VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Selvitys digitalisaation ja uusien teknologioiden vaikutuksista tiedonhallintalakiin pohjautuvaan tietoturvallisuussääntelyyn ja suosituksiin

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja – 2023:41

Valtiovarainministeriön julkaisuja 2023:41

Selvitys digitalisaation ja uusien teknologioiden vaikutuksista tiedonhallintalakiin pohjautuvaan tietoturvallisuus-sääntelyyn ja suosituksiin

Esiselvitys

Tiedonhallintalautakunta

Valtiovarainministeriö Helsinki 2023

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

ISBN pdf: 978-952-367-437-0
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2023

Kuvailulehti
xx.xx.2023

Selvitys digitalisaation ja uusien teknologioiden vaikutuksista tiedonhallintalakiin pohjautuvaan tietoturvallisuussääntelyyn ja suosituksiin : Esiselvitys

Valtiovarainministeriön julkaisuja 2023:41		**Teema**	Julkisen hallinnon ICT
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	suomi	**Sivumäärä**	63

Tiivistelmä

Tämän selvitystyön tavoitteena oli ennakoivasti tunnistaa ja nostaa tiedonhallintalautakunnan alaisen tietoturvallisuusjaoston käsiteltäväksi, miten digitalisaatio ja uudet teknologiat vaikuttavat tietoturvallisuussääntelyyn ja miten muutokset tulisi huomioida jaoston vastuulla olevissa suosituksissa. Selvitystyö toteutettiin tutkimalla avoimia tietolähteitä, järjestämällä asiantuntijahaastatteluja ja toteuttamalla työpaja tietoturvallisuusjaoston jäsenille tunnistettujen ilmiöiden vaikutusten arvioinnista.

Uusi teknologia, digitalisaatio ja niihin liittyvät riskit luovat tarpeita uusille suosituksille ja nykyisten suositusten päivittämiselle. Selvitystyön tuloksissa korostuvat kehittämistarpeet suositusten käytännönläheisyyden ja konkreettisuuden lisäämiseksi. Luvun 6 yhteenveto sisältää suosituskohtaiset koosteet ehdotetuista toimenpiteistä sekä aiheet jatkoselvityksille. Lisäksi suositusten laadinnan prosesseja ja toimintamalleja on syytä tarkastella kokonaisuutena selvitystyön havaintojen pohjalta ja arvioida, mitkä ehdotetut kehittämistoimenpiteet tuovat suosituksille parempaa vaikuttavuutta ja kehittävät niiden käytännönläheisyyttä. Tavoitteena tulisi olla tiedonhallintayksiköiden parempi kyky soveltaa suosituksia omaan toimintaansa.

Tiedonhallintalautakunta hyväksyi selvitystyön 2.3.2023.

Asiasanat	julkisen hallinnon ict, tietoturva, lautakunnat, tiedonhallintalautakunta, tiedonhallintalaki, julkinen hallinto, digitalisaatio		
ISBN PDF	978-952-367-437-0	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-437-0		

Presentationsblad
xx.xx.2023

Utredning om vilka konsekvenser digitaliseringen och ny teknik har för de informationssäkerhetsbestämmelser och de rekommendationer som baserar sig på informationshanteringslagen

Finansministeriets publikationer 2023:41		**Tema**	Offentliga förvaltningens ICT
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	finska	**Sidantal**	63

Referat

Syftet med utredningen var att proaktivt identifiera och informera informationshanteringsnämndens sektion för informationssäkerhet om vilka konsekvenser digitalisering och ny teknik har för bestämmelserna om informationssäkerhet och hur dessa bör beaktas i de rekommendationer som sektionen ansvarar för. Utredningsarbetet genomfördes genom att undersöka öppna informationskällor, intervjua experter och ordna en workshop för medlemmarna i sektionen för informationssäkerhet om bedömning av konsekvenserna av fenomen som identifierats.

Ny teknik, digitalisering och riskerna som är kopplade till dem skapar behov att ge nya rekommendationer och uppdatera de nuvarande rekommendationerna. I utredningens resultat betonas behovet av att göra rekommendationerna mer praktiska och konkreta. I kapitel 6 sammanfattas vilka åtgärder som föreslås i fråga om de enskilda rekommendationerna samt vilka ärenden som kräver fortsatta utredningar. Det finns också skäl att se över processerna och verksamhetsmodellerna för utarbetandet av rekommendationer utifrån iakttagelserna som gjorts i utredningen och bedöma vilka av de föreslagna utvecklingsåtgärderna som kan ge rekommendationerna bättre genomslag och göra dem mer praktiska. Målet är att informationshanteringsenheterna har bättre förmåga att anpassa rekommendationerna till sin egen verksamhet.

Informationshanteringsnämnden godkände utredningen den 2 mars 2023

Nyckelord	ICT inom offentlig sektor, informationssäkerhet, nämnder, informationshanteringsnämnden, informationshanteringslag, offentlig sektor, digitalisering		
ISBN PDF	978-952-367-437-0	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-437-0		

Sisältö

Julkaisun ulkopuoliset liitteet:
Liite on tallennettu omana tiedostonaan osoitteeseen https://urn.fi/URN:ISBN:978-952-367-437-0

1 Johdanto

Julkinen hallinto on alkanut hyödyntää digitalisaatiota viime vuosina merkittävästi aiempaa enemmän, minkä vuoksi digitaalinen turvallisuus ja sen ohjeistaminen lainsäädännöllä sekä erilaisilla suosituksilla on yhä tärkeämpää. Julkisen hallinnon tiedonhallintaa ja tietoturvaa koskevien suositusten tarkoituksena on auttaa julkisen hallinnon organisaatioita soveltamaan lainsäädännön vaatimuksia omaan toimintaansa.

Suosituksilla voidaan ohjeistaa myös uusien teknologioiden hyödyntämistä lainsäädännön vaatimukset huomioiden. Tästä esimerkkinä toimivat pilvipalveluihin liittyvät suositukset. Digitalisaation hyödyntämiseen liittyvien ohjeiden ja suositusten tavoitteena julkisessa hallinnossa on myös lisätä tehokkuutta ja kehittää palveluja. Suositusten avulla julkisen hallinnon toimijat voivat määritellä käyttämiensä teknologioiden ja tietoturvamenetelmien vaatimukset sekä varmistaa, että ne ovat annettujen vaatimusten ja tavoitteiden osalta yhdenmukaisia.

Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019), jäljempänä *tiedonhallintalaki*, 10 §:ssä säädetään julkisen hallinnon tiedonhallintalautakunnan tehtävästä edistää tiedonhallintalaissa säädettyjen menettelytapojen ja vaatimusten toteuttamista. Tehtävän toteuttamiseksi lautakunta antaa ohjeita ja suosituksia sille laissa säädetyn tehtävän alalla. Tiedonhallintalautakunnan tietoturvallisuusjaoston tehtävänä on laatia ja kehittää julkisen hallinnon tiedonhallintalain 4 luvussa säädettyihin vaatimuksiin perustuvia suosituksia.

Tietoturvallisuusjaosto käynnisti syksyllä 2022 selvitystyön, jonka tavoitteena oli ennakoivasti tunnistaa ja nostaa tietoturvallisuusjaostoon käsiteltäväksi tiedonhallintaan ja tietoturvallisuuteen kohdistuvat muutokset sekä se, miten nämä tulisi huomioida jaoston vastuulla olevissa suosituksissa. Selvitystyössä tarkastellaan erityisesti julkisen hallinnon digitalisaation ja teknologian kehittymisen ilmiöitä. Lähtökohtana selvitystyölle on, että sen tuloksia hyödynnetään vuonna 2023 tiedonhallintalautakunnan antamien suositusten kehittämiseen.

Selvitystyö toteutettiin tutkimalla avoimia tietolähteitä, järjestämällä haastatteluja valtiovarainministeriön ja Digi- ja väestötietoviraston avainhenkilöille sekä toteuttamalla työpaja tietoturvallisuusjaoston jäsenille tunnistettujen ilmiöiden vaikutusten arvioinnista. Selvityksessä esitellään työn taustalla olevat suositukset sekä yleisellä tasolla vastaavissa selvityksissä hyödynnettyjä julkaisuja. Selvitystyöhön rajattiin tietyt aihealueet

haastattelujen pohjalta, joiden vaikutusta arvioitiin työpajan ja selvitystyön asiantuntijoiden kesken. Näistä muodostettiin havainnot ja ehdotukset tiedonhallintalautakunnan tietoturvallisuusjaoston vastuulla olevien suositusten kehittämiselle.

Selvityksen loppuun on koottu tulokset, jotka muodostavat kokoelman kehitysehdotuksia suositusten kehittämiselle. Työssä tunnistettiin useita jatkotutkimuksen aiheita, joita on listattu työn viimeiseen lukuun.

2 Julkisen hallinnon suosituksista

Tiedonhallintalaki ja valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä *turvallisuusluokitteluasetus*, tulivat voimaan 1.1.2020. Lain tarkoituksena on edistää tiedonhallinnan yhdenmukaistamista, tietoturvallisuutta ja digitalisointia viranomaistoiminnassa. Tiedonhallintalaissa säädetään julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa. Laki sisältää koko julkista hallintoa koskevat säännökset tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteentoimivuudesta, tietojärjestelmien yhteentoimivuuden toteuttamisesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta. [13]

Tiedonhallintalain 10 §:ssä säädetään valtioneuvoston nimittämän tiedonhallintalautakunnan tehtävästä arvioida ja edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja lain vaatimusten toteuttamista. Edistämistehtävän kohteena ovat tiedonhallintalain soveltamisalaan kuuluvat viranomaiset sekä julkista hallintotehtävää hoitavat yksityiset ja yhteisöt. Tiedonhallintalautakunta on asettanut jaostoja, jotka laativat ja ylläpitävät tiedonhallintalaissa säädettyjen vaatimusten toteuttamista koskevia suosituksia. Tiedonhallintalautakunnan suositukset eivät ole velvoittavia tai sitovia, vaan niissä ohjataan tiedonhallintayksikköjä ja viranomaisia toteuttamaan tiedonhallintalaissa säädetyt vaatimukset hyviin käytänteisiin pohjautuen. [14]

Tiedonhallintalain 4 luvussa säädetään tietoturvallisuutta koskevista vähimmäisvaatimuksia, jotka kaikkien tiedonhallintalain soveltamisalaan kuuluvien viranomaisten tulee täyttää. Tiedonhallintalautakunnan tietoturvallisuusjaoston tehtävänä on kehittää tähän lukuun pohjautuvia suosituksia lain soveltamisen ja vaatimusten toteuttamisen tueksi. Tämän selvitystyön taustana toimivat seuraavassa listatut suositukset. Selvitystyön tuloksena kappaleessa 6 on kuvattu ehdotukset suositusten kehittämiselle.

- **Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta, VM 2021:65** – Suosituskokoelma sisältää soveltamisohjeita useille tiedonhallintalaista nouseville tietoturvallisuusäännöstöille. Suosituskokoelma ottaa kantaa tiedonhallintalain §:ssä 12–17 asetettuihin säännöksiin. [15]

- **Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä, VM 2021:5** - Suosituksessa opastetaan tiedonhallintayksiköitä ja viranomaisia turvallisuusluokitteluasetuksessa säädettyjen tietoturvallisuusvaatimusten toteuttamisessa. Suositus ottaa tiedonhallintalain osalta erityisesti kantaa 18 §:ään. [16]
- **Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa, VM 2022:4** - Suositus täydentää aiemmin annettua suositusta turvallisuusluokiteltavien asiakirjojen käsittelystä. Nämä kaksi suositusta opastavat täyttämään tiedonhallintalain 18 §:n ja turvallisuusluokitteluasetuksen vaatimuksia. [17]
- **Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), VM 2022:43** - Suosituksessa kuvataan julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), ja ohjeistetaan sen käytöstä. Arviointikriteeristö tukee koko julkishallinnon tietoturvallisuuden kehittämisen ja arvioinnin tarpeita. Sitä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä [18]

Selvitystyössä kartoitettiin tiedonhallintalakiin pohjautuvien suositusten lisäksi muut olemassa olevat tietoturvallisuuteen liittyvät julkisen hallinnon ohjeistukset. Ohjeita ja suosituksia kartoitettiin valtiovarainministeriön, Digi- ja väestötietoviraston ja Kyberturvallisuuskeskuksen julkaisuista. Liitteeseen 1 on kerätty laajempi kokoelma tietoturvallisuuteen liittyviä ohjeistuksia. Liitteessä kuvattujen ohjeiden lisäksi on olemassa myös muita toimialakohtaisia tietoturvaan liittyviä ohjeistuksia. Tiedonhallintalautakunnan suositukset löytyvät tiedonhallintalautakunnan sivuilta.

