



Hätäkeskustietojärjestelmän tietojen luokittelun kehittäminen

Mika Taavitsainen

2022 Laurea



Laurea-ammattikorkeakoulu

Hätäkeskustietojärjestelmän tietojen luokittelun kehittäminen

Mika Taavitsainen
Tradenomi, turvallisuusala
Opinnäytetyö
Toukokuu, 2022

Mika Taavitsainen

Hätäkeskustietojärjestelmän tietojen luokittelun kehittäminen

Vuosi

2022

Sivumäärä

49

Tämän opinnäytetyön tavoitteena oli tuottaa malli, jolla hätäkeskustietojärjestelmän tietoaineistot voidaan tyypitellä ja sen pohjalta luokitella. Opinnäytetyön tavoitteena oli perehtyä siihen, mitä tietojen luokittelu on ja kuinka tietoaineistot voidaan luokitella. Opinnäytetyön tarkoitus oli tuottaa Hätäkeskuslaitokselle luokittelumalli, jolla voi toteuttaa vuosittain hätäkeskustietojärjestelmän tietojen luokittelun arviointi. Opinnäytetyö toteutettiin Hätäkeskuslaitoksen toimeksi antamana.

Tässä opinnäytetyössä teoreettisen viitekehyksen luovat ensisijaisesti lainsäädäntö, valtionhallinnon ohjeistukset sekä standardit. Opinnäytetyön tietoperustaa varten perehdyttiin lisäksi muihin luotettaviin julkaisuihin, kuten aihetta käsittelevään kirjallisuuteen, opinnäytetöihin, tieteellisiin julkaisuihin sekä Hätäkeskuslaitoksen ohjeistukseen.

Opinnäytetyössä käytettiin menetelmällisinä ratkaisuinä kirjallisuuskatsausta, havainnointia sekä haastatteluja. Opinnäytetyön aineisto kerättiin menetelmällisten ratkaisujen kautta. Kirjallisuuskatsauksella hankittiin syvälinen tietoperusta tiedon luokitteluun ja valittiin toteutettava malli. Havainnoinnilla selvitettiin Hätäkeskustietojärjestelmän tietotyypit ja laadittiin menetelmäomake. Haastatteluilla toteutettiin hätäkeskustietojärjestelmän tietotyyppien luokittelu.

Opinnäytetyön keskeisenä tuloksena on saatu aikaan hätäkeskustietojärjestelmän tietojen luokittelumalli. Tiedon luokittelua voidaan raportoida vuosittain Hätäkeskuslaitoksessa. Raportilla voidaan todentaa rekisterinpitäjän osoitusvelvollisuutta hätäkeskustietojärjestelmän osalta. Opinnäytetyön keskeisenä kehitysehdotuksena tulee selvittää tietoaineiston keskinäisen riippuvuuden käyttäytyminen hätäkeskustietojärjestelmässä. Tällä on vaikutusta hätäkeskustietojärjestelmän tietojen luokitteluun luottamuksellisuuden, saatavuuden ja eheyden näkökulmasta.

Asiasanat: eheys, luottamuksellisuus, saatavuus, tiedon luokittelu

Mika Taavitsainen

Developing an Information Classification Method with the ERC system

Year

2022

Pages

49

The objective of this thesis is to produce a model where the datasets of the emergency center information system can be typed and classified. The purpose is to examine what is the basis for data classification, and how the data then can be classified. The purpose of this thesis is to produce a classification model for the Emergency Response Centre Agency. The model may be used annually to carry out an assessment of the classification of data in the ERC system. The thesis is commissioner by the Emergency Response Centre Administration.

In this thesis, the theoretical framework primarily review legislation, government guidelines and standards. Other reliable publications, such as literature, other theses, scientific publications, and instructions from the Finnish ERC Agency, are also studied for the theoretical framework of the thesis.

This thesis uses literature reviews, observations, and interviews as its methodological solutions. The literature review provided an in-depth framework for the classification of information and selected the model to be implemented. The observation was used to determine the data types of the Emergency Response Centre Information System and to draw up a method form. The interviews carried out revealed the data classification types of the emergency response center information system.

The ERC system's data classification model is the key outcome of the thesis. The ERC system's data classification report can be carried out annually at the Emergency Response Centre. The report can be used as an obligation to prove the ERC's data system. The key development proposal of the thesis is to investigate how the ERS system's data behaves internally and is dependent on the other data sets. All this has an impact on the classification of data in the system. This will have an effect of the confidentiality, availability and integration of the data and its usage.

Keywords: availability, Classification of information, confidentiality, integrity

Sisällys

1	Johdanto.....	6
2	Opinnäytetyön tavoite.....	7
2.1	Opinnäytetyön tavoite ja saavutettu hyöty	7
2.2	Opinnäytetyön rajaukset	9
3	Teoreettinen viitekehys ja keskeiset käsitteet	9
3.1	Lainsäädäntö.....	10
3.2	Aiemmat tutkimukset ja tieteelliset julkaisut	11
3.3	Katsaus tietojen luokitteluun	15
3.4	Keskeiset käsitteet.....	19
4	Opinnäytetyön prosessi	21
4.1	Kehittämistyön kulku ja muoto	21
4.2	Kirjallisuuskatsaus	24
4.3	Havainnointi	25
4.4	Teemahaastattelu.....	26
4.5	Aineiston analysointi.....	27
5	Tulokset	28
5.1	Tiedon menetelmälomake ja tietotyyppien luokittelun aputaulukko	29
5.2	Luottamuksellisuuden arviointi	31
5.3	Saatavuuden arviointi	32
5.4	Eheyden arviointi.....	32
5.5	Kasautuvuuden arviointi.....	33
5.6	Henkilötiedon arviointi	34
6	Pohdinta	35
6.1	Opinnäytetyön luotettavuus ja eettisyys	35
6.2	Keskeisten tulosten tarkastelu	36
6.3	Johtopäätökset ja kehitysehdotukset	37
	Lähteet.....	40
	Kuviot	43
	Taulukot	43
	Liitteet	44

1 Johdanto

Laki hätäkeskustoiminnasta (692/2010) 2 luvun 4 § 1-2 määrittää, että Hätäkeskuslaitoksen ydintehtävä on hätäkeskuspalvelujen tuottaminen sekä niihin liittyvä pelastustoimen, poliisitoimen, sekä sosiaali- ja terveystoimen viranomaisten toiminnan tukeminen. Ydintehtävä toteutetaan pysyvällä, automaattiseen tietojenkäsittelyyn tarkoitettulla hätäkeskustietojärjestelmällä, joka on rakennettu tätä toimintaa varten. Hätäkeskustietojärjestelmä on henkilörekisteri, johon on hätäkeskuspalvelujen tuottamista varten tallennettu tietoja lain hätäkeskustoiminnasta (692/2010) 4 luvun 17 §:n mukaisesti. Hätäkeskuslaitos otti käyttöön uuden hätäkeskustietojärjestelmän vuonna 2019 (Hätäkeskuslaitos 2022b).

Hätäkeskustietojärjestelmässä käsitellään turvallisuusluokiteltua aineistoa sekä henkilötietoja. Tietojärjestelmästä on laadittu rekisteriä ja tietosuojaa koskeva rekisterinpitäjän seloste käsittelytoimista eli tietosuojaseloste. Tietosuojaselosteessa on ilmoitettu Hätäkeskuslaitoksen tietosuojavastaava sekä hätäkeskustietojärjestelmän yhteyshenkilö rekisterinpitöä koskevissa asioissa. Käytännössä rekisterinpitäjänä toimii virasto. Selosteeseen on kirjattu mm. rekisterin tietosisältö, säännönmukaiset tietolähteet sekä tekniset ja organisatoriset turvatoimet. (Hätäkeskuslaitos 2022a.)

Euroopan parlamentin ja neuvoston asetus (2016/679) tunnetaan EU:n yleisenä tietosuojasetuksena. Tietosuojasetus velvoittaa erilaisia asioita henkilötietojen käsittelyyn liittyen. Tietosuojasetuksen artikla 5 mukaan rekisterinpitäjän tulee kyetä osoittamaan, että henkilötietoja käsitellään tietosuojalainsäädännön mukaisesti. Rekisterinpitäjän tulee artikla 24 mukaan erilaisilla tavoilla osoittaa, että tietosuojavaatimuksista on asianmukaisesti huolehdittu. Osoitusvelvollisuudella kuvataan, että tietosuojavaatimukset ovat toteutuneet ja että ne on huomioitu. Nämä voidaan käytännössä osoittaa dokumentein, sekä sillä, että tietosuojavaatimukset ovat osa viraston prosesseja ja käytäntöjä (2016/679/EU, artikla 25).

Viranomaisten tulee lainsäädäntöön pohjautuen huolehtia tarpeellisista tietoturvallisuustoimenpiteistä. Tietoaineistojen saatavuus, eheys ja luottamuksellisuus tulee kyetä varmistamaan hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Tietoaineistojen turvallisuus tulee varmistaa ja viranomaisen tulee huolehtia siitä, että tieto on käyttökelpoista, ajantasaista ja virheetöntä. Lain julkisen hallinnon tiedonhallinnasta (906/2019) 4 luvun 15 §:n mukaan tarpeeton tieto ”voidaan tarvittavilta osin arkistoida”.

Hätäkeskustietojärjestelmällä työskentely edellyttää, että järjestelmään on tallennettu toimintaa varten tarpeellinen tietosisältö. Tietosisältö on syötetty järjestelmään Hätäkeskuslaitoksen, ensihoidon, pelastustoimen, poliisin ja Rajavartiolaitoksen tiedoista vastaavien toimijoiden organisoimana. Tiedon omistajana toimii tiedon syöttänyt viranomainen.

Tietoaineiston syöttämisen yhteydessä tieto luokitellaan tiedon omistajan päätöksen mukaisesti. (Laki hätäkeskustoiminnasta 692/2010, 18 §.)

Hätäkeskustietojärjestelmän tietojen luokittelun kehittämisen tuloksilla on vaikutus kaikkien hätäkeskustietojärjestelmää ylläpitävien viranomaisten tiedon ylläpitoon ja ylläpidon ohjaamiseen. Viranomaiset saavat opinnäytetyön tuloksena selkeän suunnitelman tiedon luokittelusta sekä suunnitelman tietotyyppien tarkastusta varten. Opinnäytetyö toteutetaan yhteistyössä poliisin, pelastustoimen, ensihoidon, sosiaalitoimen sekä Rajavartiolaitoksen tietojärjestelmän pääkäyttööä toteuttavien tahojen kanssa.

2 Opinnäytetyön tavoite

Tässä opinnäytetyössä hätäkeskustietojärjestelmän tietosisällölle laaditaan tiedon luokittelumalli. Luokittelumallin laadinta toteutetaan havainnoinnin pohjalta. Havainnoinnilla tietosisältö jaotellaan loogisiin kokonaisuuksiin tietotyypeiksi, joille määritetään tietoluokan tärkeys viranomaisten kanssa teemahaastattelun lopputuloksena. Opinnäytetyön lopputuloksena voidaan loogisia kokonaisuuksia verrata ja priorisoida suhteessa toisiinsa. Tämän pohjalta voidaan toteuttaa tiedon luokittelu tiedon luottamuksellisuuden, eheyden, saatavuuden ja mahdollisten muiden arvioitavien asioiden näkökulmasta. Näiden lisäksi luokittelussa on tärkeitä ottaa huomioon, sisältääkö tietoluokka henkilötietoa. Tietoluokkien tarkastukset voidaan suunnitella ja dokumentoida. Tiedon luokittelua voidaan hyödyntää vuosittaisessa tietosuojan raportoinnissa tietosuoja-asetuksen (2016/679/EU) 5 artiklan mukaisesti rekisterinpitäjän osoitusvelvollisuuden toteuttamiseksi.

2.1 Opinnäytetyön tavoite ja saavutettu hyöty

Opinnäytetyön tilaaja ja omistaja on Hätäkeskuslaitos ja opinnäytetyö tuotetaan Hätäkeskuslaitoksen kehittämisosaston pääkäyttöyksikölle ja hätäkeskustietojärjestelmän rekisterinpitäjälle. Opinnäytetyö toteutetaan hätäkeskustietojärjestelmän tiedonhallinnan ja tietojen ylläpidon kehittämiseksi. Opinnäytetyöllä kehitetään järjestelmällinen prosessi, jolla Hätäkeskuslaitos voi rekisterinpitäjänä ohjata ja valvoa hätäkeskustietojärjestelmän tiedon luokittelua. Tiedon luokittelun tarkastaminen toteutetaan vuosittain. Tarkastus dokumentoidaan ja sen pohjalta laaditaan raportti, jolla tuetaan hätäkeskustietojärjestelmän rekisterinpitäjän osoitusvelvollisuutta. (Hätäkeskuslaitos 2021.)

Hätäkeskustietojärjestelmän rekisterinpitäjänä toimii Hätäkeskuslaitos (Hätäkeskuslaitos 2022a). Hätäkeskuslaitoksen johto vastaa viraston tietosuojan kokonaishallinnasta. Tietosuojan kokonaishallintaa varten johto tarvitsee kokonaiskuvan tietosuojaa koskevista asioista virastossa. Kokonaiskuvan tuottamisesta vastaavat viraston virkamiehet työjärjestyksen mukaisesti. Rekisterinpidosta, tietosuojasta, tietojen ylläpidosta, ohjeistuksesta, koulutuksesta

sekä käyttöoikeuksien ylläpidosta vastaavat henkilöt tuottavat kokonaiskuvan raportein. Raportointi on säännöllistä ja jatkuvaa sekä tietosuoja-asetuksen (2016/679/EU) 5 artiklaan pohjautuvaa.

Hätäkeskuslaitos (2020) on todennut, että hätäkeskustietojärjestelmä aiheuttaa henkilötietojen käsittelyyn korkean riskin rekisteröityjen kannalta. Tästä johtuen hätäkeskustietojärjestelmään on tehty tietosuoja-asetuksen (2016/679/EU) artiklan 35 mukainen tietosuojan vaikutuksenarviointi DPIA (*data protection impact assessment*). Tietosuojan vaikutuksenarvioinnin toteuttaja on laatinut vaikutuksenarvioinnista kirjallisen raportin (Hätäkeskuslaitos 2020). Raportin pohjalta Hätäkeskuslaitos (2020) on tehnyt korjaustoimenpiteitä raportissa kuvattujen puutteiden korjaamiseksi.

Riskejä pienennetään tai poistetaan prosesseja ja raportointia kehittämällä sekä korjaamalla havaittuja puutteita (2016/679/EU, artikla 24). Korjaavia toimenpiteitä analysoidessa on todettu, että riskien pienentämiseen tai poistamiseen voidaan vaikuttaa ennalta (Hätäkeskuslaitos 2020). Tämän opinnäytetyön toteutusta ohjaavat hätäkeskustietojärjestelmän vaikutuksenarvioinnissa esille nousseet havainnot tietoaaineistoon ja sen tietoturvaan liittyen. Tietojen luokittelun prosessia tai tietojen tarkastuksen prosessia ei ole vielä kuvattu tai toteutettu (Hätäkeskuslaitos 2020).

Hätäkeskustietojärjestelmä sisältää merkittävän määrän toimintaa varten ylläpidettävää hallinnollista tietosisältöä. Hallinnollisen tietosisällön avulla järjestelmän tietomalli koostaa tieto-olioita erilaisiksi toiminnallisiksi kokonaisuuksiksi. Näitä tietokokonaisuuksia käytetään hyödyksi automaattisen tietojenkäsittelyn eri käytännön toimintojen toteuttamiseksi. Jotta järjestelmä voi toimia oikein, tulee sen tietosisältö olla saatavissa käyttöön. Tietosisällön tulee lisäksi olla toiminnallisesti eheää ja tiedon luottamuksellisuuden on oltava kunnossa.

Opinnäytetyössä laaditaan tutkimuksellisenä kehittämistyönä käytänteet hätäkeskustietojärjestelmän sisältämien tietojen luokittelulle. Opinnäytetyön tuloksena saavutetaan tapa, jolla Hätäkeskuslaitos voi vuosittain arvioida ja raportoida tietojen luokittelun hätäkeskustietojärjestelmän osalta osoitusvelvollisuuden täyttymiseksi. Opinnäytetyössä selvitetään; ”*Kuinka hätäkeskustietojärjestelmän hallinnollinen tietosisältö kootaan kokonaisuuksiksi eli tyypitetään ja miten ne niiden pohjalta luokitellaan?*” Tietoaaineiston tyypittely toteutetaan siten, että tietoa ei yksilöidä salassa pidettävyyden tai turvaluokittelun näkökulmasta ja siten, että tietotyyppiä voidaan käsitellä julkisena tietona.

Ratkaisu testataan neljässä haastattelutilaisuudessa eri haastateltavien ryhmien kanssa. Tiedon luokittelua varten laaditaan kolmiportainen luokittelumittari tietotyypin tärkeyden osoittamiseksi. Kolmiportaisuuden lisäksi arvioidaan, sisältääkö tietotyyppi henkilötietoa tai kasautuuko tieto. Myös tietotyypit, joita viranomaisen ei käytä, merkitään tätä edustavalla merkinnällä. Haastattelutilaisuudessa tietotyypeille määritetään tiedon tärkeys eli luokittelu.

Tulosten arvioinnin jälkeen laaditaan johtopäätökset ja tehdään esitys tiedon luokittelulle hätäkeskustietojärjestelmässä.

2.2 Opinnäytetyön rajaukset

Opinnäytetyö rajataan koskemaan järjestelmän hallinnollista tietoaaineistoa eli dataa. Hallinnollinen data on tietoaaineistoa, jota laaditaan ja ylläpidetään järjestelmässä, jonka avulla hätäkeskustietojärjestelmän operatiivinen käyttöliittymä voi toimia oikein. Yksilöivää tietoaaineistoa tai henkilötietoja ei tässä opinnäytetyössä käsitellä. Tietoluokkien käsittelyn osalta tämän opinnäytetyön ulkopuolelle rajataan tiedon käsittelytapaan, käsittelypaikkaan, tallentamiseen, arkistointiin ja tulostamiseen liittyvät asiakokonaisuudet. Tässä opinnäytetyössä tiedon salassa pidettävyyteen ja turvaluokitukseen liittyvät kokonaisuudet rajataan opinnäytetyön ulkopuolelle pelkistämällä arviointi tiedon tärkeydeksi. Salassa pidettävään tietoon ja turvaluokitteluun viitataan tiedon luokittelun aputaulukossa esimerkinomaisesti.

