela, M. (2017). Helsingin Kamari Oy. Vantaa: Hansaprint Oy.

IfSecGlobal. (2019). Genetec unseats Milestone as world´s biggest VMS vendor. Haettu 6.4.2020 osoitteesta https://www.ifsecglobal.com/video-surveillance/genetec-unseats-milestone-as-worlds-biggest-vms-vendor/

IHSmarkit. (2019). Security technologies: Top trends for 2020. Haettu 20.4.2020 osoitteesta https://cdn.ihsmarkit.com/www/prot/pdf/1219/IHS_Markit_Technology-Top_Trends_in_Security_Technologies_for_2020.pdf

Innovative Security. (2017). The world´s first security camera. Haettu 20.1.2020 osoitteesta https://innovativesecurity.com/the-worlds-first-security-camera/

Inside Privacy. (2020). European Commission Presents Strategies for Data and AI. Haettu 15.4.2020 osoitteesta https://www.insideprivacy.com/artificial-intelligence/european-commission-presents-strategies-for-data-and-ai-part-1-of-4/?_ga=2.15091062.1162833267.1586890716-1865939949.1586890716#more-10430

Intermin. (2019). Poliisin henkilötietolaki auttaa torjumaan rikollisuutta digiaikakaudella. Haettu 8.4.2020 osoitteesta https://intermin.fi/ajankohtaista/blogi/-/blogs/poliisin-henkilotietolaki-auttaa-torjumaan-rikollisuutta-digiaikakaudella

IPVM. (2019). Dahua wiretapping vulnerability. Haettu 5.4.2020 osoitteesta https://ipvm.com/reports/dahua-audio?code=allow

IPVM CCTV. (2019). CCTV Is the past, cloud video surveilance is the future. Haettu 20.4.2020 osoitteesta https://ipvm.com/reports/cctv-internet

ISO. (2019). ISO in brief. Haettu 25.4.2020 osoitteesta https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf

ISO 28000. (2012). Specification for security management systems for the supply chain. Haettu osoitteesta https://www.iso.org/standard/44641.html

Jokinen, A. & Juhila, K. (2002). Diskurssianalyysi liikkeessä. (2. painos). Vastapaino

Kiintolevyjen elinkaaren hallinta. (2016). Kyberturvallisuuskeskus ohje. Haettu 16.3.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-ylikirjoitus.pdf

Koivisto, R., Leikas, J., Auvinen, H., Vakkuri, V., Saariluoma, P., Hakkarainen, J. & Koulu, R. (2019).). Tekoäly viranomaistoiminnassa - eettiset kysymykset ja yhteyskunnallinen hyväksyttävyys. Helsinki: Valvioneuvoston kanslia.

Korja, J. (2016). Biometrinen tunnistaminen ja henkilötietojen suoja. Tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta (Akateeminen väitöskirja). Lapin yliopisto.

Kuntalehti. (2019). Kuntatalous ajautui kriisiin: Kaksi kolmest kunnasta teki negatiivisen tuloksen. Haettu 3.2.2020 osoitteesta https://kuntalehti.fi/uutiset/talous/kuntatalous-ajatutui-kriisiin-kaksi-kolmesta-kunnasta-teki-negatiivisen-tuloksen/

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitäminen yhteydessä. 1054/2018.

Laki julkisen hallinnon tiedonhallinnasta. 906/2019.

Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa. 30.3.2007/370.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. 1406/2011.

Laki yksityisistä turvallisuuspalveluista 1085/2015

LDV Capital. 2017. 45 billion cameras by 2020 fuel business opportunities. Haettu 20.4.2020 osoitteesta https://www.ldv.co/insights/2017

Leikas, J. (2008). Ikääntyvät, teknologia ja etiikka – näkökulmia ihmisen ja teknologian vuorovaikutustutkimukseen ja -suunnitteluun. VTT Working Papers; 110. Espoo: VTT

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. (2019). Arviointi, hyväksyntä ja neuvonta. Haettu 5.3.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. (2019). Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit. Haettu 5.3.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. (2019). Näin suojaudut tietomurroilta. Haettu 5.4.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. (2019) Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri. Haettu 14.2.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. (2020). Tietoturvan vuosi 2019. Kyberturvallisuuskeskuksen vuosikatsaus. Haettu 1.3.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_tietoturvanvuosi_2019_WEB_aukeamittain.pdf

Magossystems. (2020.) Solutions. Haettu 7.4.2020 osoitteesta https://magossystems.com

Marttinen, J. (2018). Palvelukseen halutaan robotti. Aula & Co. Helsinki.