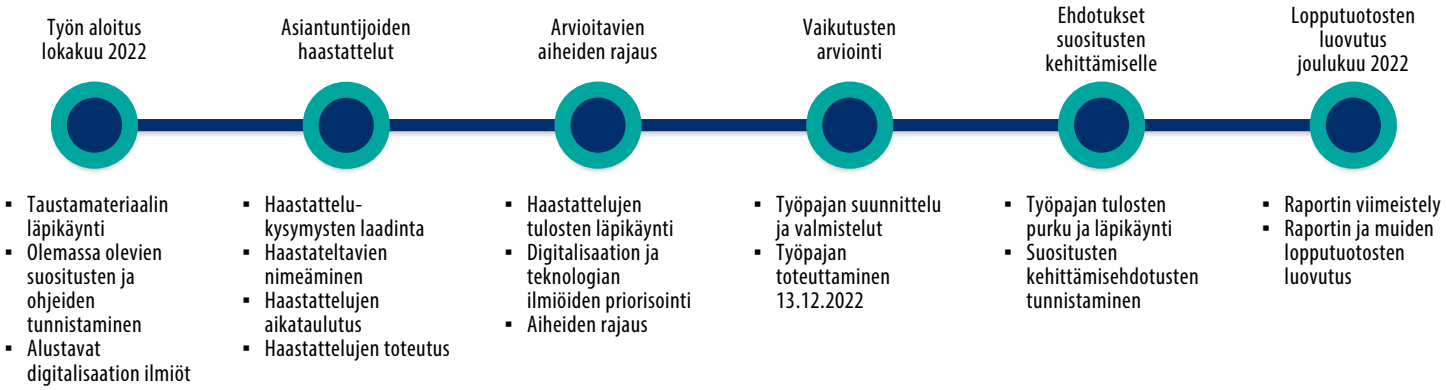
Julkisen hallinnon organisaatioiden tietoturvaa ja tiedonkäsittelyä on ohjeistettu useilla suosituksilla ja ohjeilla, joita eri julkisen hallinnon organisaatiot ovat erilaisista näkökulmista tuottaneet. Ohjeiden kohderyhmä vaihtelee, sillä osa on selkeästi kohdennettu julkisen hallinnon organisaatioille, osa myös yksityisille yrityksille ja kansalaisille. Valtiovarainministeriön ja tiedonhallintalautakunnan julkaisut on selkeästi kohdennettu julkisen hallinnon organisaatioille, mutta esimerkiksi Digi- ja väestötietoviraston ja Kyberturvallisuuskeskuksen ohjeiden kohderyhmä on monessa tapauksessa laajempi.

Organisaation voi olla haastavaa tunnistaa ja löytää selkeästi siihen kohdistuvat suositukset ja ohjeet, koska niitä on nykyisellään useilla eri sivustoilla, niitä on tuotettu useista eri näkökulmista ja niiden velvoittavuus ei ole nopeasti tunnistettavissa. Lisäksi julkaisijoiden verkkosivuilta löytyvät ohjeet ja suositukset ovat osittain vanhentuneita, jolloin niiden taustana voi olla vanhentunutta lainsäädäntöä, eivätkä ne välttämättä huomioi nykyajan digitalisaation hyödyntämistä ja moderneja työskentelytapoja. Julkaisuissa ohjeistetaan monissa tapauksissa samoista asioista. Esimerkiksi pilvipalveluita, etätyötä ja riskienhallintaa käsitellään monessa erillisessä ohjeessa.

3 Selvitystyön toteuttaminen

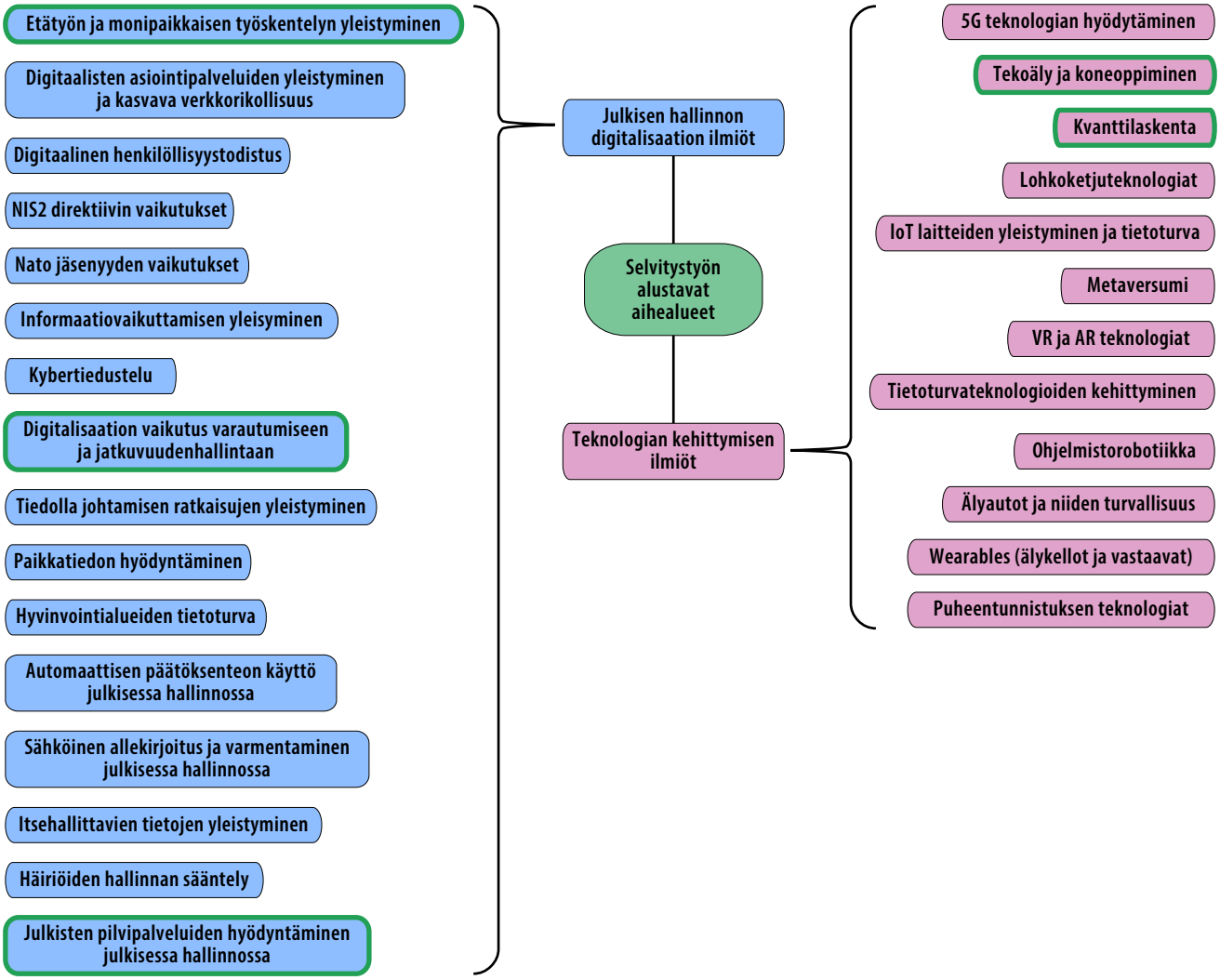
Selvitystyö toteutettiin tutkimalla digitalisaation ja teknologian ilmiöitä sekä näiden tulevaa kehitystä julkisista lähteistä ja haastattelemalla valtiovarainministeriön ja Digi- ja väestötietoviraston asiantuntijoita. Tunnistettujen ilmiöiden vaikutuksia arvioitiin tietoturvallisuusjaostolle järjestetyssä työpajassa joulukuussa 2022, jonka perusteella luotiin lopulliset ehdotukset olemassa olevien suositusten kehittämiselle ja uusien suositusten luomiselle. Lopputuotokset luovutettiin joulukuun 2022 lopussa tietoturvallisuusjaostolle. Kuviossa 1 on esitetty selvitystyön eri vaiheet.