Hätäkeskustietojärjestelmän päävastuullinen rekisterinpitäjä on Hätäkeskuslaitos, mutta poliisin tietojen osalta rekisterinpitäjänä toimii poliisihallitus. Hätäkeskustietojärjestelmän tietoluokat, jotka kuuluvat suoraan poliisin rekisterinpidon alaisiin tietoihin, rajataan tämän opinnäytetyön ulkopuolelle. Poliisin rekisterinpidon alaiset tietoluokat ovat liitettävissä viralliseen, rekisterinpitäjälle toimitettavaan tietojen luokittelun raporttiin sen kirjausajankohdaksi.

Hätäkeskustietojärjestelmän käyttöoikeudet niin toiminnallisilta kuin hallinnollisilta osin rajataan tämän opinnäytetyön ulkopuolelle. Opinnäytetyössä ei käsitellä sitä, millaisin käyttöoikeuksin tai missä roolissa mitään tietotyyppiä voidaan käsitellä. Hätäkeskustietojärjestelmää varten laaditut käyttöoikeustasot ja niiden myöntäminen on määritetty hätäkeskustietojärjestelmän käyttöehdoissa ja käyttöoikeuspolitiikassa (Hätäkeskuslaitos 2018a; 2018b).

3 Teoreettinen viitekehys ja keskeiset käsitteet

Tämän opinnäytetyön lähestymiskulmana on saavuttaa toimintaprosessin kehittämisen kautta parantunut tietoturva. Parantunut tietoturva tiedon eheyden ja luottamuksellisuuden kautta säännöllisenä prosessina tukee rekisterinpitäjän osoitusvelvollisuutta tietosuojasäilytyksessä. Tässä opinnäytetyössä teoreettisen viitekehysten luovat ensisijaisesti lainsäädäntö, valtiohallinnon ohjeistukset sekä standardit. Opinnäytetyön tietoperustaa varten perehdytään lisäksi muihin luotettaviin julkaisuihin, kuten aihetta käsittelevään kirjallisuuteen, opinnäytetöihin, tieteellisiin julkaisuihin sekä Hätäkeskuslaitoksen ohjeistukseen.

Tietosuojaa yrityksissä, kunnissa tai valtionhallinnossa on käsitelty erilaisista näkökulmista monessa opinnäytetyössä ja tutkimuksessa. Myös tietoturvaa käsitteleviä töitä on olemassa

hyvin paljon. Töissä, joihin olen perehtynyt, on lähestymiskulma ollut oikeusopillinen, henkilön työtehtävien lähestymiskulma tai yrityksen, kunnan tai viraston selviäminen määritetystä tietosuojan tai tietoturvan osakokonaisuudesta. Tietojen luokittelua osana tietoturvaa käsitteleviä tutkimuksia on löytynyt muutama. Näistä töistä on muutama valittu osaksi tietoperustaa.

3.1 Lainsäädäntö

EU:n yleinen tietosuoja-asetus GDPR, myöhemmin tietosuoja-asetus, eli *General Data Protection Regulation* (2016/679/EU) määrittää tietosuoja-asioiden sääntelyn Euroopassa. Tietosuoja-asetuksen (2016/679/EU) 5 artiklan keskeisimpiä periaatteita on rekisterinpitäjän osoitusvelvollisuus. Sen perusteella rekisterinpitäjän on kyettävä osoittamaan, että henkilötietoja käsitellään tietosuojalainsäädäntöjen mukaisesti (2016/679/EU, 5 artikla).

EU:n tietosuoja-asetus (2016/679/EU) vaatii sen artiklojen 5, 24 ja 25 mukaan, että rekisterinpitäjä aktiivisin ja monin toimenpitein osoittaa, että organisaatiota koskevat tietosuoja-vaatimukset on huomioitu. Vaatimukset tulee tietosuoja-asetuksen (2016/679/EU) 25 artiklan mukaan viedä organisaation henkilötiedon käsittelyprosesseihin ja käsittelykäytäntöihin. Tietosuoja-asetuksen (2016/679/EU) 5 artiklan mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan, että tieto on asianmukaisesti suojattu eheyden ja luottamuksellisuuden näkökulmasta hyödyntäen organisatorisia ja teknisiä toimia.

Tietosuojalaki (1050/2018) täydentää EU:n tietosuoja-asetusta. Lailla annetaan täsmennyksiä ja sitä sovelletaan rinnakkain tietosuoja-asetuksen kanssa. Tietosuojalain (1050/2018) 2 luvun 4 § määrittää henkilötietojen käsittelyn lainmukaisuudesta siten, että käsittelyn tulee olla ”tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi”. Tietosuojalain (1050/2018) 3 luvun 8 §:ssä säädetään, että toimivaltaisena valvontaviranomaisena tietosuoja-asioissa toimii Suomessa tietosuojavaltuutettu. Lain 2 luvun 6 § määrittää, että tietosuojavastaava tulee nimittää silloin kun henkilötietoa käsitellään toisen lain pohjalta (Tietosuojalaki 1050/2018).

Lain julkisen hallinnon tiedonhallinnasta eli tiedonhallintalain (906/2019) tarkoituksena on sen 1 luvun 1 § perusteella varmistaa, että viranomaisten tietoaineistoja hallitaan yhdenmukaisesti ja laadukkaasti sekä taata niiden tietoturvallinen käsittely. Edelleen tiedonhallintalaki (906/2019) 1 luvun 1 § määrittää, että lain tarkoituksena on ”edistää tietojärjestelmien ja tietovarantojen yhteentoimivuutta”.

Tiedonhallintalain (906/2019) 4 luvun 15 § määrittää, että tietoaineistojen tulee olla ajantasaisia, niiden virheettömyys tulee olla varmistettu ja tietoaineiston on oltava käyttökelpoista. Tietoturvallisuustoimenpiteillä tarkoitetaan tiedonhallintalain (906/2019) 1 luvun 2 §:n

määritelmän mukaisesti ”tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimilla”.

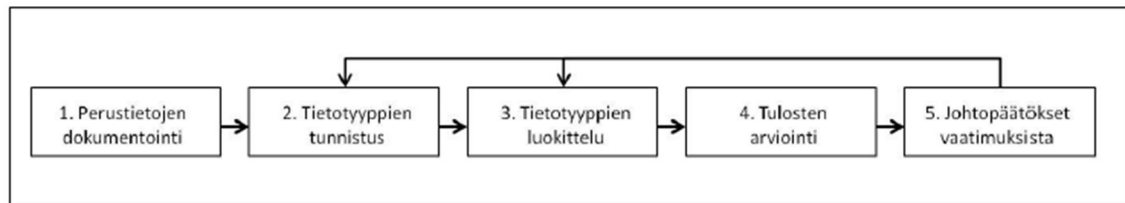
Tiedonhallintalain (906/2019) 4 luvun 13 §:n 3 momentti säätää, että ”viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa”. Käytännössä säädös ohjaa tämän opinnäytetyön toteuttamista siten, että tässä opinnäytetyössä tunnistetaan tietovarantojen tietorakenteet sekä määritetään näille tiedon tärkeys. Tiedon tärkeyden yhteydessä arvioidaan myös tiedon luottamuksellisuutta siitä näkökulmasta, onko tiedolle tarpeen merkittä turvallisuusluokkaa koskeva merkintä (Tiedonhallintalaki 906/2019, 18 §; Valtiovarainministeriö 2021, 10-11).

Laki hätäkeskustoiminnasta (692/2010) määrittelee 4 luvun 17 §:ssä hätäkeskustietojärjestelmään talletettavan tietosisällön. Järjestelmään voidaan tallentaa lain 2 luvun 4 §:ssä säädettyjen tehtävien kannalta tehtävän hoitoon liittyviä, tarpeellisia tietoja. Lain 4 luvun 17 §:n 2 momentti määrittelee myös, kuka on oikeutettu näkemään hätäkeskustietojärjestelmään tallennettua tietoa, millä perusteella tämä oikeus syntyy sekä sen, milloin tieto tulee poistaa.

3.2 Aiemmat tutkimukset ja tieteelliset julkaisut

Tässä opinnäytetyössä hyödynnetään aikaisempia tutkimuksia sekä tieteellisiä julkaisuja tiedon luokittelun ympäriltä. Simi (2017) on tutkinut Jyväskylän yliopiston tietojenkäsittelytieteen pro gradu -tutkielmassaan tiedon luokittelua osana organisaation kokonaisarkkitehtuurin riskinarvioprosessia. Tutkimuksen lopputuloksena on kehitetty malli arvioida tiedon luokittelua tietoturvallisuuden näkökulmasta (Simi 2017). Mallia tullaan hyödyntämään pohjana tälle opinnäytetyölle. Simin (2017) tutkimuksen luokittelumatriisi sekä tietotyypin luokittelun aputableluko toimivat tämän opinnäytetyön esimerkkipohjina. Luokittelumatriisista muokataan hätäkeskustietojärjestelmää koskevat menetelmäomake sekä tietotyypin luokittelun aputableluko. Simin (2017) tutkimus ei suoraan vastaa tämän opinnäytetyön tutkimuskysymyseen, vaan sitä sovelletaan uudelle käyttötavalle.

Simi tutki kokonaisarkkitehtuuriprojektien tai tietojärjestelmäprojektien tietoturvallisuusvaatimusten luokittelua. Tutkielmassa Simi laati ryhmähaastatteluja varten luokitteluun pohjautuvan menetelmäomakkeen. Menetelmäomake sisälsi luokittelumatriisin. Lisäksi Simi laati tietotyypin luokittelun aputablelkon selventämään luokittelumatriisin esimerkkejä. Luokittelussa arvioitiin tietotyypin luottamuksellisuutta, saatavuutta ja eheyttä. Tietoluokat jaoteltiin korkeaan, normaaliin ja matalaan sekä kansainvälisten tietoturva-vaatimusten luokkiin. Tuloksina todettiin, että yksinkertaistettu luokittelumalli toimii erityisesti määrittelyssä ja toteutuksessa olevissa tietojärjestelmäprojekteissa. Tutkielmassaan Simi käytti menetelmää, joka on pelkistetty alla olevaan kuvaan. (Simi 2017.)



Kuvio 1: Tietojen luokittelun menetelmä (Simi 2017).

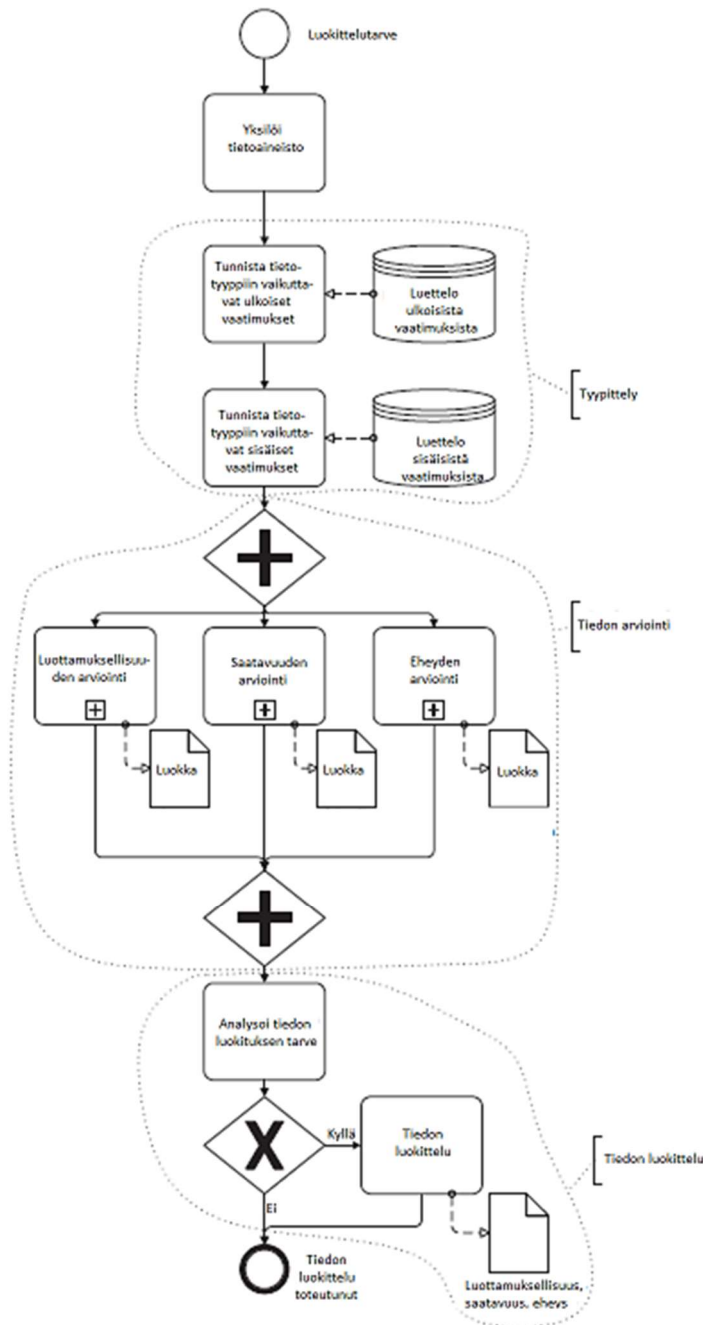
Tutkielman johtopäätöksissä Simi (2017) toteaa menetelmän soveltuvan hyvin käyttötarkoitukseensa. Kokonaisarkkitehtuurin tietotyypit onnistuttiin menetelmällä tunnistamaan sekä toisaalta tietotyypit pystyttiin luokittelemaan järkevästi. Tietotyyppien luokittelu toteutettiin siten, että luokka ei sisältänyt eksaktia päätelmää siitä, mihin tiedon suojaustasoon kyseinen luokka luottamuksellisuuden, saatavuuden tai eheyden osalta kuului. Luokittelu johti luokiteltavan projektin näkökulmasta siihen, että pystyttiin tuottamaan informaatiota järjestelmän suunnittelun ja johtamisen välille. Tietotyyppien luokittelulla pystyttiin osoittamaan tietotyypit, jotka tarvitsivat erityistä huomiota tietoturvasuoritusvaatimusten osalta. Tällöin kyettiin tunnistamaan, onko järjestelmäsuunnittelussa aukkoja tietoturvasuorituksen osalta. Tämä mahdollisti projekteihin johtamistoimenpiteitä, joilla tietoturva-asteet ovat mahdollista projektissa arvioida tai korjata.

Teemu Nykänen (2016) on tutkinut tiedon luokittelua suojaustarpeiden määrittämiseksi organisaatiossa Laurea-ammattikorkeakoulun ylemmän ammattikorkeakoulun opinnäytetyössään. Nykänen on tutkinut tiedon luokittelun pohjalta luotua prosessimallia ja taulukkomallia. Nykänen on tutkimuksessaan (2016, 34) todennut prosessimallin erittäin raskaaksi ja toisaalta sen tueksi kehitetyn taulukkomallin käyttökelpoiseksi valtionhallinnossa. Tämä opinnäytetyö hyödyntää osaltaan Nykäsen (2016) tutkimaa tietoa tiedon luokittelusta ja yhdistää havainnot Simin (2017) mallista saadun tiedon kanssa. Nykäsen (2016) tuottama taulukkomalli ei sovellu suoraan tämän opinnäytetyön malliksi. Arvion pohjalta tiedon kokoamisen malli on muokattavissa tätä opinnäytetyötä palvelevaksi Simin (2017) tutkimuksen pohjalta.

Bergström, Karlsson & Åhlfeldt (2021) ovat julkaisussa *Developing an information classification method* esitelleet kaksi erilaista mallia tiedon luokittelulle. Tiedon luokittelun mallien erot toisiinsa nähden ovat siinä, että toinen malli pyrkii pelkistämään asiat mahdollisimman laveisiin kokonaisuuksiin, joiden luottamuksellisuutta, eheyttä ja saatavuutta arvioidaan. Mallilla "aineistojen tiedon luokittelun prosessi" (*route for classifying high granularity assets*) pyritään löytämään tietokokonaisuuksia, joiden tietoturvasuoritusvaatimusten, eheyden ja saatavuuden näkökulmasta (Bergström ym. 2021, 229).

Toinen Bergström ym. (2021, 224) julkaisussa esitelty malli koskee vastaavaa, mutta "matalan, dataa koskevan mallin" (*the low granularity route*) arviointia. Tässä mallissa kaikkea dataa arvioidaan luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta. Malli on tältä

osin hidas. Erilaiset mallit soveltuvat toisistaan erityyppisille järjestelmille. Tämän opinnäytetyön näkökulmasta Bergström ym. (2021) mallit ovat työläitä verrattuna Simin (2017) malliin. Tämän opinnäytetyön näkökulmasta on perusteltua toteuttaa opinnäytetyö Simin (2017) mallia mukaillen sen yksinkertaisuuteen perustuen. Kuviossa 2 on esitetty mukaillen Bergströmin ym. (2021, 229) malli *route for classifying high granularity assets*.