Merilehto, A. (2018). Tekoäly: matkaopas johtajalle. Alma Talent. Helsinki.

Metropolitan Police Service. (2020). Live Facial Recognition Trials. Evaluation report. London: National Physics Laboratory

Metsämuuronen, J. (2000). Laadullisen tutkimuksen perusteet. Helsinki: METHELP.

Milestone. (2020). Marketplace. Haettu 6.4.2020 osoitteesta https://www.milestonesys.com/community/marketplace/start-exploring/?index=0&country=FI&usage=HumDet

Milestone Marketplace. (2020). BriefCam. Haettu 6.4.2020 osoitteesta https://www.milestonesys.com/marketplace/briefcam-usa/briefcam-video-content-analytics-platform/

Milestone UXSS. (2020). Up Extreme Smart Surveilance. https://www.milestonesys.com/marketplace/aaeon-technology-europe-b.v/up-xtreme-smart-surveillance/

Määttä, T., Tolvanen, M., Väätänen, U., Kolehmainen, A., Myrsky, M. & Keinänen, A. (2012). Oikeudellisen ajattelun perusteita. Oikeustieteiden laitos. Joensuu.

Norton. (2020). How does facial recognition work? Haettu 4.2.2020 osoitteesta https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html

Nuutila, A., Majanen, M. (2009). RL 24 Luku Yksityisyyden, rauhan ja kunnian loukkaamisrikokset. Teoksessa Rikosoikeus 2009, 3 uudistettu painos. Helsinki 2009.

OASC. (2020). About Open & Agile Smart Cities. Haettu 4.2.2020 osoitteesta https://oascities.org/about-oasc/

Oikeusministeriö. (2020). Automaattisen päätöksentekoon liittyvät yleislainsäädännön sääntelytarpeet. Esiselvitys. Oikeusministeriö. Helsinki.

Oikeusministeriö. (2018). Uusi tietosuojalaki voimaan vuoden 2019 alusta. Haettu 31.3.2020 osoitteesta https://oikeusministerio.fi/artikkeli/-/asset_publisher/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta

Oulu. (2019). Tietosuojaseloste keskitetyn kameravalvonnan rekisteri. Haettu 5.3.2020 osoitteesta https://www.ouka.fi/documents/5340458/18571431/Keskitetyn+kameravalvonnan+rekisteri.pdf/115dd56a-0a70-4b9b-883f-0ea44536a198

Pelastuslaki. 379/2011.

Pelastustoimi. (2014). Selvitys alueellisen pelastustoimen synnystä. Pelastuslaitosten kumppanuusverkoston julkaisu 3/2014. Haettu 1.5.2020 osoitteesta https://www.pelastuslaitokset.fi/upload/1456325740_pelastustoimensynty.pdf

Pelastustoimi. (2020). Onnettomuuksien ehkäisy. Haettu 1.5.2020 osoitteesta https://www.pelastustoimi.fi/pelastustoimi/onnettomuuksien-ehkaisy

Perustuslaki. 731/1999.

Philips, J., Yates, A., Hu, Y., Hahn, C., Noyes, E., Jackson, K., Cavanos, J., Jeckln, G., Ranjan, R., Sankaranaraynan, S., Chen, J., Castillo, C., Chelappa, R., White, D & Toole, J. (2018) Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. PNAS. 2018

Physicsworld. (2019). AI gears up for data analysis. Haettu 4.2.2020 osoitteesta https://physicsworld.com/a/ai-gears-up-for-data-analysis-making-the-most-of-machine-learning/

Pietikäinen, M., Silvén, O. 2019. Tekoälyn haasteet – koneoppimisesta ja konenäöstä tunnetekoälyyn. Oulu: Konenäön ja signaalianalyysin keskus

Pikaar, R., Koningsveld, E. & Settels, P. (2007). Meeting diversity in Ergonomics. Elsevier Ltd

PngWave. (2020). DIKW-pyramid. Haettu 4.2.2020 osoitteesta https://w0.pngwave.com/png/118/322/dikw-pyramid-knowledge-data-information-system-wisdom-others-png-clip-art-thumbnail.png

Poliisi. (2020). Poliisin sisäisen ja ulkoisen viestinnän käsikirja. Haettu 15.3.2020 osoitteesta https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/15034_POLIISI_viestintakasikirja_v090511.pdf?30307aa9fc6ed588