Kuvio 1. Selvitystyön vaiheet



Työn alkuvaiheessa tutustuttiin olemassa oleviin suosituksiin ja muihin ohjeisiin sekä kartoitettiin, millaisia julkisen hallinnon digitalisaation ilmiöitä on havaittu julkisen hallinnon toimintakentässä ja mitkä niihin liittyvät teknologiat yleistyvät tällä hetkellä. Käsiteltäviä ilmiöitä kartoitettiin myös selvitystyön haastatteluissa. Näistä muodostettiin yhteenveto, joka on koottu kuvioon 2.

Kuvio 2. Selvitystyön alustavat aihealueet



Haastatteluissa pyrittiin tunnistamaan ilmiöiden lisäksi millaisia haasteita ja kehityskohteita olemassa olevissa tietoturvallisuuteen liittyvissä suosituksista ja ohjeistuksissa on havaittu sekä millaisille uusille suosituksille nähdään tarpeita. Haastattelut järjestettiin Teams-kokouksina sekä osittain kirjallisina haastatteluina. Haastattelun kysymykset on esitetty liitteessä 2. Haastateltavat henkilöt olivat:

- Jarkko Levasma, ICT-johtaja, valtiovarainministeriö (kirjallinen haastattelu)
- Mikko Pitkänen, Yksikön johtaja, Digi- ja väestötietovirasto
- Kirsi Janhunen, Johtava asiantuntija, Digi- ja väestötietovirasto
- Juho Reivo, Erityisasiantuntija, Digi- ja väestötietovirasto
- Tuomas Pelttari, Johtava asiantuntija, Digi- ja väestötietovirasto
- Martti Setälä, Johtava asiantuntija, valtiovarainministeriö
- Tommi Oikarinen, Tietohallintoneuvos, valtiovarainministeriö
- Tuija Kuusisto, Tietohallintoneuvos, valtiovarainministeriö.

Haastattelujen pohjalta selvitystyöhön rajattiin viisi aihealuetta, joiden vaikutusta julkisen hallinnon organisaatioihin arvioitiin yhteisessä työpajassa 13.12.2022. Työpajaan oli kutsuttu tiedonhallintalautakunnan tietoturvallisuusjaoston jäsenet, tiedonhallintalautakunnan sihteeristö sekä asiantuntijoilta. Arviointiin rajatut aiheet olivat:

1. Uuden teknologian hyödyntäminen julkisessa hallinnossa (erityisesti tekoäly ja kvanttilaskenta)
2. Julkisten pilvipalveluiden hyödyntäminen julkisessa hallinnossa
3. Etätyön ja monipaikkaisen työskentelyn yleistyminen julkisessa hallinnossa
4. Digitalisaation vaikutus varautumiseen
5. Suositusten kehittäminen yleisesti.

Työpajassa esiteltiin valitut aihealueet, jonka jälkeen arvioitiin niiden mahdollisuuksia, riskejä ja haasteita sekä ehdotuksia suositusten kehittämiselle. Osallistujien ajatukset kerättiin yhteen Miro-sovelluksella.

Tuloksista muodostui aihealuekohtaisesti kattava kooste riskeistä, mahdollisuuksista ja suositusten kehittämisehdotuksista. Näiden tarkemmat havainnot on kuvattu luvussa 4. Ilmiöiden ja muutosten vaikutusta julkiseen hallintoon arvioitiin erityisesti seuraavista näkökulmista.

1. Kuinka digitalisaation ilmiöt ja muutokset näkyvät julkisen hallinnon organisaatioissa, mitä riskejä tai uhkia ne tuovat organisaatiolle sekä kuinka niiltä voidaan suojautua.
2. Kuinka julkisen hallinnon toimijat voivat hyödyntää ja hyödyntävät uusia teknologioita sekä mitä tietoturvariskejä tai -uhkia niiden käyttäminen sisältää.
3. Kuinka esimerkiksi verkkorikolliset voivat hyödyntää uusia teknologioita ja julkisen hallinnon digitalisaation ilmiöitä sekä kuinka tältä voidaan suojautua.
4. Kuinka havaitut asiat tulisi huomioida julkisen hallinnon suosituksissa ja ohjeistuksissa.

Teknologioiden vaikutusten arvioinnissa hyödynnettiin myös Goforen asiantuntijoiden näkemyksiä ja kokemuksia. Arvioinnissa huomioitiin erityisesti teknologian hyödyntämiseen liittyvät turvallisuusriskit sekä kyberrikollisten hyödyntämä uusi teknologia. Haastattelujen, kerättyjen asiantuntijoiden kommenttien ja työpajan tulosten pohjalta muodostettiin luvussa 5 esitetyt ehdotukset olemassa olevien suositusten kehittämiselle sekä ehdotukset uusien suositusten laatimiselle.

4 Digitalisaation kehittyminen julkisessa hallinnossa ja sen aiheuttamat muutokset

Digitalisaation hyödyntäminen Suomen julkisen hallinnon kehittämisessä on lisääntynyt viime vuosina merkittävästi. Tästä kertoo muun muassa hallitusohjelmaan asetettu tavoite, jossa Suomi tunnetaan edelläkävijämaana, ja jossa digitalisaation ja teknisen kehityksen tuomia mahdollisuuksia kehitetään ja otetaan käyttöön yli hallinto- ja toimialarajojen. Tavoitteena on nostaa julkisen sektorin teknologia- ja digitalisaatiokyvykkyyttä sekä kehittää julkisen ja yksityisen sektorin yhteistyötä [11].