Kuvio 2: Aineistojen tiedon luokittelun prosessi (mukaillen Bergström ym. 2021, 229)

Rekisterinpitäjän osoitusvelvollisuutta on tutkinut Helsingin yliopiston oikeustieteellisessä tiedekunnassa pro gradu -tutkielmassaan Sonja Vainio (2018). Työssä *Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa* kuvataan tietosuoja-asetuksen (2016/679/EU) rekisterinpitäjälle osoitusvelvollisuuden merkitystä käytännössä. Vainio (2018, 21) toteaa, että rekisterinpitäjän tulee kehittää organisaatiossa tietosuojaratkaisuja, jotta riski tietosuojaloukkauksille pienenee. Rekisterinpitäjän keinoja riskin pienentämiseksi ovat esimerkiksi henkilötietoja käsittelevien ja siitä päättävien velvollisuuksien vahvistaminen ja täsmentäminen (Vainio 2018, 21). Tämä käytännössä usein tarkoittaa viraston sisäisiä ohjeistuksia, politiikkoja tai vastaavia ohjaavia toimintoja.

EU:n tietosuojatyöryhmän osoitusvelvollisuutta koskevassa mietinnössä (00062/2010/EU WP 173, 9) todetaan, että rekisterinpitäjän velvollisuus on toteuttaa toimivat ja asianmukaiset ratkaisut henkilötietojen käsittelyyn liittyvien periaatteiden toteuttamiseksi. Lisäksi sama mietintö määrittää, että rekisterinpitäjän tulee kyetä osoittamaan näiden toimien toteutumisen (00062/2010/EU WP 173, 9). Käytännössä vastuu periaatteellisten ratkaisujen toteuttamiseksi ja raportoimiseksi jää rekisterinpitäjälle.

Vainion (2018, 29) mukaan Euroopan unionin tietosuojaryhmän osoitusvelvollisuutta koskevassa mietinnössä (2010, 9) rekisterinpitäjän osoitusvelvollisuus jakautuu kahteen: ensinnäkin tulee tehdä toimivat ja asianmukaiset toimet henkilötietojen käsittelyyn liittyvien periaatteiden toteuttamiseksi ja toiseksi todistaa, että toimet on tehty. Vainio (2018, 29-30) toteaa Bennetin (2010, 6) tarkastelleen rekisterinpitäjän ilmoitusvelvollisuutta ja jakaneen sen kolmeen eri elementtiin: Osoitusvelvollisuus periaatteiden tasolla (*accountability of policy*), osoitusvelvollisuus menettelyjen tasolla (*accountability of procedures*) ja osoitusvelvollisuus käytäntöjen tasolla (*accountability of practice*).

Osoitusvelvollisuus periaatteiden tasolla tarkoittaa käytännössä, että rekisterinpitäjä todistaa määritelleensä tietosuojaperiaatteet ja tietosuojakäytänteet. Osoitusvelvollisuus menettelyjen tasolla tarkoittaa sitä, että edellä mainittuja tietosuojaperiaatteita ja tietosuojakäytänteitä on otettu käyttöön. Osoitusvelvollisuus käytäntöjen tasolla koostuu dokumentaatiosta, joka on laadittu periaatteiden ja menettelyjen toteuman dokumentoinnista. (Vainio 2018, 29-30.)

Diamantopoulou, Tsohou & Karyda toteavat julkaisussaan *From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls*, että tietoturvatarkastuksista ollaan siirtymässä kohti henkilötietojen suojan valvontaa, jossa tutkitaan yrityksen standardinmukaisuutta suhteessa tietosuoja-asetuksen vaatimukseen (2020, 648). Diamantopoulou ym. (2020, 645) selvittävät julkaisussaan toimenpiteitä, joita tulee standardin noudattamisen lisäksi toteuttaa, jotta yritys selviää tietosuoja-asetuksen vaatimuksista.

Julkaisun mukaan henkilötietoja sisältävät tietoluokat olisi tunnistettava ja niistä on pidettävä luetteloa (Diamatopoulou ym. 2020, 651). Tiedon, joka järjestelmään tallennetaan, tulee olla ajantasaista ja tietojen ajantasaisuutta tulee valvoa sekä tarpeeton tieto on poistettava järjestelmästä (Diamatopoulou ym. 2020, 655). Diamantopoulou ym. (2020, 655) toteavat, että tietojen tulee olla luottamuksellisia, eheitä ja niiden saatavuus tulee varmistaa. Julkaisun tutkimustulokset vahvistavat käsitystä siitä, että henkilötietojen arviointi osana tiedon luokittelun arviointia on perusteltua.

3.3 Katsaus tietojen luokitteluun

Luvussa perehdytään kirjallisuuskatsauksen keinoin tietojen luokitteluun eri lähteiden pohjalta. Aineistoon perehtymisen pohjalta kirjoitettiin katsaus tietojen luokitteluun. Tietojen luokittelu on tämän opinnäytetyön merkityksellisin käsite. Kirjallisuuskatsauksen aineistoksi on valittu Valtionhallinnon tietoturvallisuuden johtoryhmän julkaisut VAHTI (2006) Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI (2008) Valtionhallinnon tietoturvallisuussanasto ja VAHTI (2010) Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Lisäksi kirjallisuuskatsauksessa on hyödynnetty standardia SFS-EN 27002 (2017) ja Jason Andressin (2014) teosta Tietoturvan perusteiden ymmärtäminen teoriassa ja käytännössä, *The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice*. Kirjallisuuskatsauksessa on hyödynnetty Häätäkeskuslaitoksen dokumentaatiota hätäkeskustietojärjestelmän käyttöoikeuspolitiikasta (Hätäkeskuslaitos 2018b).

Standardin SFS-EN 27002 (2017, 23) mukaan tiedon luokittelun tavoitteena on varmistaa, että tiedon suojaustaso on riittävä ja, että suojaustaso määritetään arvioimalla tiedon kasautumista, luottamuksellisuutta, eheyttä ja tiedon saatavuutta sekä muita mahdollisia vaatimuksia. Tiedon luokittelun periaatteiden tulee olla yhdenmukaiset koko organisaatiossa (SFS-EN 27002 2017, 23). Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI (2008, 101) määrittelee, että tiedon omistaja asettaa määritettyjen perusteiden mukaan tiedot luokkiin. Käytännössä siis tiedon luokittelusta päättää tiedon omistaja (VAHTI 2008, 101).

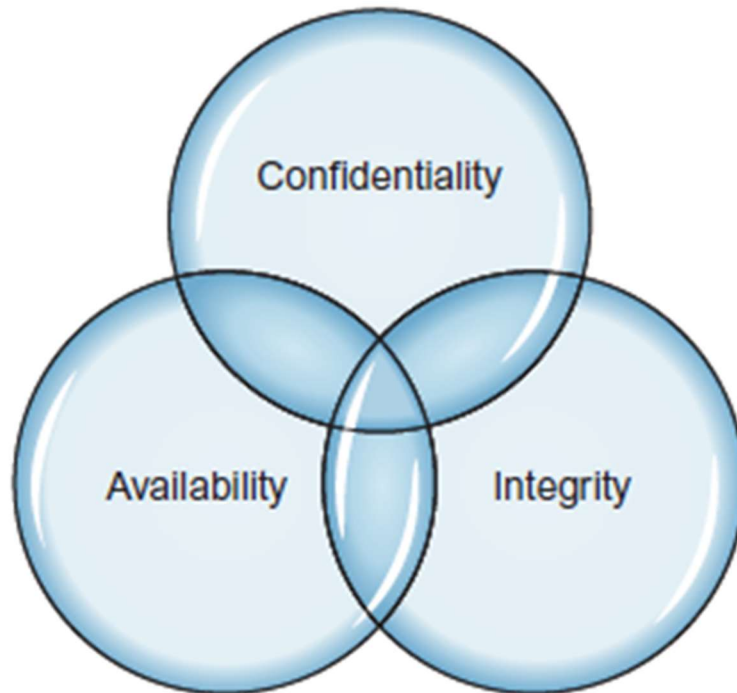
Standardi SFS-EN 27002 (2017, 6) korostaa sitä, että organisaation on tärkeä tunnistaa omat turvallisuusvaatimuksensa. Näiden vaatimusten tärkeimmät lähteet ovat lainsäädäntö, riskien arviointi sekä organisaation omat periaatteet liittyen tiedon käsittelyyn, tallentamiseen ja arkistointiin. Hallintakeinot on mitoitettava haittaan, joka voisi toteutua hallintakeinon puuttumisen vuoksi. Tässä opinnäytetyössä keskitytään kehittämään organisaatiolle hallintakeino, jolla tiedon käsittelyä ja tallentamista koskevia periaatteita määritellään tiedon luokittelun näkökulmasta. Standardin SFS-EN 27002 (2017, 6) mukaan hallintakeino voidaan valita standardista tai uusi hallintakeino voidaan tarvittaessa kehittää. Opinnäytetyön lähtökohta on kehittää uusi hallintakeino.

Tieto tulee luokitella lakisääteisten vaatimusten mukaisesti. Luokittelua täydennetään sen mukaan, mikä on tiedon arvo ja kriittisyys. Lisäksi tulee pohtia, mitä tiedon luvaton paljastuminen aiheuttaa, tai mitä tapahtuu, jos tietoa muokataan toisen näköiseksi tai toiseksi tiedoksi. Tiedon osalta tulee pohtia, kuka tietoa saa käsitellä ja nähdä. On arvioitava, mitä hyötyä tiedon näkyvyyden rajoittamisella saavutetaan, ja onko rajoittamisella joitakin haittavaikutuksia tiedon operatiiviseen käyttämiseen. Onko tieto jollakin tavalla arkaluonteista tietoa, henkilötietoa tai onko tieto toimintamallien näkökulmasta suojattavaa tietoa? (SFS-EN 27002 2017, 23.)

Standardin SFS-EN 27002:2017 (2017, 23) mukaan tiedon omistaja luokittelee oman tietonsa ja vastaa sen luokituksista. Tiedon näkökulmasta on tärkeää, että tieto luokitellaan linjakaasti ja yhtenäisesti koko järjestelmän läpi. Tiedon luokittelua voi helpottaa kokoamalla tietoryhmiä, joiden arviointi toteutetaan samojen luokitteluperiaatteiden mukaisesti. Luokittelun kriteeristö tulee olla luokittelijalla tiedossa, jotta myös myöhempi tarkastelu pystytään toteuttamaan tallennetulle tiedolle. Luokitteluperiaatteiden suojaustasoa arvioitaessa tulee arvioida ja analysoida tiedon luottamuksellisuus, eheys ja saavutettavuus sekä muut mahdolliset vaatimukset (SFS-EN 27002 2017, 23).

Tiedon luokittelussa on käytännöllistä huomioida tietosuoja-asetuksen (2016/679/EU) 4 artiklan 1 kohdan mukaiset henkilötiedot. Luokittelussa kannattaa ottaa tämä näkökulma huomioon, jotta päällekkäiseltä työltä voidaan välttyä. Tätä tietoa voidaan hyödyntää arvioitaessa tietojen tarkastusprosessin luontia ja raportointia rekisterinpitäjälle. Rekisterinpitäjä on erityisesti kiinnostunut niiden tietojen luokittelusta, joissa on suoranaisesti tai epäsuorasti henkilötietoja. Nämä tiedot ovat käytännön syistä syytä erottaa muusta tietojen luokittelusta omaksi raportoitavaksi kokonaisuudeksi.

Tiedon luottamuksellisuus (*confidentiality*), eheys (*integrity*) ja saatavuus (*availability*) ovat perusta tietoturvallisuuden yleiseen käsitteeseen, CIA-malliin (Andress 2014, 5). Tämän mallin lyhenteen kirjaimet tulevat luottamuksellisuuden, eheyden ja saatavuuden englanninkielisistä alkukirjaimista. CIA-mallista puhutaan myös tietoturvan kolmijalkana tai kolmikkona. Luottamuksellisuus, eheys ja saatavuus on termeinä avattu tarkemmin tämän opinnäytetyön tietope-
rusteiden kappaleessa 3.2 keskeiset käsitteet.



Kuvio 3: CIA-malli (mukaillen Andress 2014, 6)

Hätäkeskustietojärjestelmä on järjestelmä, joka muodostaa tietoaaineiston kokonaisuuden. Tietoaaineiston kokonaisuus sisältää erimuotoista tietoa erilaisia käyttötarkoituksia varten. Käytännössä tieto sisältää dataa eri viranomaisten toimintaa mahdollistavista tiedoista. Tiedot voivat olla luottamuksellisia tietoja, henkilötietoja tai arkaluonteisia tietoja. Data syötetään pohjatiedoksi sille, että hätäkeskustietojärjestelmällä voidaan toteuttaa sen tietosuojaselosteen mukaisia toimia. Hätäkeskustietojärjestelmä on henkilörekisteri, josta on laadittu asianmukainen tietosuojaseloste. (Hätäkeskuslaitos 2022a.)

Hätäkeskustietojärjestelmän tietojen ylläpidossa pyritään hallinnollisen tietoturvallisuuden mukaisesti siihen, että tietojen syöttövastuu on selkeä kaikissa olosuhteissa. Tiedon omistajuuden tulee aina olla selkeä, ja henkilön, joka tiedon järjestelmään syöttää, tulee tietää mitä on tekemässä (SFS-EN 27002 2017, 23). Vastuu henkilön kouluttamisesta on tiedon omistajalla. Ohjeistukset tiedon syöttämiseksi on laadittu tiedon omistajan ja Hätäkeskuslaitoksen yhteistyössä. Datan syöttömuoto ja periaatteet on sovittu käyttäjien kesken siten, että eri toimijoiden välinen tieto erottuu järjestelmästä loogisesti. Osa datasta sisältää metatietoja, joilla hallitaan tiedon näkyvyyttä ja jakelua järjestelmän sisällä hyvän tiedonhallintatavan mukaisesti.

Järjestelmän hallinnollinen data jakautuu kahteen osaan, yhteisiin tietoihin tai viranomaisen sisäisesti käytettäviin tietoihin. Hyvän tiedonhallintatavan mukaisesti järjestelmän tietojen

ylläpito on jaoteltu erilaisten käyttöoikeuksien mukaisesti viranomaisten kesken. Häätäkeskus-tietojärjestelmän käyttöoikeuspolitiikalla hallitaan järjestelmän käyttöoikeuksia siten, että tietoon voi olla lukuoikeus, muokkausoikeus tai ei oikeutta lainkaan (Hätäkeskuslaitos 2018b). Käyttöoikeuspolitiikalla hallitaan osaltaan tiedon suojaamista järjestelmän sisällä. Häätäkeskus-tietojärjestelmän käyttöoikeuspolitiikka (Hätäkeskuslaitos 2018b) määrittelee lisäksi sen, millaiset käyttöoikeustasot käyttäjäorganisaatiolla on olemassa. Eri käyttöoikeustasoilla on erilaiset käyttöoikeudet. Käytännössä käyttöoikeustasot jakautuvat tasoille: tiedon katselija, paikallisen tiedon ylläpitäjä, tiedon omistaja. Tiedon katselijan käyttöoikeutta voidaan laven-taa tarvittaessa siten, että hän kykenee toimimaan tietyn datan osalta paikallisen tiedon yllä-pitäjänä. VAHTI (2006, 35) mukaisesti käyttäjähallinnan tulee olla luotettava, ja vain käyttö-oikeutetut yksilöidyt henkilöt voivat muokata, lisätä tai arkistoida dataa järjestelmään. Tieto-ten käsittelyoikeus sidotaan henkilön työtehtäviin (VAHTI 2010, 37).

VAHTI (2010, 29) mukaan viranomaisen on säännöllisesti arvioitava tietojärjestelmänsä tal-lennetut tiedot tietojen suojauksen ja eheyden osalta. Toisaalta VAHTI (2010, 16) määritte-lee, että viranomaisen on arvioitava tietovarantoa käyttävien tietojärjestelmien ja tiedon kä-sittelyprosessien ajantasaisuus. Tieto tarkistetaan sen vuoksi, että tehtävän hoito voi sujua häiriöttömästi (VAHTI 2010, 29).

Järjestelmään syötetyn tiedon muoto on merkityksellinen tietoa syötettäessä. Tiedon muo-dolla voidaan hallita tiedon käytettävyyttä ja eheyttä. Tiedon muoto helpottaa tiedon tunnis-tamista ja sen pohjalta tietoa osataan helposti tulkita ja lukea järjestelmän käytön yhtey-dessä. Loppukäyttäjä osaa tunnistaa vakiomuotoista tietoa paremmin kuin sitä tietoa, joka ei ole vakiomuotoista. Tiedon käyttäminen operatiivisessa tilanteessa helpottuu, kun samankal-tainen tieto on yhtenäisessä muodossa.

Tiedon ylläpitäjä hyötyy tiedon eheydestä. Tiedon eheys helpottaa tietoaineistojen tarkasta-mista oikeellisuuden näkökulmasta. Tiedon muodolla saavutettu eheys vähentää epäselvyyksiä ja helpottaa ristiin vertailua silloin, kun tarkastetaan aineiston puutteita eri tietolähteiden välillä. Tiedon muoto helpottaa tiedon haettavuutta järjestelmän sisällä. Tiedon ylläpitoa varten tiedon muoto pyritään ohjaamaan yhtenäiseksi eri tiedon ylläpidosta vastaavien pää-käyttäjien kesken.

Tiedon syötön yhteydessä tallennettava tieto versioituu järjestelmässä. Järjestelmään tallen-tuu tiedon tallennushetki, tallentaja ja tallennushetken versio. VAHTI (2010, 21) mukaisesti tietotyön yhteydessä muodostuu automaattisesti tallenteita ja näitä tulee käsitellä kuin asia-kirjoja. Tallenteet helpottavat historian tarkastelua sekä ongelmatilanteiden selvittämistä. Versiohistorian tallentuminen helpottaa häiriön hallintaa ja sen kautta palaamista edelliseen versioon, jos tähän tulee kyseisen tiedon osalta tarve. VAHTI (2010, 61) mukaan tiedolta

odotetaan eheyttä ja kiistattomuutta. Versiohistoria mahdollistaa kiistattomuuden tarkastelun tiedon hallinnassa.