Pouta. (2020). Pouta-palvelu. Haettu 6.3.2020 osoitteesta https://www.poliisi.fi/turvallisuus_ja_valvonta/pouta_palv elu

Puolustusministeriö. (2015). Tietoturvallisuuden auditointityökalu viranomaisille. Haettu 14.2.2020 osoitteesta https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Recsearchgate. (2018). Convolutional neural networks based fire detection in surveilance video. Haettu 25.4.2020 osoitteesta

https://www.researchgate.net/profile/Khan_Muhammad7/publication/323589806/figure/fig2/AS:601347682496517@1520383868279/Main-operations-of-a-typical-CNN-architecture.png

SDPA. (2019). Swedish Data Protection Authority. Decision ref. DI-2019-2221.

Suojelupoliisi. (2020). Vuosikirja 2019. Helsinki: Suojelupoliisi. Haettu osoitteesta https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/79308_SUPO_Vuosikirja_2019_FI_Low7.pdf?4dfcbdf8e2d6d788

Suomen kuvalehti. (2008). Suomessa on valvontakameroita toiseksi eniten Euroopassa asukasta kohden. Haettu 10.2.2020 osoitteesta https://suomenkuvalehti.fi/jutut/kotimaa/suomessa-on-valvontakameroita-toiseksi-eniten-euroopassa-asukasta-kohden/

Säkerhetspolisen. (2020) Årsbok 2019. Tukholma: Säkerhetspolisen. Haettu osoitteesta https://www.sakerhetspolisen.se/download/18.a5cd4be16dfd84e1716a5/1585209341505/Arsbok2019.pdf

Tampere. (2018). Liikenne- ja kaupunkikameroiden henkilörekisteri. Haettu 5.3.2020 osoitteesta https://www.tampere.fi/tiedostot/t/KLQ9pOMWz/Liikenne_ja_kaupunkikameravalvonnan_rekisteri_Tietosuojaseloste.pdf

Tietosuojalaki. 1050/2018.

Tietosuojalautakunta. (2016). 10/2016. Oikeutettu etu - Henkilötieto - Liikenteenkuvaaminen

Tietosuojaryhmän WB 29 ohje 17/FI. (2017). Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa EU 2016/679 tarkoitettu ”korkea riski”.

Tietosuojavaltuutettu. (2016). 423/452/2016. Valokuva oikeudellisena kysymyksenä.

Tietosuojavaltuutettu. (2019a). Onko kameravalvonta henkilötietojen käsittelyä. Haettu 2.2.2020 osoitteesta https://tietosuoja.fi/usein-kysyttya-kameravalvonta

Tietosuojavaltuutettu. (2019b). Henkilötietojen käsittely. Haettu 22.3.2020 osoitteesta https://tietosuoja.fi/henkilotietojen-kasittely

Tietosuojavaltuutettu. (2020). Pseudonymisoidut ja anonymisoidut tiedot. Haettu 23.3.2020 osoitteesta https://tietosuoja.fi/pseudonymisointi-anonymisointi

Tivi. (2019). Miten Stuxnet-virus pääsi Iranin ydinohjelman tietokoneelle? Yahoo: Sisäpiirilähde paljasta agenttien keinot. Haettu 2.5.2020 osoitteesta https://www.tivi.fi/uutiset/miten-stuxnet-virus-paasi-iranin-ydinohjelman-tietokoneelle-yahoo-sisapiirilahde-paljasti-agenttien-keinot/606825c3-bdc9-4abc-9075-4943d3d1fb9d

TSV 6610/182/18. (2019). Tietosuojavaltuutetun vastaus dnro 6610/182/18 kameravalvontaan liittyvästä henkilötietojen käsittelystä.

TSV käsittelyperusteet. (2020). Milloin henkilötietoja saa käsitellä? Haettu 23.3.2020 osoitteesta https://tietosuoja.fi/kasittelyperusteet

TSV vaikutustenarviointi. (2020). Vaikutustenarviointi tietosuoja-asetuksessa yksilöityjen käsittelytilanteiden johdosta. Haettu 30.3.2020 osoitteesta https://tietosuoja.fi/vaikutustenarviointi

Tuominen, H., Neittaanmäki, P., Niinimäki, E., Pölönen, I., Rautiainen, I., Äyrämö, S., Ruohonen, T., Nyrhinen, R. 2019. Tekoälyn perusteita ja sovelluksia. Jyväskylä: Informaatioteknologian tiedekunta