Digitalisaation kehittyminen julkisessa hallinnossa korostaa myös digitaalisen turvallisuuden merkitystä, minkä myötä julkishallinnossa on jo käynnissä useita hankkeita, joilla pyritään parantamaan organisaatioiden ja yhteiskunnan toimintatapoja paremman digitaalisen turvallisuuden saavuttamiseksi. Näistä esimerkkeinä ovat valtiovarainministeriön Julkisen hallinnon digitaalisen turvallisuuden toimeenpano 2020–2023 Haukka -hanke, Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030-hanke ja Digi- ja väestötietoviraston Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman JUDO-hanke.

Haastattelujen perusteella julkisen hallinnon digitaalisten palveluiden kehittämisessä painotetaan kasvavissa määrin ihmis- ja yrityslähtöisyyttä, poikkihallinnollisuutta, toimintojen automatisointia ja kybervarautumista. Uusi teknologia luo mahdollisuuksia uusille tehokkaammille toimintatavoille ja digitaalisille palveluille, mutta tuo osaltaan esille myös uudenlaisia riskejä tiedon luottamuksellisuudelle, eheydelle ja saatavuudelle. Esimerkiksi itsehallittavan tiedon ja identiteetin merkitys tulee haastattelujen mukaan kasvamaan tulevaisuudessa, mutta kyberrikollisuuden kehittyessä se luo haasteen tiedon luotettavuudelle ja eheydelle.

Digitaalisten palveluiden yleistyessä julkisen hallinnon organisaatioilla on tarve saada tietoa toisilta organisaatiolta, ja tämä ilmiö kasvaa haastattelujen perusteella räjähdysmäisesti. Tällöin myös riippuvuudet eri palveluiden välillä kasvavat merkittävästi. Digitaalisten palveluiden ja digitalisaation yleistymisen myötä yhteentoimivuuden tarve kasvaa entistä enemmän, mikä on huomioitu tiedonhallintalain tuomassa sääntelyssä. Haastattelujen mukaan nykyiset julkisen hallinnon siilomaiset rakenteet tuovat tähän kuitenkin haasteita.

Kun digitaalisia palveluita kehitetään ja niissä syntyy esimerkiksi yhteisiä rekistereitä, tulisi samalla tarkastella ja uudistaa organisaatiorakenteita ja niihin liittyviä vastuita. Jos yhteisiin rekistereihin muodostuu yhteisiä vastuita, on arvioitava, kuinka tiedonhallintalain vaatimukset täytetään.

Julkisessa hallinnossa tapahtuvat hallinnolliset uudistukset ja rakennemuutokset ovat ilmiöitä, jotka vaikuttavat digitalisaation kehittymiseen. Kun perustetaan uusia virastoja ja toisia lopetetaan, voi syntyä uusia tehtäviä, joissa tietoa käsitellään uudella tavalla. Tämä ohjaa kehittämään uusia digitaalisia ratkaisuja, joihin tiedonhallintalain vaatimukset tulevat sovellettavaksi. Haastatteluissa esimerkkinä nostettiin esille työvoimapalveluiden uudistus vuonna 2023, jonka myötä on odotettavissa muutoksia palveluiden toteuttamiseen ja yhteisiin tietovarantoihin.

Kun digitalisaatio julkisessa hallinnossa kehittyy, syntyy tarve kehittää lainsäädäntöä ja luoda siihen pohjautuvia suosituksia ja ohjeistuksia. Lainsäädännön myötä julkisen hallinnon organisaatioille kohdistuu lisää uusia vaatimuksia ja odotuksia, mikä tarkoittaa myös tarvetta budjetti- ja henkilöstöresursseille. Tässä koetaan haastattelujen perusteella tällä hetkellä ristiriitaa, koska kyseiset resurssit eivät kohtaa kasvavien vaatimusten kanssa.

4.1 Julkisten pilvipalveluiden käytön yleistyminen

Valtiovarainministeriön vuonna 2018 julkaisemissa julkisen hallinnon pilvipalvelulinjauksissa mainitaan, että pilvipalveluita tulisi suosia, mikäli niiden hankinnalle ei ole esteitä ja ne tarjoavat parhaan hyödyn. Lisäksi ei-julkista tietoa voidaan käsitellä julkisessa pilvipalvelussa, jos palvelun tietoturva ja tietosuoja ovat kunnossa. [12] Julkipilvipalveluiden käyttöönottoa on edistetty julkisessa hallinnossa merkittävästi viime vuosina, mutta palveluiden käyttö on edelleen haaste erityisesti turvallisuusviranomaisille, jotka käsittelevät tehtävissään paljon turvallisuusluokiteltua tietoaineistoa.

Teknologian kehittyessä enemmän pilvipalveluiden varaan ajaudutaan ennen pitkään tilanteeseen, jossa perinteisiä, paikallisiin konesaleihin asennettavia järjestelmiä ei ole enää tarjolla. Vastaavasti monen uuden teknologian hyödyntäminen vaatii aiempaa suuremman määrän laskentakapasiteettia, jota ei ole järkevää toteuttaa organisaation omaan konesaliin. Näiden myötä pilvipalveluiden käyttöönotto tulee vastaan ennemmin tai myöhemmin kaikille digitalisaatiota hyödyntäville organisaatiolle.

Julkipilvipalveluiden käyttämiseen liittyviä haasteita julkisessa hallinnossa ovat esimerkiksi salassa pidettävän ja turvallisuusluokitellun tiedon käsittely, varautumisen ja jatkuvuudenhallinnan näkökulmat, tietosuojan ja muun lainsäädännön toteutuminen sekä sopimusehdot. Haastattelujen perusteella tiedonhallintalain ei nähdä suoraan estävän

pilvipalveluiden käyttöä, mutta erityisesti nykyisen tietosuojaan liittyvä lainsäädännön on nähty aiheuttavan erilaisia tulkintoja julkipilvipalveluiden käyttämisestä. Tiedonhallintalautakunnan pilvipalveluihin liittyvissä suosituksissa korostetaan riskipohjaista arviointia pilvipalveluiden käyttämiselle, mikä jättää viranomaiselle harkintamahdollisuuden niiden käyttöönotolle eri käyttötilanteissa.