Järjestelmän toiminnallisuuksia ja toimintaa ohjataan erilaisilla tietojen konfiguraatioilla. Konfiguraatio on usein lukuisten eri tietoaineistojen tai parametrien kokonaisuus, jossa tiedolla ohjataan järjestelmän toiminnallisuuksia. Jos testauksessa konfiguraatio havaitaan puutteelliseksi tai virheelliseksi, voidaan toiminnallisuus palauttaa takaisin edelliseen toimivaan konfiguraatioon. Konfiguraatiomuutoksista tallennetaan versiohistoria ja tätä kautta tiedon tallentajalla on mahdollisuus palata edelliseen toimivaan konfiguraatioon. Häätäkeskuslaitoksessa järjestelmätason konfiguraatiosta vastaa häätäkeskuslaitoksen pääkäyttö. Järjestelmätason konfiguraation muutoksenhallinta on suunnitelmallista ja ennalta aikataulutettua. Muutokset järjestelmätasolla testataan ennen käyttöönottoa muutoksen toimivuuden varmistamiseksi.

3.4 Keskeiset käsitteet

Tietosuoja on perusoikeus, määrittää tietosuojavaltuutettu. Tietosuoja turvaa rekisteröidyn, käytännössä henkilön, oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Sen tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Henkilötietojen käsittelyn on aina perustuttava lakiin. (Tietosuojavaltuutetun toimisto 2022.)

Henkilötiedolla tarkoitetaan EU:n tietosuoja-asetuksen (2016/679/EU) 4 artiklan 1 kohdan mukaan sellaisia tietoja, jotka liittyvät luonnolliseen henkilöön. Tunnistettavuus voi toteutua joko suoraan tai epäsuorasti tunnistetietojen perusteella.

Rekisterinpitäjällä tarkoitetaan EU:n tietosuoja-asetuksen (2016/679/EU) 4 artiklan 7 kohdan määritelmän mukaisesti luonnollista henkilöä tai oikeushenkilöä, viranomaista tai virastoa, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä arvioi henkilötiedon käsittelyyn liittyviä riskejä. Rekisterinpitäjä arvioi rekisteröidyn näkökulmasta, mitä oikeuksia ja vapauksia käsittely voi vaarantaa tai millaisia vahinkoja rekisteröidylle voi aiheutua.

Tietosuojavastaava tulee nimittää aina kun tietojenkäsittelyä suorittaa viranomaisen tai julkishallinnon elin. Tietosuojavastaava tulee nimittää, kun ydintehtävät muodostuvat käsittelytoimista, jotka näiden luonteen, laajuuden tai tarkoituksen vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä tai järjestelmällistä seuranta. Lisäksi jos henkilötietoja käsitellään laajamittaisesti erityisiin henkilöryhmiin liittyen, on tietosuojavastaava nimitettävä. (2016/679/EU, artikla 37.)

Tietosuojavastaava seuraa ja valvoo henkilötietojen käsittelyä. Tietosuojavastaava tuo esille havaitsemansa puutteet tietosuojassa ja auttaa virastoa tietosuojasäännösten

noudattamisessa. Tietosuojavastaava neuvoo ja ohjaa viraston johtoa toimimaan oikein tietosuojasäännösten mukaisissa velvollisuuksissa. Tietosuojavastaava ohjaa henkilötietoja käsitteleviä henkilöitä toimimaan virastossa oikein. (Tietosuojavaltuutetun toimisto 2022.)

Tietoturva on yksi tietosuojan toteuttamisen keino, ja sillä suojataan tietoaineistoa sekä tietojärjestelmiä. Tietoturvalla tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus hallinnollisesti, teknisesti tai organisatorisesti. Lisäksi tietoturvalla tässä opinnäytetyössä tarkoitetaan erityisesti tietoaineistojen turvaamista. (Tiedonhallintalaki 906/2019.)

Tiedon luokittelun tavoitteena on varmistaa, että tiedon suojaustaso on riittävä. Suojaustaso määritetään arvioimalla tiedon kasautumista, luottamuksellisuutta, eheyttä ja tiedon saatavuutta sekä muita mahdollisia vaatimuksia. Tiedon luokittelun periaatteiden tulee olla yhdenmukaiset koko organisaatiossa. (SFS-EN 27002 2017, 23.)

Tiedon saatavuudella tarkoitetaan sitä, miten tieto on hyödynnettävissä vaaditulla tavalla ja haluttuna aikana (VAHTI 2008, 54. Sanastokeskus 2021). Häätäkeskustietojärjestelmän näkökulmasta saatavuudella on merkitystä tilanteissa, joissa toimintoja joudutaan mahdollisesti siirtämään palveluiden osalta varajärjestelyiden puolelle. Varajärjestelyt ovat osa häätäkeskustoitinnan varautumistoimenpiteitä. Tiedon saatavuus voidaan arvioida tietoluokakohtaisesti tiedon luokittelun yhteydessä.

Tiedon eheydellä tarkoitetaan sitä, että tieto ei ole muuttunut luvatta tai vahingossa. Tiedon eheydellä tarkoitetaan myös sitä, että muutokset voidaan aina todentaa jälkikäteen sekä sen, kuka muutoksen on toteuttanut. Tiedon teknisellä eli muodollisella eheydellä tarkoitetaan sitä, että tietoaineiston samanlainen tieto on syötetty samassa teknisessä muodossa järjestelmän sisällä. Häätäkeskustietojärjestelmän käytön näkökulmasta on erityisen tärkeää, että keskenään yhtäläinen tekninen tieto on kirjattu muodollisesti eheästi ja ristiriidattomasti. (VAHTI 2008, 25; Sanastokeskus 2021.)

Tiedon luottamuksellisuudella tarkoitetaan sitä, että tieto on vain niiden henkilöiden käsiteltävissä, jotka tietoon ovat oikeutettuja (SFS-ISO 27002, 33). Tieto ei saa paljastua toisille. Käytännössä tiedon luottamuksellisuutta parannetaan esimerkiksi käyttöoikeuksien hallinnalla sekä määrittämällä erilaisille tietoluokille tai tietoalkiotyypeille tiedon jakelu ja tarvittaessa turvallisuusluokka (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtioneuvostossa 1101/2019).

Tiedon kasautuminen tarkoittaa eri tietoaineistojen keskinäistä sidosta, joka muodostaa kokonaisuuden. Yksittäiset suojattavat tiedot voivat muodostaa kytkeytyessään yhteen tietovarannon, jonka turvallisuusluokka voi johtaa kokonaisuuden turvallisuusluokan korottumiseen, ja siten olla korkeampi kuin yksittäisen suojattavan tietoalkion. Kasausvaikutusta tulee aina

arvioida tapauskohtaisesti. Kasausvaikutusta arvioitaessa tulee huomioida, muodostaako tietoalkioiden joukko yhdistettynä tietokasauman, jonka joutuminen ulkopuolisen käsiin voisi aiheuttaa vahinkoa hätäkeskustoimintaan osallistuvien viranomaisten toiminnalle, esimerkiksi paljastamalla viranomaisen toimintamallin tietyssä tilanteessa. (Valtiovarainministeriö 2021, 34-35.)

4 Opinnäytetyön prosessi

Tämä opinnäytetyö on tutkimuksellinen kehittämistyö, joka toteutetaan konstruktiivisella lähestymistavalla. Tutkimusmetodeina käytetään kirjallisuuskatsausta, havainnointia ja haastatteluja. Opinnäytetyön perusteet nousevat lainsäädännön noudattamisesta. Teorian laatimisessa hyödynnetään lainsäädännön ja valtionvarainministeriön tiedonhallintalautakunnan suositusten lisäksi erilaisia julkaisuja, standardeja, opinnäytetöitä, tieteellisiä julkaisuja ja kirjallisuutta.

Tutkimuksellinen kehittämistyö sopii käytännön ratkaisujen hakemiseen sekä prosessien kehittämiseen. Tutkimuksellisen kehittämistyön tarkoituksena on luonnostella ja kehittää ratkaisuja ennen niiden käyttöönottoa. Pyrkimyksenä on, että opinnäytetyön avustuksella voidaan kehittää toimiva ratkaisumalli tutkittavaan ongelmaan ja parantaa vallitsevaa tilannetta tai löytää uusia ratkaisuja. (Ojasalo, Moilanen & Ritalahti 2015, 21.)

4.1 Kehittämistyön kulku ja muoto

Tutkimuksellisen kehittämistyön prosessin tavoitteena on ottaa saadut tutkimuksen tulokset käytännön työelämässä käyttöön (Ojasalo ym. 2015, 21). Kehittämistyöllä halutaan selvittää ja saada aikaiseksi selkeä prosessi tiedon luokittelulle. Tämän pohjalta on selvitettävissä, miten ja millaisella syklillä tietojärjestelmän tietoluokkien tietoja tarkastetaan. Tarkastamisen ajallinen sykli voi vaihdella luokituksen tärkeyden tason pohjalta.

Kehittämistyön lopputuloksena opinnäytetyöstä saadaan hyöty työelämään: pystytään kehittämään ja julkaisemaan virastolle hätäkeskustietojärjestelmän tiedon luokittelumalli. Ojasalo ym. (2015, 24) kuvaavat, että tekemällä lopputuloksista johtopäätökset selvitetään, onko kehittämistyöstä ollut arvoa ja miten työtä voi jatkokehittää opinnäytetyön valmistumisen jälkeen. Uusia kehitysnäkymiä on tarpeen kirjata, jos niitä havaitaan (Ojasalo ym. 2015, 24).

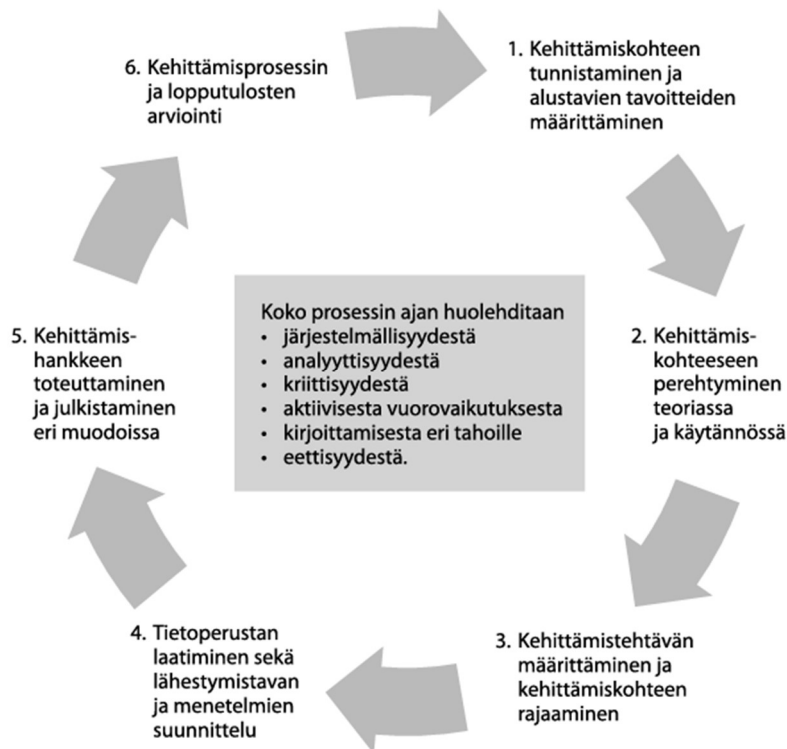
Työn toteutuksen tarve nousi esille Hätäkeskuslaitoksen sisäisen tietosuojan vuosikellotyöryhmän (Hätäkeskuslaitos 2021) työskentelyn kautta keväällä 2021. Hätäkeskustietojärjestelmän vaikutustenarvioinnissa oli havaittu tarve hätäkeskustietojärjestelmän tietojen luokittelulle (Hätäkeskuslaitos 2020). Tavoitteeksi asetettiin, että tiedon luokittelulle on malli vuoden 2022 aikana. Opinnäytetyön kirjoittaja sitoutui toteuttamaan luokittelumallin luomisen

virkaehtäviin liittyvänä työtehtävänä. Työtehtävä oli mielekästä yhdistää tämän opinnäytetyön prosessiin.

Kehittämistyön toteuttamiseksi valittiin tutkimuksellisen kehittämisen prosessiksi Ojasalon ym. (2015, 24) avaama prosessi. Prosessi on esitetty kuvana alla (kuvio 4). Prosessissa kehittämiskohteen tunnistamisen ja alustavien tavoitteiden määrittämisen jälkeen perehdytään kehittämiskohteeseen teoriassa ja käytännössä. Tiedon luokittelun teoriaa on selvitetty laajalaisesti tekemällä hakuja internet-sivustoille sekä tutkimalla kirjallisuutta, opinnäytetöitä, standardeja sekä muita julkaisuja. Häätäkeskustietojärjestelmän tietoaaineisto on virkatyön kautta syvällisesti tuttua. Tietoaaineistoja ylläpidetään ja siten käytännön perehtymistä tapahtuu virkatöiden ohella koko ajan. Kehittämistehtävän tarkempaa määrittelyä toteutettiin syksyllä 2021 opintojen ohella. Syksyllä 2021 osallistuin Laurea-ammattikorkeakoulun opintojaksolle Tutkimus- ja kehittämismenetelmät. Opintojakson kautta aloitin opinnäytetyön tutkimussuunnitelman laatimisen ja jatkoin kehittämistehtävän määrittämistä ja kehittämiskohteen rajaamista aihepiirin ympärillä.

Opinnäytetyön kirjoittamisen pohjana oli tietoperustan laatiminen sekä lähestymistavan ja menetelmien suunnittelu. Tutkin tietoperustaa laajasti ja päätin pohjata opinnäytetyön erityisesti lainsäädännön ja keskeisten käsitteiden ympärille. Täydensin tietoperustaa standardeihin, julkaisuihin, kirjallisuuteen ja aiempiin tutkimuksiin perehtymällä. Aiemmissä tutkimuksissa erityinen mielenkiintoni kohdistui valitun aihepiirin, tietojen luokittelun, ympärille. Tietojen luokittelusta oli kaiken kaikkiaan hyvin hajanaista tietoa eri lähteissä, joten päätin kirjata erillisen kirjallisuuskatsauksen tietojen luokittelun ympäriltä. Tämä kirjallisuuskatsaus toimii myös yhtenä tutkimusmenetelmänä. Aiempien tutkimusten ja tieteellisten julkaisujen kautta sain myös arvokkaita konkreettisia esimerkkejä tietojen luokittelun määrittämisen taivoista.

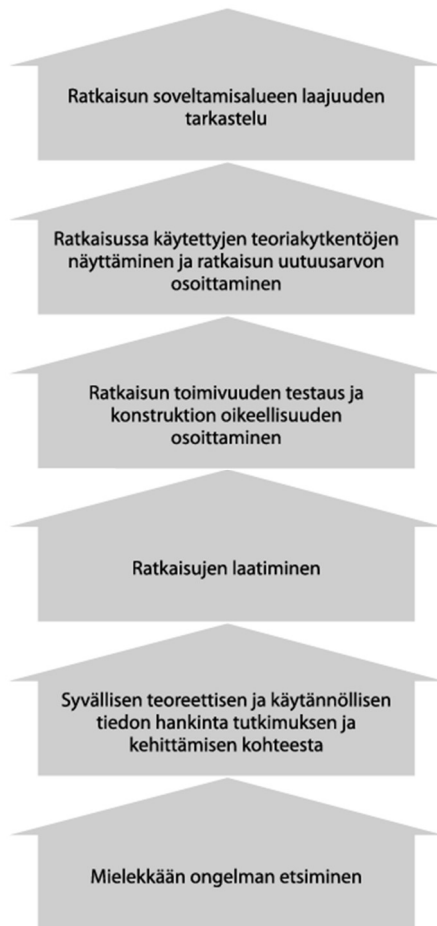
Kehittämistyön toteuttamiseksi tutkimusmenetelminä käytin kirjallisuuskatsausta, havainnointia ja teemahaastatteluja. Havainnoinnin tavoitteena oli laatia menetelmälomake, jotta teemahaastattelut voidaan toteuttaa menetelmälomaketta hyödyntäen. Havainnoinnin tuloksena syntyi tämän opinnäytetyön menetelmälomake (liite 1), tietotyyppien luokittelun aputaulukko (liite 2) ja palautekysely (liite3). Teemahaastattelut päätin toteuttaa viranomaisittain. Teemahaastatteluissa käydään läpi haastattelun kulku, kerrotaan viranomaiselle mitä teemahaastattelun aikana tehdään ja toteutetaan itse tiedon luokittelu. Haastattelun yhteydessä kerätään palaute haastattelutilaisuuden tuntemuksista. Kehittämisprosessin ja lopputulosten arviointi toteutetaan tulosten analysoinnin ja johtopäätösten kautta.



Kuvio 4: Tutkimuksellisen kehittämistyön prosessi (Ojasalo ym. 2015, 24)

Opinnäytetyö toteutetaan konstruktiiivisella lähestymistavalla. Konstruktiiivisella lähestymistavalla tarkoitetaan, että opinnäytetyötä varten on etsitty mielekäs ongelma, tiedon luokittelun tarve. Luokittelumallin toteutus ratkaistaan konstruktiiivisen tutkimuksen prosessin (kuvio 5) mukaisesti (Ojasalo ym. 2015, 66). Opinnäytetyössä pureudutaan syvällisesti teoriaan. Teorian kautta haetaan tietoa kehityksen kohteesta (Ojasalo ym. 2015, 66). Tutkimuksen edistämiseksi ja eri mallien havainnoimiseksi tietoa on haettu aiemmin toteutetuista tutkimuksista ja tieteellisistä julkaisuista. Näitä malleja tarkastellaan ja hyödynnetään, jotta parhaat puolet voidaan huomioida tässä opinnäytetyössä. Omaan ammattitaitooni pohjautuen tuon asiantuntemuksen substanssiin hätäkeskustietojärjestelmän tietomallista sekä arkkitehtuurista.