Työ- ja elinkeinoministeriö. 2019. Edelläkävijänä tekoälyaikaan. Tekoälyohjelman loppuraportti. Helsinki: Työ- ja elinkeinoministeriö

Työ- ja elinkeinoministeriö. 2018. Tekoälyajan työ: neljä näkökulmaa talouteen, työllisyyteen, osaamiseen ja etiikkaan. Työ- ja elinkeinoministeriön julkaisuja 19/2018. Helsinki: Työ- ja elinkeinoministeriö

Työ- ja elinkeinoministeriö. (2017). Ministeri Lintilä: Suomesta tekoälyn soveltamisen kärkimaa. Haettu 1.4.2020 osoitteesta https://tem.fi/artikkeli/-/asset_publisher/ministeri-lintila-suomesta-tekoalyn-soveltamisen-karkimaa

Schiphol. (2019). Travel with facial recognition pilot. Haettu 6.4.2020 osoitteesta https://www.schiphol.nl/en/download/1561967459/2oPvcpb9ZiCIsyueWES6yq.pdf

SmartTampere. (2019). Tampereelle yli 3 miljoonan EU-rahoitus kaupunki- ja tapahtumaturvallisuuden kehittämiseen. Haettu 4.2.2020 osoitteesta https://smarttampere.fi/tampereelle-yli-3-miljoonan-eu-rahoitus-kaupunki-ja-tapahtumaturvallisuuden-kehittamiseen/

Suomen standardisoimisliitto. (2014). 62676-1-1 standardi. Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1-1: järjestelmävaatimukset. Yleiset vaatimukset. Haettu osoitteesta

https://sales.sfs.fi/fi/index/tuotteet/SFS/CENELEC/ID2/6/285255.html.stx

Suomen standardisoimisliitto. (2014). 62676-1-2 standardi. Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1-2: Järjestelmävaatimukset. Videonsiirtoa koskevat suorituskykyvaatimukset. Haettu osoitteesta https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID2/6/297306.html.stx

Ulkoministeriö. (2020). EU-lakien suhde Suomen Lakiin. Haettu 1.4.2020 osoitteesta https://eurooppatiedotus.fi/suomi-ja-eu/eu-lakien-suhde-suomen-lakiin/

UK High Court of Justice. (2019). Haettu 7.4.2020 osoitteesta https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

US Congress. H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019. Haettu 5.4.2020 osoitteesta https://www.congress.gov/bill/115th-congress/house-bill/5515/text

Valtioneuvosto. (2019). Julkisen hallinnon pilvipalvelulinjaukset. Valtiovarainministeriön julkaisu 35/2018. Haettu 30.3.2020 osoitteesta http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161294/VM_35_2018_Julk_hallinnon_pilvipalvelulinjaukset.pdf?sequence=1&isAllowed=y

Valtioneuvosto. (2018). Tekoälyn kokonaiskuva ja osaamiskartoitus. Helsinki: Valtioneuvoston kanslia

Valtioneuvosto (2019). Tekoäly viranomaistoiminnassa – eettiset kysymykset ja yhteiskunnallinen hyväksyttävyys. Helsinki: Valtioneuvoston kanslia

Valtiovarainministeriö. (2020). Kansallinen tekoälyohjelma AuroraAI. Haettu 1.4.2020 osoitteesta https://vm.fi/tekoalyohjelma-auroraai

Valtionvarainministeriö. (2019). Kuntien digitalisaation kannustinjärjestelmä. Haettu 4.2.2020 osoitteesta https://vm.fi/kuntien-digitalisaation-kannustinjarjestelma

Valtiovarainministeriö. (2019). Luottamus Suomen kilpailuedun ja hyvinvoinnin lähteenä. Haettu 1.2.2020 osoitteesta https://vm.fi/documents/10623/10841416/Blomqvist-luottamus-kilpailuedun-l%C3%A4hteen%C3%A4.pdf/a70d0ace-de43-14cc-51c2-72240af8573c/Blomqvist-luottamus-kilpailuedun-l%C3%A4hteen%C3%A4.pdf

VM 22/2017. (2017). Ohje riskienhallintaan. Valtiovarainministeriö. Helsinki.

Valtiovarainministeriö. (2019). Palautekierros tiedonhallintalain tiedonhallinan kuvausten suosituksista. VM/977/00.01.00.01/2019

VM 8/2017. (2017). Tietoturvapoikkeamatilanteiden hallinta. Valtiovarainministeriö. Helsinki.