Turvallisuusluokitellun tietoaineiston osalta vuonna 2020 julkaistun Pilvipalveluiden turvallisuuden arviointikriteeristö, jäljempänä *PiTuKri*, vaatimuksena on, että turvallisuusluokka IV-tason tietoaineiston fyysinen sijaintipaikka tulee olla Suomen rajojen sisällä. Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. [19] Tyypillisesti PiTuKria käytetään valtiohallinnon pilviympäristöjen tietoturvan arviointikriteeristönä ja sen myötä esimerkiksi AWS:n tai Microsoft Azuren julkipilvipalvelujen hyödyntäminen ei ole tällä hetkellä täysimääräisesti mahdollista TLIV-tason tietoaineiston käsittelyyn tai tallentamiseen. Googlen julkipilvipalvelussa on olemassa Suomen Haminassa oma palvelualue (region), jolloin tieto voidaan käsitellä ja tallentaa Suomen rajojen sisäpuolella. Käytön arvioinnissa on kuitenkin huomioitava, että tarvittavat pilvipalveluiden toiminnot ovat saatavilla kyseisellä alueella ja varmistettava, että palveluntuottajat eivät pääse tietoon käsiksi.

Tiedon turvallisen sijainnin osalta tulisi arvioida, onko Suomessa sijaitseva oma konesali erilaisissa kriisitilanteissa turvallisempi kuin toiseen maahan hajautettu ympäristö. Tämä näkökulma tuli esille useammassa haastattelussa jatkuvuuden ja varautumisen osalta. Ukrainassa käytävän sodan myötä osa siellä sijaitsevista toimijoista on siirtänyt palveluitaan ulkomailla sijaitseviin pilvipalveluihin, koska omassa maassa sijaitsevat konesalit ovat alttiina jatkuvalle pommitukselle ja esimerkiksi kriittisen infrastruktuurin häiriöille kuten sähkökatkoksille. Suosituksissa tulisi arvioida myös monipilven tuomia etuja jatkuvuuden näkökulmasta ja toisaalta sitä, millaisia haasteita tai riskejä se tuo esille. Haastattelujen perusteella tällä hetkellä näkemyksenä on, että nykyiset pilvipalveluihin liittyvät ohjeistukset ja suositukset eivät ole riittäviä tukemaan pilvipalveluiden käyttöönottoa julkisessa hallinnossa.

Julkipilvipalveluiden tuottaminen keskittyy tällä hetkellä muutamille globaaleille toimijoille. Haastattelujen perusteella pilvipalveluiden hyödyntämistä arvioitaessa tulisi pohtia, millaisia riskejä tämä muodostaa organisaatiolle ja onko esimerkiksi avoimen lähdekoodin ratkaisujen hyödyntäminen parempi vaihtoehto, mikäli halutaan välttää toimittaja- ja ekosysteemilukkoja sekä riippuvuutta tietyistä isoista palvelutoimittajista. Kun aiotaan siirtyä pilvipalvelun käyttäjäksi, tulee luoda myös suunnitelma, jossa kuvataan, kuinka palveluntarjoajaa vaihdetaan tai kuinka data kotiutetaan esimerkiksi omaan konesaliin tarpeen vaatiessa. Tämä ajattelutapa luo toisaalta myös haasteen hyödyntää niin kutsuttuja

serverless-palveluita, joissa palvelut tarjotaan kustannustehokkaasti SaaS-palveluna pilvialustalta. Monissa organisaatioissa palvelut toteutetaan julkipilvialustaan esimerkiksi konttiteknologiaa hyödyntäen, jolloin palvelualustaa on tarvittaessa helpompi vaihtaa.

Tiedonkäsittelyn siirtyessä pilvipalveluiden päälle tarvitaan myös kyvykkyydet tiedon käsittelyn valvontaan ja seuraamiseen. Haastattelujen perusteella pilvipalvelun hyödyntäjällä tulee olla riittävän hyvä ymmärrys palvelun toiminnasta ja sisällöstä. Lisäksi tarvitaan selkeä ohjeistus siihen, miten palvelu otetaan oikealla tavalla käyttöön. Tätä voisivat tukea esimerkiksi referenssiarkkitehtuurit ja konkreettisemmat julkipilvipalvelukohtaiset suositukset tai ohjeistukset.

Pilvipalveluissa toimivan ratkaisun ymmärtäminen korostuu erityisesti silloin kun käsitellään henkilötietoa, salassa pidettävää tietoa tai turvallisuusluokiteltua tietoa. Tällöin on pystyttävä todistamaan tiedon omistajalle, että tietoa käsitellään turvallisesti ja vain siihen tarkoitukseen kuin on aiottu. Esimerkiksi jos jokin toimija käyttää kaupungin tuottamaa palvelua, joka hyödyntää pilvipalvelua, tulee tiedon omistajan ja palvelun käyttäjän ymmärtää palvelun toiminnasta riittävästi, jotta voidaan varmistua lakien velvoitteiden toteutumisesta. Tämän myötä haastatteluissa nostettiin esille tarve suositukselle tai ohjeistukselle siitä, mitä dokumentaatiota pitää syntyä kehitettävästä digitaalisesta palvelusta ja mitä tietoa palvelusta tulee antaa palvelun käyttäjälle.

Tietoturvallisuusjaostolle järjestetyssä työpajassa käsiteltiin julkisten pilvipalveluiden mahdollisuuksia, riskejä ja ehdotuksia suositusten kehittämiselle. Tunnistetut julkisten pilvipalveluiden käyttöön liittyvät mahdollisuudet on esitetty kuviossa 3.

Kuvio 3. Julkisten pilvipalveluiden käytön mahdollisuudet

Tuloksista voidaan todeta, että julkiset pilvipalvelut tuovat skaalautuvuutta, kustannustehokkuutta ja joissain määrin parempaa tietoturvaa sekä mahdollistavat uuden teknologian hyödyntämisen. Työpajassa ehdotettiin myös kansallisen pilvipalvelun instanssin kehittämistä. Riskien osalta nousi esiin erityisesti palvelutarjoajiin ja niiden luotettavuuteen liittyvät riskit. Lisäksi haasteeksi koettiin epäselvyydet siinä, miten pilvipalvelut on rakennettu ja millaisia vastuita niiden palveluketjuissa on. Työpajassa tunnistetut julkisten pilvipalveluiden käyttöön liittyvät riskit ja haasteet on esitetty kuviossa 4.

Kuvio 4. Julkisten pilvipalveluiden käytön riskit ja haasteet

Suositusten kehittämisen osalta vastauksissa korostui tarve konkreettisille tarkastuslistoille, yhteisille kriteeristöille ja työkaluille riskiperusteiseen arviointiin. Lisäksi sopimuksiin liittyville ohjeistuksille ja suosituksille koetaan tarvetta sekä pilvipalveluiden käyttöönoton koulutusta ja tukea tiedonhallintayksiköille tarvitaan lisää. Työpajassa tunnistetut julkisten pilvipalveluiden käyttöön liittyvät ehdotukset suositusten kehittämiselle on esitetty kuviossa 5.