Ratkaisu valitaan ja sen pohjalta laaditaan tapa, jolla tutkimusta edistetään. Ratkaisua testataan projektin kuluessa ja tarvittaessa mallia muutetaan vastaamaan tehtyjä havaintoja. Ratkaisussa pyritään löytämään uutuusarvo, jonka pohjalta voidaan todeta, että malli on toimiva. Jos mallin toimivuudessa havaitaan puutteita, korjataan ratkaisumallia suuntaan, jolla toimivuutta voidaan parantaa. Ratkaisun soveltuvuutta muihin soveltamiskohteisiin tutkitaan. (Ojasalo ym. 2015, 66-67.)



Kuvio 5: Konstruktiivisen tutkimuksen prosessi (Ojasalo ym. 2015, 67)

4.2 Kirjallisuuskatsaus

Opinnäytetyöhön vaikuttavaan teoriaan perehdytään kirjallisuuskatsauksen muodossa. Kirjallisuuskatsauksessa pureudutaan asiaan erityisesti tiedon luokitteluun standardien, valtionhallinnon tietoturvallisuuden johtoryhmän dokumenttien, kirjallisuuden sekä tieteellisten julkaisujen kautta. Tutkimuksen teoriaa käsitellään monipuolisesti erilaisten lähteiden avulla ja niiden avulla selkeytetään tutkittavaa kokonaisuutta. Kirjallisuuskatsaus rajataan koskemaan tutkittavaa asiaa, tiedon luokittelua (Jamk 2022).

Kirjallisuuskatsauksen muotona toteutetaan kuvaileva kirjallisuuskatsaus, jonka orientaatio on narratiivinen. Katsauksen toteutustapana tuotetaan toimituksellinen kirjallisuuskatsaus. Narratiivinen kirjallisuuskatsaus on metodisesti kevyin kirjallisuuskatsauksen muoto. Tutkittavaa ilmiötä kuvataan opinnäytetyön näkökulmasta riittävän laaja-alaisesti pureutumalla puhtaasti käsiteltävään aiheeseen. Kirjallisuuskatsaus ei tuota opinnäytetyölle tuloksia tutkittavaan asiaan. (Salminen 2011, 6-8.)

Toimituksellinen kirjallisuuskatsaus tarkoittaa lyhyehköä kirjallisuuskatsausta, joka tukee tässä opinnäytetyössä käsiteltävää teemaa. Käsiteltävä aineisto on kohtuullisen suppea eikä sisällä kaikkea aiheesta kirjattua aineistoa. Katsaus on kirjoitettu helppolukuisesti ja kirjoituksen synteesi voi muodostua puolueelliseksi. Kirjallisuuskatsauksen tavoitteena on tuottaa taustatietoa käsiteltävästä aiheesta kirjoittajan silmin. (Salminen 2011, 7.)

Kirjallisuuskatsauksen aineistoksi valikoitui Valtionhallinnon tietoturvallisuuden johtoryhmän julkaisut VAHTI (2006) Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI (2008) Valtionhallinnon tietoturvallisuussanasto ja VAHTI (2010) Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Lisäksi kirjallisuuskatsauksessa on hyödynnetty standardia SFS-EN 27002 (2017) ja Jason Andressin (2014) teosta *The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice*. Kirjallisuuskatsauksessa on hyödynnetty Häätäkeskuslaitoksen dokumentaatiota hätäkeskustietojärjestelmän käyttöoikeuspolitiikasta (Hätäkeskuslaitos 2018b).

4.3 Havainnointi

Ratkaisujen laatimisessa ideoidaan ja kerätään aineisto testausvaihetta varten havainnoimalla hätäkeskustietojärjestelmää. Ratkaisujen laadinnan vaiheen aikana toteutetaan haastatteluja varten menetelmämakepohja. Menetelmämakepohjaa käytetään teemahaastattelun runkona. Menetelmämakepohjan laatimisessa hyödynnetään aiempia tutkimuksia, erityisesti Simin (2017) tutkimusta. Ratkaisut on saatu laadittua, kun menetelmämake sisältää kaikki tutkimuksen kannalta oleelliset tietotyypit ja muut tarpeelliset tiedot. Muita tarpeellisia tietoja on tietotyyppien luokittelua selventävä sanallinen kuvaus ja valmistautuminen palautteen saamiseen. Havainnointivaiheessa opinnäytetyön tekijällä on tarkoitus hyödyntää viraston asiantuntijaresursseja. Asiantuntijaresursseilta selvitetään idean ja tietosisällön toimitavuutta, käytännössä testataan ratkaisua (Ojasalo ym. 2015, 67).

Puusa & Juuti (2020, 127) kuvaavat, että ”havainnointi on tieteellisen aineistonhankinnan perusmenetelmä, jota tosiasiaassa tekee jokainen tutkija, joka on suorassa yhteydessä tutkittavaan ilmiöön”. Käytännössä tietoaineistoa kerätään järjestelmästä jäsenellen samalla aineistoa kohti sen lopullista muotoa. Havainnointi keskittyy tietoaineistoon ja niiden välisiin yhteyksiin hätäkeskustietojärjestelmässä. Tietoaineisto muokkautuu havainnoimalla tietotyypeiksi ja sitä kautta ne voidaan lisätä menetelmämakeelle osaksi luokittelua. Etuna voidaan todeta, että aineistosta voidaan toteuttaa muistiinpanoja ja sen kautta päästään tekemään päätöksiä, miten tietotyypeihin jakaminen on järkevä toteuttaa. Muistiinpanojen toteuttaminen on Valli & Aaltola (2015a, 157) mukaan esianalyysin toteuttamista. Työ on ketterää ja joustavaa tutkijan kannalta. Havainnoinnin pohjalta iteroidaan menetelmämake, jota hyödynnetään haastatteluissa.

4.4 Teemahaastattelu

Kirjallisuuskatsauksen ja havainnoinnin pohjalta on laadittu menetelmälomake. Menetelmälomakkeen toimivuuden testaus on tarkoitus toteuttaa laadullisella menetelmällä, neljässä eri teemahaastattelussa (Ojasalo ym. 2015, 105). Jokaiseen haastatteluun pyydetään mukaan hätäkeskustietojärjestelmää käyttävistä viranomaisista heidän viranomaispääkäyttäjänsä tai alueellisia tiedon ylläpitäjiä. Haastattelutilaisuudet järjestetään erillisinä haastatteluina Hätäkeskuslaitoksen, ensihoidon, pelastustoimen sekä poliisitoimen viranomaispääkäyttäjille. Haastattelut toteutetaan anonymisti. Haastateltavien henkilöllisyys raportoidaan toimeksiantajalle varsinaisen raportin yhteydessä.

Teemahaastattelun aihepiirit ovat ennalta määritelty samoiksi kaikissa haastatteluissa, vaikka niitä ei käsitellä välttämättä samassa järjestyksessä (Valli & Aaltola 2015a, 29). Haastattelun henkilömäärä haastattelua kohti on kokonaisuudessaan 2-3 henkilöä. Hirsjärvi, Remes ja Saja-vaara (2005, 200) kertoo Lähteenmaan (1991) tehneen tutkimuksia ja todenneen kokemukseensa perustuen, että ryhmässä haastateltavien määrän rajoittuvan kahdesta kolmeen. Tämän opinnäytetyön vahvuutena nähdään, että ryhmäkeskusteluihin osallistuvat henkilöt tuntevat toisensa hyvin. Luottamusta ei siis tarvitse rakentaa ventovieraiden kesken.

Aloitushetkellä tilaisuuden kulku käydään haastateltaville läpi. Teemahaastattelut toteutetaan siten, että vetäjä luo avoimen keskustelukulttuurin haastattelutilanteeseen. Vuorovaikutustilanne halutaan tietoisesti sellaiseksi, että haastateltavat pohtivat erityisesti keskenään teemaa, jota käsitellään. Tarvittaessa haastattelijan on tarkoituksenmukaista ohjata keskustelua kysymyksiin tai osallistua keskusteluun, jotta keskustelu ohjautuu oikein ja oikeaan suuntaan. Tarvittaessa keskustelutilanteen vetäjä pyrkii luomaan keskusteltavaan asiaan erilaisia lähestymiskulmia, jotta vuorovaikutus säilyy hyvänä ja avoimena keskustelijoiden kesken. Tutkimusaineisto saadaan kerättyä ryhmäkeskustelussa esille sillä, että osallistujat keskustelevat avoimessa keskinäisessä vuorovaikutuksessa ja haastattelijan ohjauksessa. Haastattelun tarkoituksena on koota tutkimusaineistoa, jonka pohjalta on mahdollista muodostaa tulos ja johtopäätökset. (Puusa & Juuti 2020, 107-109.)

Haastattelu suoritetaan ennalta laaditun suunnitelman mukaan. Ryhmähaastattelun keston tavoitteeksi voidaan asettaa, että haastattelusta suoriudutaan 1-2 tunnissa. Remes ym. (2006, 200) kertoo, että tunnista kahteen tuntia on tavanomaisen teemahaastattelun kesto. Haastattelun kulku dokumentoidaan menetelmälomakkeelle empiirisen aineiston kokoamiseksi. Haastattelun päätteeksi kerätään informaatiota haastattelun onnistumisesta ja menetelmästä palautekyselyllä. Haastateltavia pyydetään antamaan palaute kokemuksesta. Kokemus kirjataan nimettömänä prosessin kehittämistä varten. Jos prosessissa ilmenee tarve toteuttaa muutoksia, pyritään muutokset toteuttamaan ennen seuraavaa haastateltavaa kohderyhmää. Tällä menetelmällä saadaan tutkimukseen mukaan konstruktivista tutkimusotetta tavoitteena

kehittää luokittelumallia paremmaksi seuraavaa haastattelua varten. Muutokset menetelmälomakkeella dokumentoidaan. (Ojasalo ym. 2015, 111-112.)

Haastattelutilaisuudet toteutetaan videoyhteyden välityksellä. Tilaisuuksia ei tallenneta tietoturvasyihin ja tiedon turvaluokitukseen vedoten. Haastattelujen sisällä käsitellään ja keskustellaan luottamuksellista tietoa. Videoyhteyden välillä voi nousta haasteeksi se, miten keskustelun vetäjä voi aistia haastateltavien kehonkieltä ja sanatonta viestintää. Tunnistamisella on merkitystä siihen, että osataan kohdentaa ja tarkentaa kysymyksiä selvitettävään asiaan. Haastattelun vetäjä laatii ennalta riittävän keinovalikoiman, jolla keskustelua saadaan aikaiseksi haastateltavien välillä. Haastattelun vetäjä kirjaa jokaisen haastattelutilaisuuden jälkeen omat ensihavainnot talteen muistin tueksi (Puusa & Juuti 2020, 120).

4.5 Aineiston analysointi

Hätäkeskustietojärjestelmän sisältö on salassa pidettävää tai turvaluokiteltua aineistoa. Tiedon kirjaaminen ja julkaiseminen opinnäytetyöhön on tietotyyppien kasaantuvuuden osalta haasteellista. Tulosten ja johtopäätösten kirjaamisen vaiheessa tietosisältöä tullaan pelkistämään. Tietotyyppien nimet poistetaan ja lisätään niille numerot tuloksia esitettäessä (taulukko 1). Tällä ei kuitenkaan arvioni mukaan ole vaikutusta kehittämistyön toteuttamiseen. Opinnäytetyön kannalta merkittävää on se, toimiiko prosessin mukainen malli ja saadaanko sillä aikaan tiedon luokittelu tietotyyppien osalta (Ojasalo ym. 2015, 67). Ojasalo ym. (2015, 67) mukaan johtopäätösten osalta voidaan kuvata kokonaisuuksia ja toteutettuja käytäntöjä. Tältä osin ei ole merkityksellistä kuvata hätäkeskustietojärjestelmän detalleja.

Aineistoanalyysi toteutetaan aineistolähtöisesti. Aineiston tulokset analysoidaan ja johdetaan teemahaastattelujen pohjalta menetelmälomakkeelle kirjatusta asioista. Aineiston analyysi aloitetaan perehtymällä teemahaastattelujen yhteydessä täytettyihin menetelmälomakkeisiin. Puusa ja Juuti (2020, 148) kirjoittavat, että ensin tutkijan tulee saada kokonaiskuva tutkimusaineistoon. Tämän jälkeen aineisto pilkotaan osiin ja tarkastellaan pienemmissä osissa (Puusa ja Juuti 2020, 148). Aineistoa koodataan värikartaksi ja kokonaisuuksia muodostaviksi taulukoiksi. Puusa ja Juuti (2020, 150) toteavat, että ”tyypittelyn tavoitteena on havainnollistaa aineistoa yhdistettyjen eli eräänlaisten mallien avulla”. Taulukot muodostetaan tyypittelyn pohjalta. Kokonaisuutta täydennetään teemahaastatteluista litteroiduilla alkuperäisilmaisuilla, joita hyödynnetään täydentämään tyypittelyn pohjalta johdettavia tuloksia.

Taulukossa 1 esitellään, kuinka menetelmälomakkeet koodataan värein siten, että luottamuksellisuuden, saatavuuden ja eheyden sarakkeissa solut saavat värin. Väri lisätään sen mukaan, onko tietotyyppi analysoitu kolmiportaisuuden osalta korkeaan (K), normaaliin (N) vai matalaan (M) luokkaan. Korkea luokka merkitään punaisella värillä, normaali luokka merkitään sinisellä värillä ja matala luokka merkitään keltaisella värillä (taulukko 1). Värikartan avulla

voidaan tehdä tulkintoja tai johtaa tuloksia luottamuksellisuuden, saatavuuden ja eheyden luokitteluerovaihtelusta tai samankaltaisuudesta eri viranomaisten välillä.

Tietotyyppi	Poliisi			Pelastus			Ensihoito			Hätäkeskuslaitos		
	L	S	E	L	S	E	L	S	E	L	S	E
5	N	K	K	M	N	M	M	K	K	N	N	N
6	M	M	M	N/A	N/A	N/A	M	M	M	N/A	N/A	N/A

Taulukko 1: Tietotyyppien koodaus värein ja esittäminen taulukossa

Menetelmälomakkeista tyypitellään erilaisia taulukoita. Taulukossa 2 on yksi esimerkki taulukosta. Taulukoita kootaan tiedon luottamuksellisuuden, saatavuuden, eheyden, kasautumisen ja henkilötiedon tiedoista. Luottamuksellisuuden, saatavuuden ja eheyden osalta kootaan viranomaisittain lukumääräiset tulokset korkean, normaalin, matalan ja arvioimattomien tietotyyppien osalta (taulukko 2). Tuloksia esitetään yksittäisinä taulukkoina siten, että viranomaisittain rivien solut sisältävät kukin lukuarvon. Taulukoiden pohjalta suoritetaan aineiston analysointia ja johdetaan tuloksia.

Luottamuksellisuus	Korkea	Normaali	Matala	N/A
Poliisi	kpl	kpl	kpl	kpl
Pelastustoimi	kpl	kpl	kpl	kpl
Ensihoito	kpl	kpl	kpl	kpl
Hätäkeskuslaitos	kpl	kpl	kpl	kpl

Taulukko 2: Tiedon koontin esimerkkitaulukko

Analyysissä vertaillaan eri viranomaisten päätöksiä tietotyyppien luokittelusta ja koostetaan saadut havainnot tyypittelyn pohjalta. Havainnoista voidaan analysoida työlle tuloksia. Vallin & Aaltolan (2015b, 44) mukaan kokonaisuudet voidaan järjestää tutkimuksessa tutkijan tutkimuskysymyksen ehdoilla. Analyysin tavoitteena on ymmärtää kokonaisuus, jolla johdetaan päätökset tutkimusongelman ratkaisemiseksi (Vilka 2021, 91). Analyysillä arvioidaan eri viranomaisten eroavaisuuksia käsiteltävän tietoa-aineiston näkökulmasta ja pyritään löytämään yleistyksiä asioiden ympäriltä. Löydökset raportoidaan keskeisiin tuloksiin (Vilka 2021, 95). Keskeisten tuloksien pohjalta johdetaan opinnäytetyön johtopäätökset.

5 Tulokset

Tulokset kootaan havainnoinnin ja neljän teemahaastattelun perusteella. Tuloksissa käsitellään menetelmälomakkeen muokkautumista iteratiivisesti sekä teemahaastattelujen tuloksista johdettuja havaintoja. Tuloksia on johdettu tiedon kasaantumisesta, sen sisältämästä henkilötiedosta, tiedon luottamuksellisuudesta, saavutettavuudesta ja eheydestä. Tuloksien pohjalta laaditaan tälle opinnäytetyölle johtopäätökset.

En kyllä vielä yhtään tiedä mitä tässä käydään tekemään mutta kai se kohta meille selviää (pelastustoimen haastateltava 2).

Teemahaastattelut suoritettiin järjestyksessä: poliisi, pelastustoimi, Hätäkeskuslaitos ja ensihoito. Teemahaastattelut toteutettiin kolmen haastattelun osalta videoyhteyttä hyödyntäen ja yhden haastattelun osalta kasvokkain samassa neuvottelutilassa. Haastattelut kestivät puolestatoista tunnista kahteen tuntiin. Teemahaastattelut sisälsivät alustuksen, menetelmäosuuden ja palautteen keräämisen haastateltavilta palautekeskusteluna. Alustuksen kautta annettiin haastateltaville henkilöille perustiedot siitä, mitä haastattelussa tehdään ja miksi näin toimitaan. Alustus ennen varsinaisen arviointityön käynnistymistä todettiin tarpeelliseksi koska pohja-aineistoksi lähetetty tietoisku koettiin haastateltavien näkökulmasta riittämättömäksi.