Viestintävirasto. (2016). Kiintolevyjen elinkaaren hallinta. Haettu 30.3.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-ylikirjoitus.pdf

Viestintävirasto. (2016) Lokien keräys ja käyttö - Ohje 4/2016.

Wired. (2019). Inside Finland's plan to become an artificial intelligence powerhouse. Haettu 11.3.2020 osoitteesta https://www.wired.co.uk/article/finland-artificial-intelligence-online-course

World Economic Forum. (2020). Global Risk Report. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

Yle. (2009). Yle - Valvontakameroilla tarkkaillaan jo omia perheenjäseniä. Haettu 20.1.2020 osoitteesta https://yle.fi/uutiset/3-5863160

Yle. (2019c). Poliisi ja Tulli saivat oikeuden automaattiseen kasvojen tunnistamiseen ihmisvirrasta. Haettu 8.4.2020 osoitteesta https://yle.fi/uutiset/3-10815487

Yle. (2019b). Oulun kaupungin ja poliisin kamerasopimus on tietosuojavaltuutetun mukaan ongelmallinen. Haettu 9.2.2020 osoitteesta https://yle.fi/uutiset/3-10995967

Yle. (2020a). Poliisi kokoaa kartastoa koko maan valvontakameroista. Haettu 20.3.2020 osoitteesta https://yle.fi/uutiset/3-11166610 [Viitattu 20.3.2020]

Yle. (2020b). Valtion kyberturvallisuusjohtajaksi valittu Rauli Paananen: Suomi on kyberturvallisuuden kärkimaita. Haettu 1.3.2020 osoitteesta https://yle.fi/uutiset/3-11230455

LIITE 1 - HAASTATTELUKYSYMYKSET

1. **Kameravalvontaan liittyvä regulaatio**
   - Miten määritellään kameravalvontakuva ja missä vaiheessa se luokitellaan henkilötiedoksi ja erityiseksi henkilötiedoksi?
   - Miten muun datan yhdistäminen ja ns. sensorifuusio vaikuttavat henkilötietojen luokitteluun?
   - Erityisten henkilötietojen, kuten biometristen tunnisteiden osalta soveltuva, GDPR 2 luku 9 artikla i kohta ”käsittely on tarpeen kansanterveyteen liittyvän yleisen edun vuoksi”, minkälaisissa tilanteissa ko. kohta soveltuu? Soveltuuko kasvojentunnistusteknologian käyttö?
   - Tulisiko kasvojentunnistusteknologian lainsäädäntöä keventää?
   - Mitkä lait tai säädökset määrittelevät henkilötietojen ja erityisten henkilötietojen datan säilyttämisen vaatimukset Suomessa? Onko lainsäädännössä eroja julkisen ja yksityisen sektorin osalta?
   - Onko lainsäädäntö tällä hetkellä riittävän selkeä kameravalvonnan ja tekoälyteknologian käytön suhteen?
   - Rajoittaako lainsäädäntö kameravalvonnan kykyjä tällä hetkellä?
   - Pitäisikö Suomessa olla kansallinen erityislainsäädäntö tekoälylle ja kameravalvonnalle? Kyllä / Ei? Perustele vastaus
     - Onko lainsäädäntö tasapuolinen yksityisellä, julkisella ja viranomaissektorilla?

2. **Kameravalvonnasta muodostuvat henkilötiedot**
   - Kaupunkikamerajärjestelmät kuvaavat kaupungissa yleisiä paikkoja. Kamerat ovat sijoitettu ylös, jotta suoranaisesti niistä henkilöitä ei ole tunnistettavissa. Kameroilla on kuitenkin mahdollista tarkentaa kuvaa siten, että henkilö on niistä täysin tunnistettavissa. Lisäksi kameroiden kuvamateriaalia voidaan hyödyntää muiden tietojen kanssa, jolloin henkilö on tunnistettavissa. Tällöin voidaan olettaa kameramateriaalia olevan GDPR:n artikla 4 mukaisesti henkilötietoja. Kamerat kuvaavat mielenilmauksia tai muita poliittisia tapahtumia, joita järjestetään kaupungeissa. Materiaalista on selvitettävissä esimerkiksi henkilön poliittinen mielipide ja henkilö voidaan materiaalia kautta yksilöidä. Onko kyseessä tällöin erityinen henkilötietoryhmä ja voidaanko tällaista materiaalia tallentaa. Voidaanko tällaista materiaalia hyödyntää ja millä perustein?
   - Miten eräässä (South Wales Police) tapauksessa voitiin käsitellä sellaisten ihmisten biometrisia tunnisteita, joita ei ole syötetty “etsintäkuulutuslistalle”? Yleiselle paikalle asennettu kamera kuvaa kaikki kohteet ja tekee vertailua etsittävän henkilön biometrisen tunnisteen perusteella. Henkilön kasvokuva on lyhyen käsittelyn aikaa tallennet-