Kuvio 5. Julkisiin pilvipalveluihin liittyvät ehdotukset suositusten kehittämiselle

Yhteenvetona suositusten kehittämisessä tulisi huomioida seuraavia asioita:

- Koulutusten ja ohjeistusten lisääminen yleisesti julkisten pilvipalveluiden käytöstä. Näiden toteuttamisessa voisi hyödyntää esimerkiksi eOppiva-koulutuksia.
- Suositukset sopimusten laadinnasta julkisten pilvipalvelutarjoajien kanssa. Sopimusehtoihin liittyen on käynnissä valtiovarainministeriön Cirrus-hanke, jonka tuotokset voivat tuoda tähän ohjeistusta.
- Selkeät tarkastuslistat pilvipalveluiden käyttöönotolle ja niiden turvallisuusratkaisuille.
- Selkeä työväline riskien arviointiin, jolla pystytään tekemään yhdenmukaisia riskiarviointeja.
- Suosituksiin mukaan esimerkkejä hyväksytyistä jäännösriskeistä ja soveltamistavoista.

- Haasteeksi tunnistetun auditoinnin vaikeuden osalta ohjeistus pilviympäristön turvallisuusarviointiin ja auditoinnin toteuttamiseen.
- Pilvipalveluiden käyttö varautumisen näkökulmasta. Varautumista suunniteltaessa on arvioitava, onko tarpeen, että jotkin palvelut ja tiedot ovat saatavilla ulkomailla sijaitsevista tietovarannoista esimerkiksi tilanteissa, jossa Suomessa olevat konesalit menetetään tai ne ovat muuten alttiina erilaisille paikallisille häiriöille kuten sähkönjakelun häiriöille kriisitilanteissa.

4.2 Etätyö ja monipaikkainen työskentely

Covid-19-pandemian myötä etätyön ja monipaikkaisen työn mallit ovat yleistyneet useissa organisaatiossa. Pandemian aikana välttämätön etätyömallien käyttöönotto osoitti, että tiettyjä työtehtäviä pystytään suorittamaan kotoa käsin yhtä hyvin tai jopa tehokkaammin kuin toimistolta tehtäessä. Pandemian laannuttua etätyön mallista on tullut pysyvä käytäntö useisiin yrityksiin. Myös julkisen hallinnon organisaatioissa etätyön mahdollisuudet ovat yleistyneet modernien digitaalisten työvälineiden myötä.

Rekrytointitilanteissa työnhakijan mahdollisuus valita työskentelypaikka tai suorittaa työtä omalta kotitoimistolta voi olla etu ja lisätä tehtävien houkuttelevuutta. Monissa yrityksissä etätyöskentelystä on tullut normaali käytäntö, joka helpottaa työntekijöiden vapaa-ajan ja työelämän yhteensovittamista. Pakotetusta työpaikalla läsnäolosta voikin syntyä kynnys edes hakea tiettyjä tehtäviä, mikä saattaa nostaa osaamispulaa esimerkiksi digitalisaation asiantuntijatehtävien osalta.

Valtiovarainministeriön mukaan valtion työtehtävistä noin puolet ovat sellaisia, joita on mahdollista tehdä monipaikkaisesti, joko työnantajan osoittamista työpisteissä tai kotona etätyönä. [8] Valtiovarainministeriön teettämän kyselyn perusteella paikkasidonnaista työtä on arvioitu vuosina 2020 ja 2021 tehtävän noin 40 % valtion työtehtävistä ja etätyö on mahdollistettu noin 60 % työtehtävistä. Kyselyn mukaan selkeästi eniten paikkasidonnaista työtä tehdään myös jatkossa turvallisuussektorin organisaatioissa. [9] Tietosuoja ja -turva on todettu eräiksi rajoittaviksi tekijöiksi etätyölle ja erityisesti salassa pidettävän ja turvallisuusluokitellun tietoaineiston käsittely tuo haasteen etätyön tekemiselle.

Vuonna 2021 valtiovarainministeriö on muodostanut monipaikkaisuuden edistämisen linjaukset valtionhallinnossa. Linjauksissa mainitaan muun muassa seuraavat asiat:

- valtio edistää työnteon tapojen uudistumista investoimalla työn digitalisoimiseen, tätä tukeviin välineisiin ja työtiloihin sekä henkilöstön osaamiseen,
- valtiolla käytetään työnantajan tarjoamia työvälineitä, järjestelmiä ja mobiiliyhteyksiä, jotka mahdollistavat monipaikkaisen työnteon turvallisesti, sekä
- muualla kuin työnantajan osoittamissa työtiloissa työntekijä huolehtii, että kalustus, työympäristö sekä verkkoyhteydet ovat turvallisia ja työskentely on tietosuoja- ja tietoturvaohjeiden mukaista.