5.1 Tiedon menetelmälomake ja tietotyyppien luokittelun aputaulukko

Tiedon menetelmälomake rakentui Simin (2017) pro gradu -tutkielmassa käytetyn lomakemallin pohjalta. Menetelmälomake muodostettiin havainnoimalla hätäkeskustietojärjestelmää. Havainnointi kohdistettiin työkaluun, jonka kautta hätäkeskustietojärjestelmän tietoaaineisto syötetään järjestelmän käyttöön. Hätäkeskustietojärjestelmän työkaluja analysoitiin havainnoinnin yhteydessä kaikkiaan 87 kappaletta. Työkaluista valittiin tämän opinnäytetyön menetelmälomakkeelle mukaan 54 eri tietotyyppiä. Työkalut, jotka jätettiin valitsematta, olivat sen kaltaisia, että ne joko liittyivät kiinteästi toiseen tietotyyppiin, tai olivat itsenäistä tietoaaineistoa sisältämättömiä työkaluja. Tietotyyppien nimet pelkistetään tässä opinnäytetyössä tuloksien arvioinnin yhteydessä tiedon kasautumisesta johtuen salassapitoon ja turvaluokitukseen viitaten nimille: Tietotyyppi 1, Tietotyyppi 2, Tietotyyppi n ja niin edelleen. Tietotyypin nimiä voidaan yksittäisesimerkkeinä nostaa kuvaamaan tuloksia konkreettisemmän esimerkin havainnollistamiseksi.

Toisen teemahaastattelun aikana havaittiin, että on tarpeen nostaa hätäkeskustietojärjestelmän työkaluista kolme uutta tietotyyppiä arvioitavaksi menetelmälomakkeelle. Tietotyypit nostettiin mukaan pelastustoimen teemahaastatteluun ja tältä osin menetelmälomaketta täydennettiin. Kolmannen haastattelun yhteydessä todettiin, että on tarve nostaa vielä yksi työkalu tietotyyppinä mukaan arvioitavaksi. Näin menetelmälomake täydentyi opinnäytetyön kannalta lopulliseen muotoonsa, sisältäen 58 eri arvioitavaa tietotyyppiä. Kolmannessa ja neljännessä teemahaastattelussa arviointi suoritettiin opinnäytetyön näkökulmasta lopullisella menetelmälomakkeella. Taulukossa 3 on esitetty tietotyyppien lukumäärän iteroituminen alkuperäisestä 54 kappaleesta lopulliseen 58 kappaleeseen. Taulukko 3 sisältää myös haastattelujärjestyksen sekä tietotyyppien luokittelun viranomaisittain.

Lomakkeet ja tapa toimi hyvin näin. Hiukan minua jäi pohdituttamaan, pysyikö meillä sama katsontakanta asiaan samanlaisena vai muovautuiko katsontakanta

palaverin aikaan. Onko tarvetta uudelleen arvioinnille? (Hätäkeskuslaitoksen haastateltava 1.)

Tässä alkoi omastakin mielestä olla järkeä (poliisin haastateltava 1).

Tietotyyppi	Poliisi			Pelastus			Ensihoito			Hätäkeskuslaitos		
	L	S	E	L	S	E	L	S	E	L	S	E
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N	N	M
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	K	K	K
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	K	K	K
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	K	K	K
5	N	K	K	M	N	M	M	K	K	N	N	N
6	M	M	M	N/A	N/A	N/A	M	M	M	N/A	N/A	N/A
7	M	M	M	M	M	M	M	M	M	M	M	M
8	N	K	K	N/A	N/A	N/A	M	M	N	M	M	M
9	M	M	M	M	N	M	N/A	N/A	N/A	M	M	M
10	M	M	M	N/A	N/A	N/A	N/A	N/A	N/A	M	M	M
11	N	N	N	M	N	M	M	K	K	N	K	K
12	N	K	K	N	K	N	K	K	K	K	N	N
13	N	K	K	M	N	M	N	K	K	K	K	K
14	N	K	K	N	K	N	N	K	K	K	K	K
15	M	N	N	M	N	M	N	N	N	N	N	N
16	N	K	K	K	N	N	K	M	M	M	M	M
17	N	N	N	N	M	M	K	K	K	K	K	K
18	K	N	K	N	M	N	K	M	K	K	N	N
19	K	N	K	N	M	M	K	M	K	N	M	N
20	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N	N
21	M	M	M	N	M	M	K	M	N	M	M	N
22	M	M	M	M	K	N	N/A	N/A	N/A	N	N	N
23	N	N	N	M	K	N	M	K	K	N	N	N
24	K	K	K	M	K	N	M	K	K	N	N	N
25	M	M	M	M	K	N	N/A	N/A	N/A	N	N	N
26	K	N	N	M	M	M	N/A	N/A	N/A	K	M	N
27	N	N	N	M	K	N	M	K	K	N	M	N
28	K	K	K	M	K	N	N	K	K	N	N	N
29	M	M	M	M	M	M	N/A	N/A	N/A	M	M	M
30	K	K	K	M	K	N	M	K	K	N	N	N
31	M	N	N	M	K	N	M	K	K	N	K	K
32	M	K	K	M	M	M	M	M	M	M	M	M
33	M	M	M	M	M	M	N/A	N/A	N/A	M	M	M
34	K	K	K	N	K	N	K	K	K	K	K	K
35	N	K	K	M	K	N	M	K	N	N	K	N
36	N	K	K	M	K	N	M	K	K	N	N	N
37	M	N	N	N/A	N/A	N/A	N/A	N/A	N/A	K	K	K
38	M	N	N	N/A	N/A	N/A	N/A	N/A	N/A	N	N	N
39	N	K	K	M	K	N	N	K	K	N	N	N
40	K	K	K	M	N	N	N	K	K	N	N	N
41	K	K	K	M	M	M	N/A	N/A	N/A	M	M	M
42	K	N	N	N/A	N/A	N/A	N/A	N/A	N/A	K	M	N
43	K	K	K	N	K	K	K	K	K	K	N	K
44	K	K	K	M	K	K	N	K	K	N	N	N
45	K	K	K	M	N	M	N	K	K	N	N	N
46	M	N	N	M	M	M	N	K	K	M	M	N
47	N/A	N/A	N/A	M	K	N	N/A	N/A	N/A	M	M	M
48	N/A	N/A	N/A	N	N	N	N/A	N/A	N/A	N	N	N
49	N/A	N/A	N/A	M	N	N	N	K	K	M	M	M
50	M	K	K	M	N	M	N	K	K	N	N	N
51	K	K	K	N	K	K	K	K	K	K	K	K
52	K	K	K	M	N	N	N	K	K	K	K	K
53	N	K	K	M	M	M	M	M	M	M	M	M
54	K	K	K	N	K	N	K	K	K	K	K	K
55				N	N	M	K	K	K	N	N	N
56				N	N	N	N	N	N	K	N	N
57				N/A	N/A	N/A	N/A	N/A	N/A	N	K	K
58				N/A	N/A	N/A	N	K	N	N	N	N

Taulukko 3: Haastattelut ja tietotyyppien luokittelu

Tietotyyppien luokittelun aputaulukko (liite 2) laadittiin ennen teemahaastatteluja. Teemahaastattelujen yhteydessä nousi keskusteluun sen sisällön päivittäminen. Päivittämisen osalta

esimerkkeinä nostettiin, että aputaulukosta pitäisi ilmetä selkeämmin ja tarkemmin, mitä tarkoitetaan. Toisaalta osa haastateltavista oli sitä mieltä, että liitteen 2 aputaulukon tulisi olla viranomaiskohtainen. Viranomaiskohtaisuudella olisi mahdollista saavuttaa parempi ja tasalaatuisempi tuki viranomaiselle. Tietotyyppien luokittelun aputaulukkoa, liite 2, ei päivitetty teemahaastattelujen aikana tasalaatuisen arvioinnin turvaamiseksi. Aputaulukon osalta päivittämisen tarve kuitenkin tunnistettiin.

Tämä on tehokas tapa ja malli arvioida kokonaisuutta. Tämä edesauttaa toimialaa ymmärtämään tiedon tärkeyden ja eheyden merkityksen (ensihoidon haastateltava 1).

Lukuohjeistusta eli luokittelun aputaulukkoa pitää parantaa, että kuvaa konkreettisemmin mitä haetaan (pelastustoimen haastateltava 3).

5.2 Luottamuksellisuuden arviointi

Tiedon turvaluokittelu nousi voimakkaasti esille teemahaastatteluissa luottamuksellisuuden arvioinnin yhteydessä. Koettiin, että luottamuksellisuuden arviointi oli hyvin lähellä tiedon turvaluokittelua ja tämä osaltaan ohjasi haastateltavien ajatuksia. Teemahaastattelun aikana haastateltavien ajatusnäkökulma muuttui kaikissa haastattelutilaisuuksissa turvaluokittelun arvioinnista luottamuksellisuuden arvioinnin suuntaan.

Turvaluokittelu sekoitti kokonaisuutta. Koko ajan meinasi peilata turvaluokitteluun (poliisin haastateltava 1).

Kuntasektorin toimijat eivät ole tutustuneet niin syvällisesti tietoaaineiston turvaluokitteluun ja luokitteluperusteisiin kuin valtionsektorin toimijat. On luonnollista, että tullaan siis hiukan takamatkalta luokittelun osalta. (pelastustoimen haastateltava 3.)

Taulukon 4 mukaan tietotyyppien luottamuksellisuus luokiteltiin korkeaksi useimmiten poliisin ja hätäkeskuslaitoksen tietoaaineistojen osalta. Taulukon 4 mukaan ensihoidon arvio tietotyyppien luottamuksellisuudesta korkeaan luokkaan oli hyvin samalla tasolla kokonaisuuteen nähden kuin Hätäkeskuslaitoksella ja poliisilla. Pelastustoimi taas arvioi luokittelunsa pohjaksi, että heillä ei käytännössä ole korkeaksi luokiteltavaa tietoaaineistoa. Poliisin, Hätäkeskuslaitoksen ja ensihoidon haastatteluissa nousi voimakkaasti esille tarve suojata tiedon luottamuksellisuutta teknisten ja taktisten toimintamallien osalta. Pelastustoimi ei kokenut vastaavaa tarvetta tietoaaineistojen näkökulmasta niin kriittisenä kuin muut toimijat.

Luottamuksellisuus	Korkea	Normaali	Matala	N/A
Poliisi	16	14	16	8
Pelastustoimi	1	13	31	12
Ensihoito	11	14	14	19
Hätäkeskuslaitos	17	26	14	1

Taulukko 4: Koonti luottamuksellisuuden näkökulmasta

5.3 Saatavuuden arviointi

Saatavuuden arvioinnin näkökulmasta poliisi ja ensihoito arvioivat hätäkeskustietojärjestelmän tietotyyppien saatavuuden tarpeen erittäin merkittäväksi (taulukko 5). Hätäkeskuslaitos ja pelastustoimi arvioivat tietotyyppien saatavuuden tarpeen merkittäväksi (taulukko 5). Saatavuuden osalta eniten epätietoisuutta haastatteluihin osallistuvilla aiheutti kysymys tietokantarelaatioiden toiminnasta. Kaikille oli epäselvää, millainen merkitys tiedon kytkeytymisellä toiseen tietoon on. Jos esimerkiksi kytkeytyvä tieto ei olisi saatavilla, miten käy toiselle tietotyyppille tässä tapauksessa?

Miten järjestelmän oliot kytkeytyvät toisiinsa ja miten toimii, jos esimerkiksi laittaa arkistoiduksi. Asiaa pitää selvittää yhdessä järjestelmätoimittajan kanssa. Löytyykö rakenteellisia heikkouksia. Toimiiko samalla tavalla läpi järjestelmän vai eroaako koodi olioiden välillä? Miten toimii, jos lennosta tapetaan, mitä tapahtuu vai ei mitään. Istunnon lopetuksen vaikutus? (Hätäkeskuslaitoksen haastateltava 2.)

Riippuvuudet aiheuttivat haasteita koska tietomalli ei ole niin tuttu (pelastustoimen haastateltava 1).

Hätäkeskustietojärjestelmä on toimijoiden näkökulmasta kriittinen järjestelmä. Saatavuuden arvo nousee merkittäväksi, koska viranomaisten tulee kyetä toimimaan kaikissa tilanteissa. Jos tiedot eivät ole saatavuuden näkökulmasta turvattuja, voi kaikkien viranomaisten toiminta vaarantua ja se saattaa aiheuttaa epäsuotuisat olosuhteet avun tarvitsijalle. Pahimmassa tapauksessa avun tarvitsijan henki, terveys tai omaisuus voi vaarantua.

Saatavuus	Korkea	Normaali	Matala	N/A
Poliisi	24	13	9	8
Pelastustoimi	19	14	12	12
Ensihoito	28	2	9	19
Hätäkeskuslaitos	15	22	20	1

Taulukko 5: Koonti saatavuuden näkökulmasta

5.4 Eheyden arviointi

Tiedon eheyden arvioinnin osalta koettiin samankaltaista epätietoisuutta haastatteluihin osallistuvien kesken siitä, mikä on tietokantarelaatioiden vaikutus kokonaisuuteen. Eheyden arvioinnissa pohdittiin lukuisia kertoja tietoaineiston riippuvuutta toiseen tietoaineistoon. Miten eheys toteutuu tilanteissa, joissa tietotyyppiin kytkeytyvä tieto korruptoituu, tuhoutuu tai muutoin vahingoittuu jonkin tapahtuman seurauksena?

Miten järjestelmä toimii tässä tiedon eheyden osalta? Pitää selvittää järjestelmän tekijöiltä riippuvuuksien toiminta (pelastustoimen haastateltava 3).

Eheyden arvioinnin osalta poliisi ja ensihoito pitävät tietotyyppien eheyttä erittäin merkittävänä asiana hätäkeskustietojärjestelmän toiminnan kannalta (taulukko 6). Poliisi ja ensihoito perustelivat haastatteluissa itselleen asiaa toiminnan organisoitumisen kautta. Jollei tietoaineistot tietotyyppien sisällä ole eheitä, ei viranomaistoiminta voi toteutua. Hätäkeskuslaitoksen osalta kriittisen tärkeitä korkean eheyden omaavia tietotyyppijä taas oli sen toiminnalle tärkeä puhelintoiminnallisuuksien, hätäilmoitusten arviointilomakkeiden ja viranomaisten hälytysuunnitelmien eheys. Pelastustoimen lähtökulma tiedon eheyden arviointiin oli se, että jos tiedon eheydessä on ongelmaa, riittää kunhan tieto saadaan toimivaltaisen viranomaisen käyttöön. Tällöin pelastustoimi voi itse huolehtia muilla keinoin toiminnan organisoimisen ja sen toteuttamisen. Pelastustoimelle hälytysuunnitelmat olivat erityisen tärkeä tietoaineisto, jolle oli erityisen korkean eheyden tarve. Myös muille haastateltaville hälytysuunnitelmien kokonaisuus oli tärkeäksi tietotyyppiksi luokiteltu tietoaineisto.

Eheys	Korkea	Normaali	Matala	N/A
Poliisi	26	11	9	8
Pelastustoimi	3	23	19	12
Ensihoito	28	6	5	19
Hätäkeskuslaitos	15	29	13	1

Taulukko 6: Koonti eheyden näkökulmasta

5.5 Kasautuvuuden arviointi

Hätäkeskustietojärjestelmän toiminnot kytkeytyvät monilta osin toisiinsa, jotta eheä kokonaisuus saavutetaan. Tämä toimintojen kokonaisuus näkyy tiedon kasautuvuudessa. Tietoaineistoa kasautuu kohtuullisen paljon, mikä takaa sen, että järjestelmäominaisuuksia varten saadaan riittävät tiedot kytkettyä toisiinsa. Tiedon kasautuvuuden kokonaisuudesta hätäkeskustietojärjestelmässä Hätäkeskuslaitoksella on suurin tiedon kasautuvuus (taulukko 7). Tämä on luonnollista, koska Hätäkeskuslaitoksella on paljon tietotyyppijä, joita muilla viranomaisilla ei järjestelmässä ole käytössä. Tällaisia tietotyyppijä ovat esimerkiksi hätäpuheluiden ohjaamiseen tarvittavat tietoaineistot. Viranomaisten näkökulmasta tieto kasaantuu käytännössä samojen tietotyyppien kautta koska kaikilla on yhtenevät työkalut käytössä.

Kasautuvuus	kpl	N/A	Yhteensä
Poliisi	18	8	54
Pelastustoimi	18	12	57
Ensihoito	17	19	58
Hätäkeskuslaitos	29	1	58

Taulukko 7: Koonti kasautuvuuden näkökulmasta

Tiedon kasaantuvuuden osalta teemahaastatteluissa nousi esille se, että kasaantuvuudella kokonaisuudessaan ei ole merkittävää vaikutusta tiedon luottamuksellisuuden, saatavuuden tai eheyden luokittelun näkökulmasta. Teemahaastattelussa todettiin, että tietotyypin luonne on enemmän määräävä tekijä arvioitaessa luottamuksellisuutta, saatavuutta tai eheyttä. Tiedon kasaantuvuudella ei ole myöskään vaikutusta siihen, pitääkö tietosisältö henkilötietoja sisältää vai ei.

Kasaantuvuuden ja henkilötiedon vaikutus ei juurikaan ollut arvioinnissa korotavana tekijänä (Hätäkeskuslaitoksen haastateltava 1).

5.6 Henkilötiedon arviointi

Hätäkeskustietojärjestelmä on henkilörekisteri ja siten sisältää henkilötietoja. Tässä opinnäytetyössä arvioitiin järjestelmään syötettävien tietotyyppien näkökulmasta sitä, sisältääkö tietotyyppi henkilötietoja. Hätäkeskustietojärjestelmän tietoaaineistoissa henkilötietoja on tyypillisesti puhelinnumeroissa, joita käytetään erilaisten kohteiden tai asiantuntijoiden tai vastaavien tavoittamiseksi. Lisäksi henkilötietoja on luonnollisesti tehtäviä suorittavien partioiden henkilöstössä tai tehtävädokumentaation osana erilaisissa raporteissa.

Taulukosta 8 voidaan todeta, kuinka monessa tietotyyppissä tallennetaan tietoaaineiston osana henkilötietoja. Luku on esitetty viranomaisittain. Taulukosta 8 nähdään, että viranomaisittain tietoaaineistossa on melko paljon eroa. Ensihoito tallentaa järjestelmään huomattavasti vähemmän henkilötietoja tietotyyppien lukumääräisestä näkökulmasta arvioiden kuin esimerkiksi pelastustoimi tai Hätäkeskuslaitos. Poliisin käytössä olevien tietotyyppien osalta kappalemääräinen lukumäärä asettuu muiden viranomaisten väliin.