tuna, mutta koska osumaa ei tule, järjestelmä ei tallenna tietoa säilö-
Poliisi ei käsitellyt ko. tapauksissa biometrista dataa, vaan vain järjestelmän antamia teknisiä tuloksia eli ns. osumia. Periytyykö erityisten henkilötietojen luokka myös näihin teknisiin tietoihin eli osumiin?

- Voiko poliisi muokata taltioimansa videomateriaalin biometrisesti haettavaan muotoon ja hakea koko materiaalista henkilön biometrisella tunnisteella (kuva, josta luotu biometrinen malli)?
- Pitääkö henkilötiedot ja erityiset henkilötiedot käsitellä tai säilyttää (fyysisesti / teknisesti) erillisissä järjestelmissä?
- Voiko (todella) suuri määrä henkilötietoja ns. kasautua, jolloin vaatimuksissa niiden eheyden, luottamuksellisuuden ja turvallisuuden takaamiseksi edellytetään lisävaatimuksia?
- Miten luokittelet henkilötiedot ja erityiset henkilötiedot?
- Koetko luokittelun tällä hetkellä oikeaksi? Pitäisikö sitä muuttaa?
- Mitkä tunnukset voidaan luokitella erityisiksi henkilötiedoiksi? Esimerkiksi natsitunnukset tai vastaavat?

3. Kameravalvontajärjestelmien suunnittelu ja käyttö

- Mistä jo tutkitut vaikutustenarvioinnit löytyvät? Voidaanko niitä hyödyntää ja millä perusteilla / minkälaisissa tilanteissa?
- Suoritettaessa biometrisilla tunnisteilla kuten kasvokuvalla vertailua, ketkä pääsevät alueelle tai eivät. Saako kameravalvontaa käyttää sellaisiin tahoihin, jotka eivät ole antaneet suostumusta kasvokuvien käsittelyyn. Käytettävä ohjelmisto ei tallenna biometrisesti tietoa vaan tekee vertailua ainoastaan henkilön luovuttamaan kuvan kanssa?
- Valvonta ei saa kohdistua suunnitelmallisesti keneenkään, mutta jos henkilö itse päätyy paikkaan, jossa sijaitsee yleisvalvontaan tarkoitettuja valvontakameroita, voidaan niitä hyödyntää yksittäisen kohteen tarkkailuun sen ajan, kun henkilö on laitteiden toiminta-alueella?
- Voidaanko yhteisrekisterinpidossa olevassa kamerajärjestelmässä säilöä yleisellä paikalla tallennettua kuvaa 6kk ajan siten, että vain poliisilla on pääsy materiaaliin vai tarvitseeko näin pitkään säilytettävä data siirtää poliisin omiin järjestelmiin?
- Miten henkilötietoja sisältävän kameravalvontakuvan säilytysajat määrittyvät esimerkiksi kaupungin ja poliisin yhteisrekisterinpidossa?
- Kuinka tehokkaasti tekoälyä hyödynnetään nykyisen lainsäädännön puitteissa?
- Minkälaisia hyötyjä tekoälyn avulla voidaan saavuttaa tulevaisuudessa?
- Pitäisikö kasvojentunnistusteknologian käyttö mahdollistaa kameravalvonnassa viranomaisille? Vrt. tapaus South Wales Police kasvojentunnistus. Kyllä / Ei? Perustele vastaus
- (Miten erittelisit?)Voidaanko kameravalvontajärjestelmän oikeudet eritellä tarpeeksi luotettavasti teknisin keinoin?

- Mainitse tärkeimmät ominaisuudet kameravalvontajärjestelmän käytössä
- Mainitse tärkeimmät suunnitteluun liittyvät asiat kameravalvontajärjestelmälle
- Ovatko sanktiot väärinkäytöstä mielestäsi oikein mitoitettu?
- Rajoittaako sanktiot teknologian kehitystä tai käyttöä?