Henkilötieto	kpl	N/A	Yhteensä
Poliisi	9	8	54
Pelastustoimi	14	12	57
Ensihoito	6	19	58
Hätäkeskuslaitos	14	1	58

Taulukko 8: Koonti henkilötietojen näkökulmasta

6 Pohdinta

Opinnäytetyön tekeminen on ollut kirjoittajalle merkittävä oppimisprosessi. Sen koostaminen tutkimussuunnitelmasta tähän kokonaisuuteen on ollut oivallusten matka. Olen oppinut erittäin paljon tieteellisen tutkimuksen tekemisestä, sen prosessista ja erilaisista menetelmistä. Olen onnistunut hakemaan tietoperustaa ja työtä varten erilaista aineistoa. Olen saanut pohdittua menetelmät juuri tätä työtä varten. Olen pystynyt toteuttamaan jotakin aitoa, uutta ja merkityksellistä koko viraston hyödyksi tietojen luokittelun mallin muodossa. Haluan väittää, että henkilöt, jotka ovat osallistuneet tämän työn tekemiseen, ovat myös oppineet jotain uutta. Työn valmistuminen saa aikaan hyvän olon tunteen, omasta mielestä ansaitun sellaisen.

Työn aikana opinnäytetyön prosessin kokonaisuus on avautunut. Aiempien opintojen pohjalta en ollut kyennyt hahmottamaan kokonaisuuden monimuotoisuutta. Työtä tehdessä moni asia on avautunut aivan uudella tavalla. Olen oivaltanut mitä menetelmät ja analyysitavat tarkoittavat, mikä on tietoperusta ja monta muuta asiaa. Tämän opinnäytetyön kautta koen, että kirjoittajana olen kasvanut hyvin paljon. Voin rehellisesti sanoa, että olen oppinut paljon erilaisia asioita.

Opinnäytetyössä on onnistuttu kehittämään hätäkeskustietojärjestelmän tietojen luokittelun malli. Tässä luvussa esitellään opinnäytetyön luotettavuutta ja eettisyyttä koskeva arvio. Opinnäytetyön keskeiset tulokset koostetaan tämän luvun alle. Opinnäytetyö päättyy sen johdopäätösten ja kehitysehdotusten kuvaukseen ja arviointiin.

6.1 Opinnäytetyön luotettavuus ja eettisyys

Tutkimuseettisen neuvottelukunnan ohjeessa hyvä tieteellinen käytäntö ja sen loukkausepäilyt Suomessa käsitellään hyvän tieteellisen käytännön ohjeistuksia. Ohjeen keskeisiä lähtökohtia ovat esimerkiksi se, että noudatetaan rehellisyyden lisäksi yleistä huolellisuutta ja tarkkuutta tutkimustyössä ja tulosten arvioinnissa. Neuvottelukunnan ohjeeseen on kirjattu, että ”tutkimukseen sovelletaan tieteellisen tutkimuksen kriteerien mukaisia ja eettisesti kestäviä tiedonhankinta-, tutkimus- ja arviointimenetelmiä”. (Tutkimustieteellinen neuvottelukunta 2012.)

Opinnäytetyö halutaan toteuttaa objektiivisesti. Opinnäytetyön perustuu voimassa olevaan lainsäädäntöön ja tekijän henkilökohtaiset asenteet tai mielipiteet eivät saa ohjata opinnäytetyön kulkua. Opinnäytetyön luotettavuutta lisää se, että opinnäytetyölle saadaan viraston tuki. Opinnäytetyössä on selkeä toimeksiantaja, jonka kanssa opinnäytetyön tulokset voidaan käydä läpi ja siten pystytään saamaan objektiivinen arvio opinnäytetyön luotettavuudesta.

Yleistä opinnäytetyön luotettavuutta tukee hyvin se, että kaikki henkilöt, joiden kanssa opinnäytetyö toteutetaan tai joita haastatellaan opinnäytetyötä varten ovat ammattilaisia

virkatyössään. Toimin virkatyössäni hätäkeskustietojärjestelmän pääkäyttäjänä. Asiantuntijat, joita opinnäytetyössä hyödynnetään, edustavat viranomaisten vastaavaa pääkäyttöä tai Hätäkeskuslaitoksen asiantuntijoita hätäkeskustietojärjestelmän ympärillä. Henkilöillä on käytännössä pitkä kokemus järjestelmän rakentamisesta, kehittämisestä ja ylläpidosta. Haastattelut toteutetaan opinnäytetyön kannalta anonyymisti. Ne kuitenkin raportoidaan toimeksiantajalle laadittavan raportin yhteydessä.

Lähdeaineiston osalta todetaan, että se on luotettavaa. Opinnäytetyöhön liittyvä tietoperusta ja viittaukset perustuvat voimassa olevaan lainsäädäntöön. Myös muuta lähdeaineistoa käytetään ja tällöin noudatetaan asianmukaisia lähdeviittauksia. Opinnäytetyön uskottavuutta lisää se, että lähdeviittaukset toteutetaan oikein ja eettisesti. Lähdeviittauksilla kunnioitetaan tiedon kirjoittajaa ja toisaalta mahdollistetaan lukijalle se, että hän voi tarkistaa alkuperäisen kirjauksen. Luotettavuus ja eettisyys ovat toisaalta eri käsitteitä, toisaalta toisiinsa kietoutuneita käsitteitä.

Tutkimusmetodien osalta on noudatettu eettisiä arvoja siitä, kuinka käsitellään yhteistyökumppaneita tai esimerkiksi haastateltavia. Haastattelut on sovittu hyvissä ajoin ja haastattelujen sisältö selvitetään haastateltaville ennalta. Haastattelut pohjautuvat vapaaehtoisuuteen ja haastateltaville on selvitetty, mitä haastattelusta tallennetaan ja miten. Haastatteluista ei muodosteta tallenteita videoiden, nauhurien tai vastaavien kautta. Haastattelijan käsin paperille tai menetelmälomakkeelle toteutetut merkinnät edustavat haastattelujen tallenteita. Haastateltavien anonymiteetti säilytetään opinnäytetyön osalta. Opinnäytetyön tulokset raportoidaan Hätäkeskuslaitokselle. Hätäkeskuslaitokselle toteutetaan tietojen luokittelun raportointi. Tässä yhteydessä tilaisuuksiin osallistunut henkilö kirjataan luokittelun raporttiin.

Reliabiliteetin näkökulmasta haluan, että tutkimus on luotettava ja toistettava. Reliabiliteetin näkökulmasta opinnäytetyö, havainnot ja menetelmät kuvataan niin tarkasti, että tutkimus on toistettavissa. Tutkimus on toistettavissa toisen henkilön toimin.

6.2 Keskeisten tulosten tarkastelu

Tiedon luokittelun kehittämisessä onnistuttiin hätäkeskustietojärjestelmän osalta. Tietotyyppien määrittäminen tietoaaineistopohjaisesti hätäkeskustietojärjestelmän työkalujen kautta oli opinnäytetyön kannalta toimiva ratkaisu. Haastateltavien mielestä tietotyypit olivat konkreettisia ja aineiston ylläpidon kautta tuttuja. Haastateltavat totesivat, että luokittelun yhteydessä käytiin läpi koko viranomaisen tietoaaineisto erilaisista näkökulmista. Nämä näkökulmat herättivät haastatteluissa paljon viranomaisen sisäistä keskustelua. Tällaisena nostona esimerkiksi se, että onko tieto tällä hetkellä syötettynä optimaalisimmalla tavalla järjestelmään nykytiedon valossa vai pitäisikö tietoaaineiston muotoa muuttaa johonkin suuntaan. Toisaalta keskusteltiin, ovatko kaikki tietoaaineistot ylipäättään tarpeellisia viranomaisen toiminnan

kannalta vai pitäisikö toimintoja muuttaa toiseen suuntaan järjestelmän sisäisesti. Haastateltavien kommentit tietoaineiston läpikäynnistä vahvistivat tätä keskeistä opinnäytetyön tulosta.

Arvioitiin mitä tietoa meillä on, kuinka kriittistä se on meille, onko sisällössä jotain turhaa? Lisäksi aineistojen läpikäynti osoitti, kuinka merkittävää on se, että käyttöoikeudet kriittisiin toimiin on riittävän pienellä porukalla. (Ensihoidon haastateltava 1.)

Avartava ja hyvä katsaus asiaan. Tuli toteutettua syvälinen kertaus portal-toimintoihin (ensihoidon haastateltava 2).

Tässä työkalussa on hyvä malli yksittäisten tietojärjestelmien tietoelementtien tarkastukseen ja luokitteluun (pelastustoimen haastateltava 3).

Teemahaastatteluista saatiin menetelmän osalta palautetta. Tiedon luokittelun menetelmä koettiin mielekkääksi tavaksi käsitellä suuria tietoaineistoja hätäkeskustietojärjestelmän osalta. Haastattelutilaisuuksien aikana nousi esille, että tämänkaltainen tiedon analysointi eri näkökulmista tuli tarpeeseen. Arviointi sai haastateltavan pohtimaan tietoturvaerilaisista, osin uusistakin näkökulmista. Tiedon luottamuksellisuuden, saatavuuden, eheyden, tietotyyppien sisältämän henkilötiedon ja tiedon kasaantuvuuden arviointi oli uusi näkökulma tiedon ylläpitoon, ylläpidon kehittämiseen ja tietoturvan parantamiseen. Haastateltavien kommentit pyydettyä palautetta olivat käytetyn menetelmän osalta yksimielisiä. Yhteinen arvio oli se, että menetelmästä saadaan hyötyä ja se parantaa tiedonhallintaa.

Soveltuu tietojen luokitukseen. Selkeästi paneuduttu asiaan (ensihoidon haastateltava 1).

Tehokas tapa / Malli. Malli edesauttaa toimialaa ymmärtämään tiedon tärkeyden ja eheyden merkityksen (ensihoidon haastateltava 2).

Ok, työmenetelmä soveltuu tietojen luokitteluun (poliisin haastateltava 2).

Lomakkeet ja tapa toimi hyvin näin (Hätäkeskuslaitoksen haastateltava 1).

6.3 Johtopäätökset ja kehitysehdotukset

Hätäkeskustietojärjestelmän tietojen luokittelun ensimmäinen arviointikierros on toteutettu. Keskeisenä johtopäätöksenä voidaan todeta, että malli on toimiva. Hätäkeskuslaitoksen velvoittama hätäkeskustietojärjestelmän tietojen luokittelun vuosittainen arviointi ja tulosten raportointi voidaan toteuttaa tässä opinnäytetyössä laadittua menetelmää hyödyntäen. Mallin käyttäminen vuosittaisen raportoinnin pohjadata kerääjänä on yksinkertaisuudessaan tehokas vaihtoehto. Tapa ei vaadi viranomaisittain erityisen suurta työmäärää ja silti tulokset saadaan käyttöön tiedon luokittelun raporttia varten.

Hätäkeskustietojärjestelmän tietojen luokittelu ja arviointi raportoidaan tämän työn pohjalta Hätäkeskuslaitokselle. Opinnäytetyön tuotos siirretään suoraan käytäntöön.

Hätäkeskuslaitoksen pääkäyttöyksikölle velvoitettu virkatyö toteutetaan tämän opinnäytetyön mallia ja tuloksia hyödyntäen. Opinnäytetyön aikana kerätty materiaali hyödynnetään täysin vuoden 2022 raportin sisällön aineistona. Raportin koostaminen on ajankohtainen syksyllä 2022.

Hätäkeskustietojärjestelmän tietojen luokittelu vaatii jatkokehitystä. Opinnäytetyössä nousi esille keskeisenä johtopäätöksenä, että tieto kannattaa luokitella hätäkeskustietojärjestelmässä viranomaisittain. Tällä varmistutaan siitä, että toisen viranomaisen tietoaaineistojen luokitusarvoa ei pakoteta samaan muottiin tarpeettomasti. Haastattelujen johtopäätöksenä on, että toiselle tietotyyppi voi olla tärkeä mutta toiselle viranomaiselle sama tietotyyppi voi olla tärkeydeltään matala tai jopa merkityksetön. Kehitysehdotuksena esitetään, että opinnäytetyössä haastateltujen viranomaisten kanssa pidetään yhteinen palaveri tiedon luokittelun pelisääntöjen ympärillä. Pelisääntökeskustelun keskiössä on ratkaisu, luokitellaanko tiedot yhteisesti vai tekeekö kukin viranomainen sen omana luokittelunaan. Opinnäytetyön tulosten pohjalta johtopäätöksenä ja ehdotuksena on, että kukin viranomainen jatkaa omalla arvioinnillaan.

Menetelmälomake koettiin haastatteluissa selkeäksi ja toimivaksi. Menetelmälomakkeen kautta hätäkeskustietojärjestelmän tietotyyppien tietojen luokittelu voidaan toteuttaa tavalla, jolla viranomainen selkeästi pystyy arvioimaan konkreettisia ja itselleen tuttuja asioita. Tämä mahdollistaa sen, että viranomainen voi koko ajan pitää itseään tietojen luokittelun keskiössä omasta näkökulmastaan. Hätäkeskuslaitoksen toimiessa hätäkeskustietojärjestelmän tietojen luokittelun isäntänä, voidaan keskustelua ohjata yhtenäiseen suuntaan viranomaisten välillä. Kun keskustelua ohjataan yhteiseen suuntaan, koko hätäkeskustietojärjestelmän tietoaaineistoja kyetään kehitysehdotuksena eheyttämään. Hätäkeskustietojärjestelmään toteutettavien uusien ominaisuuksien mukainen tietoaaineisto on helpolla tavalla otettavissa mukaan osaksi tätä tiedon luokittelun menetelmää.

Tietojen luokittelun aputaulukkoa tulee kehittää. Haastatteluissa nousi voimakkaasti esille, että tietojen luokittelun aputaulukko vaatii yhteistä määrittelyä. Aputaulukon sisältö on laadittu tätä opinnäytetyötä varten ja sen muuttaminen yhteisesti on tarkoituksenmukaista. Aputaulukon sisältöä on pyydetty muuttamaan tarkemmaksi ja konkreettisemmaksi. Myös toivetta siihen, että aputaulukosta voitaisiin laatia toimialakohtaiset versiot, on esitetty. Johtopäätöksenä todetaan, että tietojen luokittelun aputaulukon kehittäminen kannattaa toteuttaa yhdessä viranomaisten kanssa.

Tietojen luokittelu mallipohjaa hyödyntämällä ja tietojen luokittelun raportti parantaa tietosuojaa siten, että rekisterinpitäjä voi näiden kautta muodostaa tietosuojan osoitusvelvollisuuden asiakokonaisuuden ympäriltä. Raportin kautta rekisterinpitäjä näkee samalla hätäkeskustietojärjestelmän tietojen luokittelun kokonaisuuden sekä luokitteluperusteet. Tiedon

luokittelun kautta rekisterinpitäjällä on viranomaisittain tiedossa kaikki ne tietoaaineistot, joissa viranomaisella on ilmoittanut käyttävänsä henkilötietoja. Tämän pohjalta rekisterinpitäjällä on mahdollisuus arvioida tarpeellisia valvonta- tai tarkastustoimia tietoaaineistolle tai sen käsittelylle.

Kehitysehdotuksena nostetaan esille se, että selvitetään järjestelmätoimittajalta tarkasti se, miten kytkeytyvä tieto eri tietotyyppien osalta käyttäytyy. Tällä tiedolla on suuri merkitys siihen, kuinka tiedon luottamuksellisuutta, saatavuutta ja eheyttä hätäkeskustietojärjestelmässä tulisi arvioida. Asialla on suuri vaikutus siihen, millaisia riskejä kukin tietotyyppi järjestelmälle muodostaa. Opinnäytetyön näkökulmasta tässä nostetaan esille riski lähinnä siitä, kuinka eheästi on onnistuttu tietojen luokittelussa. Hätäkeskuslaitoksen ja viranomaisten näkökulmasta selvittäminen on erityisesti tarpeen, jotta voidaan arvioida nykyisten varamenetelyjen riittävyys ja mahdolliset kehitystarpeet. Johtopäätöksenä on, että toteutettu tiedon luokittelu tulee arvioida uudelleen, kun faktat ovat selvillä. Jos asiasta nousee kehitysehdotuksia järjestelmän kehittämiseksi, tulee suurella todennäköisyydellä tietojen luokittelu toteuttaa uudelleen huomioiden kehityskohteet.

Tietoaaineistojen arvioinnissa todettiin, että poliisi ja Hätäkeskuslaitos valtion viranomaisina käsittelevät tiedon turvaluokittelun näkökulmasta tietoaaineistoja eri tavoin kuin kuntataustainen pelastustoimi. Tämä näkyi erityisesti luottamuksellisuuden arvioinnissa. Poliisilla ja Hätäkeskuslaitoksella on hyvin paljon tietoaaineistoa, joka voi paljastaa taktisia tai teknisiä toimintamalleja, jos tieto pääsee vuotamaan sivulliselle. Riski edellä mainittujen asioiden paljastumiseen ja sen seurauksiin aiheuttaa tiedon luokittelun osalta sen, että luokittelu määritellään tärkeäksi näiden osalta. Selvää on, että järjestelmä itsessään muodostaa Hätäkeskuslaitokselle merkittävän taktisia ja teknisiä toimintamalleja sisältävän ydintoimintaa toteuttavan tietojärjestelmän. Pelastustoimen siirtyminen hyvinvointialueille vuodesta 2023 lukien voi muuttaa tilannetta asian osalta. Tämä näkökulma jää selvitetäväksi kehitysehdotuksena.

Lähteet

Painetut

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2005. Tutki ja kirjoita. 11. painos. Helsinki: Tammi.

Valli, R. & Aaltola, J. 2015a. Ikkunoita tutkimusmetodeihin 1. Metodien valinta ja aineistonkeruu: virikkeitä aloittelevalla tutkijalla. 4. uudistettu ja täydennetty painos. Jyväskylä: PS-kustannus.