KYSYMYKSET TSV:

1. **Kamerajärjestelmää olisi tarkoitus pystyä hyödyntämään monen toimijan puolelta, jokaisella taholla omat tarpeet ja laillisuusperuste. Miten yhteiskäyttö olisi järkevin toteuttaa?**
    - Kaupungin omat turvallisuustarpeet
        - Tapahtumaturvallisuus
        - Liikenne
        - Omaisuuden ja henkilöiden suoja
    - Poliisilla YJT ja rikokset,
    - Pelastustoimi
    - Muut tahot, kuten data-analyysi ja kaupunkikehitys

2. **Käyttäjien tarpeet vaihtelevat esim. Kaupunki ja poliisi voisi tarvita niin järjestelmän reaaliaikaista valvontaa kuin takautuvaa materiaalia. Pelastustoimella taas tarve olisi enemmän reaaliaikaisen puolella. Voidaanko asia hoitaa tietoluvilla vai onko parempi suosia yhteisrekisterinpidollista ratkaisua?**

3. **Jos järjestelmä olisi yhteysrekisterinpidossa, tulisiko jokaiselta taholta oma ns. pääkäyttäjä/valvoja joka vastaisi oma sektorinsa seurannasta yms.?**

4. **Ylläpitäjien rooleja on vaikea rajata toisistaan, mikä luo riskin, että toisella taholla olisi tekninen pääsy katsoa toisen tahon tietoja luvattomasti. Voiko tällainen seikka olla henkilötietojen näkökulmasta yhteistyön poissulkeva asia.**
    - Esim. yksityinen taho tarkastelisi poliisin puolen järjestelmän käyttöä

5. **EDBP 3/2019 ohjeistuksessa. Kerättävien henkilötietojen määrää ja säilyttämistä pitäisi minimoida. Ohjeessa mainittiin myös ns. black box periaatteessa missä säilöttävä materiaali voidaan säilöä pidempään ja jos käyttöperuste tulee, voidaan materiaali avata.**
    - Tiedon säilytyksen tarpeet ja ohjeistukset
        - EDPB 3/2019 määre 72h, Poliisin henkilötietolaki 6kk
        - Voidaanko säilyttää samassa tietokannassa ja jakaa käyttöoikeuksin rajaten?

6. **Kaupunkikamerajärjestelmässä olisi tarkoitus käyttää tekoälyä, jonka avulla videomateriaalia saataisiin paremmin haettavaksi. Tällöin henkilötietoja käsiteltäisiin uuden teknologian avulla ja vaatisi vaikutustenarvioinnin. Onko jostain saatavissa jo TSV:n käsittelemiä arviointeja, joita voisi hyödyntää?**

7. **Tekoälyn suhteen kameroilla ei olisi tarkoitus kerätä/käsitellä erityisiä henkilötietoja. Hahmontunnistuksessa käytettävät ohjelmistot eivät pääsääntöisesti luokittele datasta saatavia objekteja henkilön yksilöllisten tai biometristen tietojen kautta.**

    - Milloin kameravalvontamateriaaliasta muodostuu erityinen henkilötietoluokka?
    - Ohjelmistoissa voidaan hakea myös kuvalla, joka esimerkiksi otetaan videoleikkeeltä suoraan ja haetaan samankaltaisia tai samaa henkilöä järjestelmän muusta aineistoista

8. **Kaupunkikamerajärjestelmät kuvaavat kaupungissa yleisiä paikkoja. Kamerat ovat sijoitettu ylös, jotta suoranaisesti niistä henkilöitä ei ole tunnistettavissa. Kameroilla on kuitenkin mahdollista tarkentaa kuvaa siten, että henkilö on niistä täysin tunnistettavissa. Lisäksi kameroiden kuvamateriaalia voidaan hyödyntää muiden tietojen kanssa, jolloin henkilö on tunnistettavissa. Tällöin voidaan olettaa kameramateriaalia olevan GDPR:n artikla 4 mukaisesti henkilötietoja. Kamerat kuvaavat mielenilmauksia tai muita poliittisia tapahtumia, joita järjestetään kaupungeissa. Materiaalista on selvitettävissä esimerkiksi henkilön poliittinen mielipide ja henkilö voidaan materiaalia kautta yksilöidä. Onko kyseessä tällöin erityinen henkilötietoryhmä ja voidaanko tällaista materiaalia tallentaa? Voidaanko tällaista materiaalia hyödyntää ja millä perustein?**
    - Miten tällaisen henkilön hakeminen järjestelmästä esim. vaatetuksen perusteella (similarity)? Henkilö esimerkiksi syyllistynyt rikokseen.

9. **Kun tekoälyohjelmisto tuottaa ja siinä käsitellään ainoastaan henkilötietoja eli videota ja siitä luotuja haettavia malleja (objekti, vaatetus, yms.) Voiko näitä käsitellä myös muut järjestelmän käyttöoikeutetut tahot, kuten tapahtumaan palkattu vartija, poliisi tai pelastustahon henkilö? Oletetaan, että käyttäjällä on kyseistä tehtäväänsä varten tarve hyödyntää näitä tietoja ja laillinen käyttöperuste käsitellä kameravalvontajärjestelmää.**

10. **Valvonta ei saa kohdistua suunnitelmallisesti keneenkään, mutta jos henkilö itse päätyy paikkaan, jossa sijaitsee yleisvalvontaan**

tarkoitettuja valvontakameroita, voidaanko niitä hyödyntää yksittäisen kohteen tarkkailuun sen ajan, kun henkilö on laitteiden toiminta-alueella?

11. **Tekoälyohjelmistojen toiminta pohjautuu siihen, että halutuista asioista/objekteista/tiedoista luodaan yksilöiviä laskennallisia malleja. Näitä malleja voidaan hakea ja vertailla tehokkaasti. Toimintaa voidaan suorittaa reaaliajassa suoraan kameran kuvavirrasta. Yleisesti erilaisia vertailutietoja syötetään ns. etsintälistalle/"triggerluotteloon" ja kun ohjelma havaitsee kuvavirrasta tällaisen, tulee siitä tieto käyttäjälle. Onko kuvanvirran jatkuva työstäminen GDPR:n mukaista henkilötietojen käsittelyä, vaikka tapahtumasta ei tallentuisi mitään?**
    - Esimerkiksi kameroista, joista ei saada tunnistettavaa kuvaa ja eivät varsinaisesti muodosta henkilötietorekisteri (liikennevirta)
    - Esimerkiksi kasvojentunnistus, jossa seulotaan vain listalle syötettyjä henkilöitä (lipun ostanut tai viranomaisen toimesta)

12. **Tekoälyn tuottama laskennallinen malli on henkilötietoja. Yleisesti ohjelma toimii omalla erillisellä palvelimella, jonne tietoa kerätään. Lisäksi kameravalvontajärjestelmä taltioi videon raakamateriaalin. GDPR:ssä tietojen sirpaloituminen on yksi riski. Toisaalta haettavuus tehostaa rekisteröidyn tietojen löytymistä suuremmastakin datamassasta. Onko tiedon sirpaloitumisesta jotain tarkempaa ohjeistuista? EDPB:n 3/2019 mainitaan, että ainakin erityisiä henkilötietoja tulisi säilyttää eri tietokannoissa.**

13. **Kameravalvontadatan analysointi anonymisoituna. Mikäli dataa kuten ihmislaskennasta syntyvää tilastoa siirretään suoraan järjestelmässä eriytettyyn tietokantaan tai käyttäjän käyttöoikeus rajataan vain tilastolliseen dataan (ei itsessään enää henkilötietoja), tarvitseeko henkilöllä olla kuitenkin laillinen käyttöperuste henkilötietojen käsittelylle? Periytyykö henkilötietojen vaatimukset tällaisessa tilanteessa?**
    - Tekoälyohjelmistoilla dataa voi työstää usealla eri tavalla, kuten etsiä miehiä ja naisia sekä luoda näistä toimintaa tehostavia raportteja. Voiko käyttäjä pyytää ohjelmaa noutamaan hänelle nämä anonymisoidut tiedot suoraan henkilötietoja sisältävästä kannasta? Olettaen ettei henkilö pääse näkemään henkilötietoja.

14. **Missä vaiheessa kameravalvonnassa käytettävän tekoälyohjelmiston hankintaa ja käyttöä tulisi aloittaa yhteistyö tietosuojavaltuutetun kanssa? Toimintaa kun ei saa edes testata, saati aloittaa ennen kuin sen on TSV:n puolelta arvioitu. Miten prosessi toimii?**

15. **Mitä näet suurimpana haasteena kameravalvonnassa käytettävän tekoälyn puolella tulevaisuudessa?**