Valli, R. & Aaltola, J. 2015b. Ikkunoita tutkimusmetodeihin 2. Näkökulmia aloittelevalla tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. 4. uudistettu painos. Jyväskylä: PS-kustannus.

Sähköiset

Andress, J. 2014. The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice. E-kirja. Waltham: Elsevier.

Bergström, E., Karlsson, F. & Åhlfeldt, R. 2021. Developing an information classification method. Information and computer security, Bingley: Emerald group publishing limited. Viitattu 21.4.2022. <https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2020-0110/full/html>

Diamantopoulou, V., Tsohou, A. & Karyda, M. 2020. From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls. Information and computer security, Bingley: Emerald group publishing limited. Viitattu 21.4.2022. <https://www.emerald.com/insight/content/doi/10.1108/ICS-01-2020-0004/full/html>

EU:n yleinen tietosuojasäädös 2016/679/EU. Viitattu 12.12.2021. <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679>

European commission. 00062/2010/EN, WP 173. Article 29 Data Protection Working Party: Opinion 3/2010 on the principle of accountability. Viitattu 19.4.2022. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

Hätäkeskuslaitos. 2022a. Viitattu 12.4.2021. <https://112.fi/hatakeskusjarjestelma-erica-n-tietosuojaseloste>

Hätäkeskuslaitos. 2022b. Viitattu 12.4.2021. <https://112.fi/juhlavuosihiistoria>

Jamk 2022. Opinnäytetyön ohjaajan käsikirja. Viitattu 30.3.2022. <https://oppimateriaalit.jamk.fi/yamk-kasikirja/kirjallisuuskatsaukset/>

Laki hätäkeskustoiminnasta 692/2010. Viitattu 12.12.2021. <https://www.finlex.fi/fi/laki/ajantasa/2010/20100692 - L4P16>

Laki julkisen hallinnon tiedonhallinnasta 906/2019. Viitattu 12.12.2021. <https://www.finlex.fi/fi/laki/alkup/2019/20190906>

Nykänen, T. 2016. Tiedon luokittelu suojaustarpeiden määrittämiseksi organisaatiossa. Ylempi AMK-opinnäytetyö. Laurea-ammattikorkeakoulu. Espoo. Viitattu 30.3.2022.

https://www.theseus.fi/bitstream/handle/10024/108542/Nykanen_Teemu.pdf?sequence=1

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. E-kirja. 3.–4. painos. Helsinki: Sanoma Pro.

Puusa, A., Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. E-kirja. Helsinki: Gaudeamus.

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyypeihin ja hallintotieteellisiin sovelluksiin. Vaasan Yliopisto. Viitattu 30.3.2022. https://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Sanastokeskus. 2021. TEPA-termipankki. Viitattu 12.12.2021. <https://termipankki.fi/tepa/fi/haku/tietoturva>

SFS-EN 27002. 2017. SFS-EN ISO/IEC 27002:2017 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Viitattu 12.12.2021. <https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/493421.html.stx>

Simi, J. 2017. Tiedon luokittelu osana organisaation kokonaisarkkitehtuurin riskienhallintaprosessia. Pro gradu -tutkielma. Jyväskylän yliopisto, tietojenkäsittelytieteiden laitos. Jyväskylä. Viitattu 30.3.2022. <https://jyx.jyu.fi/bitstream/handle/123456789/52765/URN%3aNBN%3afi%3ajyu-201701191200.pdf?sequence=1&isAllowed=y>

Tietosuojalaki 1050/2018. Viitattu 12.12.2021. <https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>

Tietosuojavaltuutetun toimisto. 2022. Viitattu 7.3.2022. <https://tietosuoja.fi/tietosuoja>

Tutkimustieteellinen neuvottelukunta. 2012. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Viitattu 30.5.2022. https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf

Vainio, A. 2018. Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa. Pro gradu -tutkielma. Helsingin yliopisto, oikeustieteellinen tiedekunta. Helsinki. Viitattu 19.4.2022. https://helda.helsinki.fi/bitstream/handle/10138/232856/Vainio_Sonja_pro_gradu_Rekisterinpit%c3%a4j%c3%a4n_osoitusvelvollisuus_EUn_yleisess%c3%a4_tietosuoja-asetuksessa.pdf?sequence=2&isAllowed=y

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019. Viitattu 12.12.2021. <https://finlex.fi/fi/laki/alkup/2019/20191101>

Valtiovarainministeriö. 2006. VAHTI 5/2006: Asianhallinnan tietoturvaluokittelusta koskeva ohje. Viitattu 20.4.2022. https://www.suomidigi.fi/sites/default/files/2020-06/main-book_5_2006.pdf

Valtiovarainministeriö. 2008. VAHTI 8/2008: Valtiohallinnon tietoturvasanasto. Viitattu 20.4.2022. https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_8_2008.pdf

Valtiovarainministeriö. 2010. VAHTI 2/2010: Ohje tietoturvaluokittelusta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Viitattu 20.4.2022. https://www.suomidigi.fi/sites/default/files/2020-06/pdf_2_2010.pdf

Valtiovarainministeriö. 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Viitattu 16.3.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162649/VM_2021_5.pdf?sequence=1&isAllowed=y

Vilkka, H. 2021. Näin onnistut opinnäytetyössä. Ratkaisut tutkimuksen umpikujaan. E-kirja. Jyväskylä: PS-kustannus.

Julkaisemattomat

Hätäkeskuslaitos. 2018a. HAK; Hätäkeskuslaitoksen päätös yhteiskäyttöisen hätäkeskustietojärjestelmän (ERICA) käyttöehdoista. Viitattu 20.4.2022.

Hätäkeskuslaitos. 2018b. HAK; Hätäkeskuslaitoksen päätös yhteiskäyttöisen hätäkeskustietojärjestelmän (ERICA) käyttöoikeuspolitiikasta. Viitattu 20.4.2022.

Hätäkeskuslaitos. 2020. HAK; Päätös toimenpiteistä koskien tietosuojassa havaittuja riskejä; ERICA 2.0.1 vaikutustenarviointi. Viitattu 20.4.2022.

Hätäkeskuslaitos. 2021. HAK; Vuosikellotyöryhmän raportti. Viitattu 20.4.2022.

Kuviot

Kuvio 1: Tietojen luokittelun menetelmä (Simi 2017).....	12
Kuvio 2: Aineistojen tiedon luokittelun prosessi (mukaiillen Bergström ym. 2021, 229).....	13
Kuvio 3: CIA-malli (mukaiillen Andress 2014, 6)	17
Kuvio 4: Tutkimuksellisen kehittämistyön prosessi (Ojasalo ym. 2015, 24)	23
Kuvio 5: Konstruktiivisen tutkimuksen prosessi (Ojasalo ym. 2015, 67)	24

Taulukot

Taulukko 1: Tietotyyppien koodaus värein ja esittäminen taulukossa	28
Taulukko 2: Tiedon koontin esimerkkitaulukko	28
Taulukko 3: Haastattelut ja tietotyyppien luokittelu	30
Taulukko 4: Koonti luottamuksellisuuden näkökulmasta.....	31
Taulukko 5: Koonti saatavuuden näkökulmasta	32
Taulukko 6: Koonti eheyden näkökulmasta	33
Taulukko 7: Koonti kasautuvuuden näkökulmasta	33
Taulukko 8: Koonti henkilötietojen näkökulmasta.....	34

Liitteet

Liite 1: Menetelmälomake.....	45
Liite 2: Tietotyyppien luokittelun aputaulukko	47
Liite 3: Palautekysely	49

Liite 1: Menetelmälomake

Menetelmä toteutettiin lomaketta hyödyntäen. Esimerkki menetelmälomakkeesta löytyy seuraavalta sivulta. Ryhmähaastattelun etenemisjärjestys oli seuraavanlainen:

1. Perustietojen dokumentointi
 - a. Arvioitava järjestelmä
 - b. Käyttötarkoitus
 - c. Tietojärjestelmän käyttäjäorganisaatio
 - d. Tietojärjestelmän käyttäjien lukumäärä organisaatiossa
2. Tietotyyppien tunnistus
 - a. Tunnistetaan tietotyypit
 - b. Luokitellaan tietotyypit
 - c. Huomioidaan tietotyypin sisältämä henkilötieto tai kasautuvuus
3. Kirjataan luokittelun sanallinen arviointi
 - a. Arvioidaan tietotyyppien sisältämä tietoaineisto ja sen ajantasaisuus viranomaisen näkökulmasta.
 - b. Analysoidaan mahdollisten uusien tietotyyppien tarve.
4. Kirjoitetaan johtopäätökset tietotyyppien tietoaineistojen sisällöstä ja viranomaisen kehitysehdotukset tietoturvallisuus- ja tietosuojavaatimusten parantamiseksi

HÄTÄKESKUSTIETOJÄRJESTELMÄN LUOKITTELUMATRIISI (tietoturvallisuus)
1) Dokumentoi tietojärjestelmän perustiedot

Arvioitava järjestelmä: Hätäkeskustietojärjestelmä ERICA, Portal tietojen ylläpitojärjestelmä
 Käyttötarkoitus: Tietoaineiston ylläpitojärjestelmä. Tavoite tuottaa asianmukaisen luottamuksellisuuden ja eheyden sisältämä tietoaineisto käyttöliittymällä käytettäväksi.

Tietojärjestelmän käyttäjäorganisaatio:

Tietojärjestelmän käyttäjien lukumäärä organisaatiossa:

2) Tunnista ja luokittele tietojärjestelmän tietotyypit

Tietotyyppi	L	S	E	HLÖ	KASA
Tietotyyppi 1					
Tietotyyppi 2					
Tietotyyppi 3					
Tietotyyppi 4					
Tietotyyppi n					

3) Luokittelun sanallinen arviointi

Tarkastetaan laadittujen tietotyyppien listaus. Ovatko kaikki tietotyypit tunnistettu?

Arvioidaan tunnistetut tietotyypit.

Kiinnitetään huomio erityisesti niihin tietotyypeihin, jotka ovat korkealla tasolla eheyden tai luottamuksellisuuden osalta tai jotka sisältävät henkilötietoja tai kasautuvuutta.

4) Johtopäätökset tietotyyppien tietoaineistojen sisällöstä ja viranomaisen kehitysehdotukset tietoturvallisuus- ja tietosuojavaatimuksien parantamiseksi

Johtopäätöksiä suunnitellaan erityisesti henkilötietoja sisältävien tietotyyppien ja eheyden näkökulmasta korkean riskin tietotyypeiksi arvioitavien tietotyyppien tarkastusprosessi ja aikataulus tarkastukselle. Tarkastellaan kasautuvuuden vaikutus.

Johtopäätöksiä laaditaan yhdessä viranomaisen kanssa suunnitelma kaikkien tietotyyppien tarkastamisesta soveltuvassa aikataulussa. Suunnittelun perusteina ovat lainsäädäntö, erityisesti tietosuojalainsäädäntö sekä järjestelmän tietoaineiston syötöstä sovitut periaatteet ja ohjeistus. Sovitaan yhteisistä toimintaperiaatteista toimijoiden kesken.

Arvioidaan tarkastustyön resurssitarpeet. Pohditaan, millaisia riskejä tarkastustyöhön liittyy ja miten niihin voidaan vähentää. Arvioidaan toimenpiteiden jälkeiset jäännösriskit.

Päätetään tietoarkkitehtuurin kuvauksesta. Viedään tämän dokumentaation tietosisältö osaksi tietoarkkitehtuurin kuvausta.

Liite 2: Tietotyypin luokittelun aputaulukko

Alla olevaan taulukkoon on koottu luokittelun apuna käytetyt esimerkit.

	Luottamuksellisuus - (L)	Saatavuus - (S)	Eheys - (E)
Korkea (K), esimerkkejä	Tietoaineisto salassa pidettävää - STIII. Paljastuessaan tuottaa riskin viranomaisen taktisen tai teknisen toimintamallin paljastumiselle. Tietoaineisto saattaa paljastaa yrityksen tai liiketalouden ja siten voi paljastuessaan aiheuttaa haittaa yrityksen tai liiketoimintaa harjoittavan tahon toiminnalle, luottamukselle, toiminnan jatkuvuudelle tai maineelle. Tietoaineisto voi olla kasautunutta.	Palvelu käytössä 24/7/365. Tietoluokka on kriittinen toiminnan jatkuvuuden näkökulmasta. Järjestelmä ei toimi ilman tietotyypin tietoaineistoa. Varajärjestelmä on oltava välittömästi saatavilla.	Aiheuttaa merkittävän riskin ihmisen terveydelle, aiheuttaa riskin organisaation päätehtävän jatkuvuudelle tai maineelle tai partioille / yksiköille erittäin vakavan riskin. Häätöilmoituksen vastaanotto tai tehtävän välittäminen viranomaisyksikölle voi häiriintyä. Tietoaineiston nimeämismuodolla on erityistä merkitystä tiedon ylläpidolle.
Normaali (N), esimerkkejä	Tietoaineisto julkista - STIII. Paljastuessaan tuottaa kohtuullisen riskin viranomaisen taktisen tai teknisen toimintamallin paljastumiselle. Tieto saattaa paljastaa yrityksen tai liiketalouden ja siten voi paljastuessaan aiheuttaa haittaa yrityksen tai liiketoimintaa harjoittavan tahon toiminnalle, luottamukselle, toiminnan jatkuvuudelle tai maineelle. Tietoaineisto voi olla kasautunutta.	Palvelu käytössä 24/7/365. Tietoluokka on tärkeä toiminnan jatkuvuuden näkökulmasta. Järjestelmä toimii, mutta ilman tietotyypin tietoaineiston saatavuutta työn toteuttaminen on haastavaa ja järjestelmästä ei saada täyttä hyötyä. Varajärjestelmä parantaa tilannetta, mutta tietoaineiston osalta sen käyttöönotto ei ole aikakriittistä.	Aiheuttaa riskin ihmisen terveydelle, aiheuttaa riskin organisaation päätehtävän jatkuvuudelle tai maineelle tai partioille / yksiköille. Hätöilmoituksen vastaanotto tai tehtävän välittäminen viranomaisyksikölle voi häiriintyä. Tietoaineiston nimeämismuodolla on merkitystä tiedon ylläpidolle.
Matala (M), esimerkkejä	Tietoaineisto julkista, salassa pidettävää tai TLIV. Paljastuessaan tuottaa matalan riskin viranomaisen taktisen tai teknisen toimintamallin paljastumiselle. Ei sisällä yrityksen tai liiketalouden. Voi aiheuttaa lievää mainehaittaa. Tietoaineisto voi olla kasautunutta.	Palvelu käytössä 24/7/365. Tietoluokan puuttuminen operatiivisesta työstä ei aiheuta merkittävää haittaa toiminnalle. Varajärjestelmä parantaa tilannetta, mutta tietoaineiston osalta sen käyttöönotto ei ole aikakriittistä. Palvelun tavanomainen käyttövarmuus riittää. Ei erityisiä varmuus-, palautus- tai ylläpitovaatimuksia.	Ei merkittävää riskiä ihmisen terveydelle. Ei aiheuta riskiä organisaation päätehtävän jatkuvuudelle tai maineelle tai partioille / yksiköille. Hätöilmoituksen vastaanotto tai tehtävän välittäminen viranomaisyksikölle ei häiriinny. Tietoaineiston nimeämismuodolla on kosmeettista merkitystä tiedon ylläpidolle.

Henkilötietoja (HLÖ) esimerkkejä	Tietotyyppi sisältää henkilötietoja. Henkilötietojen sisältyminen tietotyyppiin merkitään ruksilla (X). Henkilötietoja sisältävä luottamuksellinen tieto tulee olla vähintään salassa pidettävää, jollei tieto muun arviointiperusteen myötä ole luokiteltu turvallisuusluokitelluksi tiedoksi (TL III - TL IV). Tieto täydentää luokittelun arviointia.
Kasautuvuus (KASA) esimerkkejä	Tietotyyppi sisältää merkittävää kasautumista. Kasautuvuuden sisältyminen tietotyyppiin merkitään ruksilla (X). Kasautuvuutta sisältävä luottamuksellinen tieto tulee olla vähintään salassa pidettävää, jollei tieto muun arviointiperusteen myötä ole luokiteltu turvallisuusluokitelluksi tiedoksi (TL III - TL IV). Tieto täydentää luokittelun arviointia. Kasautuvuus voi ilmentyä myös tavalla, että tietotyyppiin liittyy kasautuva tietoaalkio, joka on jo itsessään luokiteltu tiedon luontivaiheessa.
Ei tarvetta luokitella (N/A)	Tietotyyppiä ei ole tarvetta luokitella viranomaisen näkökulmasta. Tietotyyppi voi olla epätarkoituksenmukainen kyseistä viranomaisuutta koskien. Tietotyyppi voi esimerkiksi ohjata toiminnallisuutta, joka ei arvioivalla viranomaisella ole käytössä. Merkinnän osalta perustelu tarkennetaan luokitteludokumenttiin.

Liite 3: Palautekysely

Ryhmähaastattelujen päätteeksi vastaajia pyydettiin arvioimaan käytettyä menetelmää.

KYSYMYKSET:

1. Oliko kehitetty malli soveltuva tietotyyppien luokittelun arviointiin?
2. Tuoko malli mielestäsi uusia käytännön työkaluja tietoaineiston syötön ja ylläpidon prosessin johtamiseen ja tietoturva vaatimusten tunnistamiseen?
3. Tunnistatko mallista osa-alueita, jotka tekivät siitä tehokkaan/tehottoman tai soveltuvan/soveltumattoman suunniteltuun käyttötarkoitukseen. Mitä nämä tekijät tai osa-alueet ovat?
4. Puuttuiko mallista mielestäsi jotain? Mitä puuttui?
5. Miten mallia voitaisiin kehittää?
6. Soveltuuko malli suunniteltuun käyttötarkoitukseen?
7. Muu palaute?