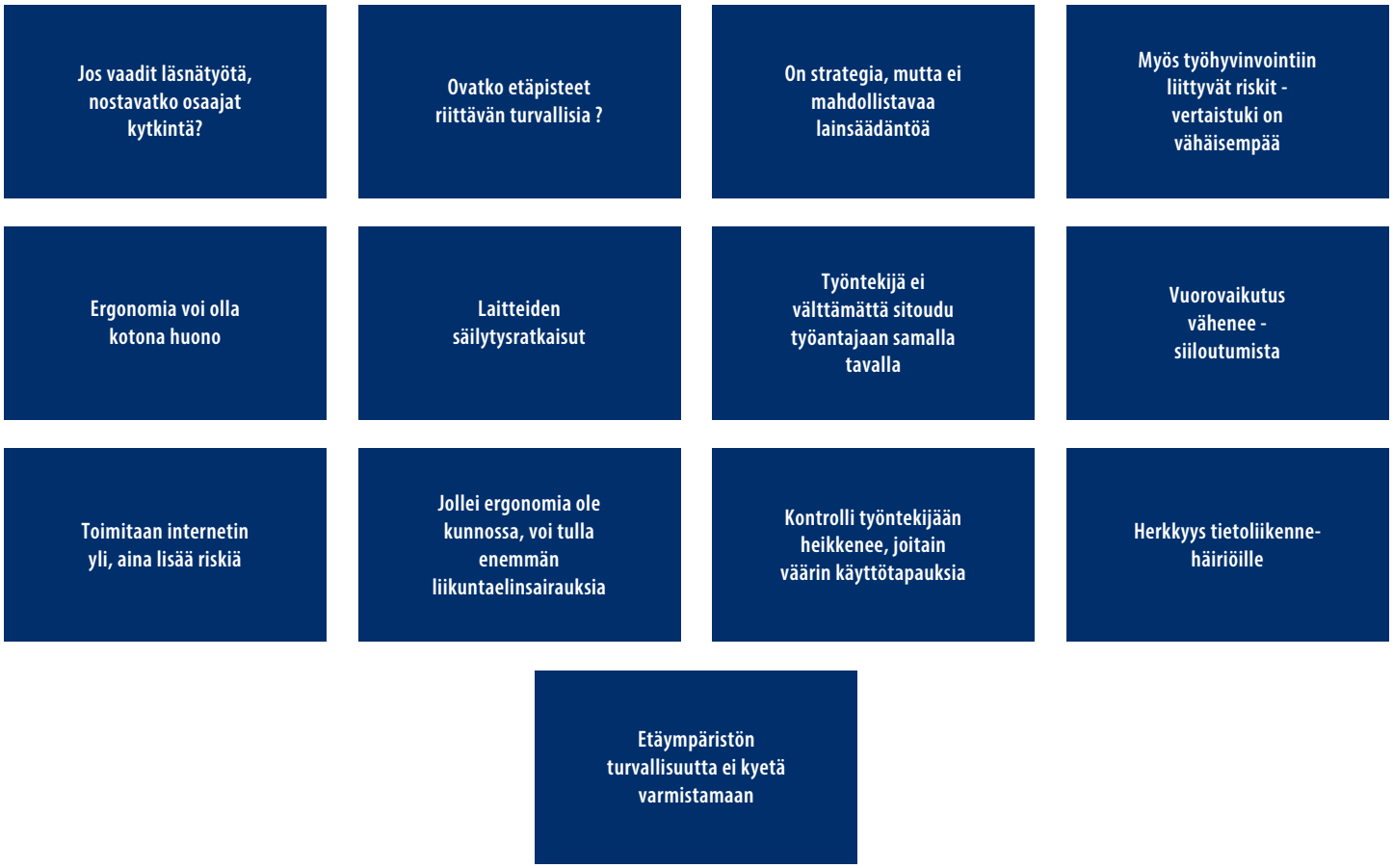
Lisäksi valtioneuvosto hyväksyi valtion toimitilastrategian periaatepäätöksenä 16. joulukuuta 2021, jossa mainitaan, että strategian tavoitteet tulee saavuttaa vuoteen 2030 mennessä. [10]. Linjauksessa 6 mainitaan, että yhteisissä työympäristöissä noudatetaan yhteistä toimitilaturvallisuuskonseptia, joka mahdollistaa salassa pidettävän tiedon asianmukaisen käsittelyn ja säilyttämisen. Edellä mainittujen linjausten myötä julkisen hallinnon organisaatioille syntyy velvoitteita mahdollistaa turvallinen työskentely etäältä ja monipaikkaisessa työympäristössä.

Etätyön ja monipaikkaisen työskentelyn aihetta käsiteltiin selvitystyön työpajassa. Mahdollisuuksien osalta työpajassa nousivat esille muun muassa rekrytointiin liittyvät edut, etätyöpisteiden ja -laitteiden turvallisuustason kasvaminen, toimitilan tarpeiden pieneneminen ja varautumisen mahdollisuudet, kuten työtehtävien suorittaminen poikkeusoloissa etätyöpisteeltä. Työpajassa tunnistetut etätyöhön ja monipaikkaiseen työskentelyyn liittyvät mahdollisuudet on esitetty kuviossa 6.

Kuvio 6. Etätyön ja monipaikkaisen työskentelyn tuomat mahdollisuudet

Riskien ja haasteiden osalta työpajassa nousivat esille erityisesti tietoliikenneyhteyksiin liittyvät riskit, etätyöympäristön turvallisuuteen liittyvät haasteet ja mahdollisiin väärinkäytötapauksiin liittyvät riskit. Riskien ja haasteiden tulokset on esitetty kuviossa 7.

Kuvio 7. Etätyön ja monipaikkaisen työskentelyn tuomat riskit ja haasteet



Suositusten kehittämisen osalta työpajassa nousi esille muun muassa jatkuvuussuunnittelun huomiointi etätyön osalta ja toimitilaturvallisuuden ohjeistuksen lisääminen. Työpajassa nousi esille myös ehdotus oman jaoston perustamiselle toimitilaturvallisuuden asioiden kehittämiselle. Suositusten kehittämisehdotuksien vastaukset on esitetty kuviossa 8.

Kuvio 8. Etätyöhön ja monipaikkaiseen työskentelyyn liittyvät ehdotukset suositusten kehittämiselle

Yhteenvetona suositusten kehittämisessä tulisi huomioida seuraavia asioita:

- Toimitilaturvallisuuden ohjeistuksen lisääminen yleisesti. Nykyiset toimitilaturvallisuuden ohjeet eivät huomio nykyaikaisia työskentelymalleja.
- Ohjeistus siihen, kuinka etätyöskentelymalli tai monipaikkaisen työn malli otetaan käyttöön tiedonhallintayksikössä. Ohjeistuksen tulisi sisältää tarkastuslistat eri työskentelymallien ympäristöille ja siinä on syytä kuvata myös teknisiä tietoturvan kontrolleja esimerkiksi väärinkäytösten ehkäisemiseen.
- Jatkuvuudenhallinnan ohjeistuksissa etätyömallien ja monipaikkaisen työn huomioiminen.
- Olemassa oleviin suosituksiin ohjeet turvallisuusluokitellun aineiston käsittelystä etätyön ja monipaikkaisen työskentelyn näkökulmista.

- Yleisesti nähdään tarve omalle suositukselle toimitilaturvallisuuteen liittyvistä asioista, joka huomioi etätyön ja monipaikkaisen työskentelyn asiat kuten esimerkiksi turvakoppien käyttämisen virastojen yhteisissä tiloissa. Esimerkiksi VAHTI 2/2013-ohje toimitilojen tietoturvallisuudesta sisältää osittain vanhaa tietoa, joten uudelle suositukselle tai ohjeelle nähdään tarve.
- On harkittava myös tarvetta uuden jaoston, joka keskittyy toimitilaturvallisuuden aihealueeseen, perustamiselle.

4.3 Digitalisaation vaikutus varautumiseen

Selvitystyön haastatteluissa tunnistettiin useita eri aihealueita, jotka koskettivat julkisen hallinnon organisaatioiden varautumista. Näitä olivat muun muassa kyberrikollisuuden merkittävä kasvaminen, valtiollinen kybertiedustelu ja -vakoilu sekä informaatiovaikuttaminen. Myös Nato-jäsenyyden vaikutukset nousivat keskusteluissa esille.

Useammassa haastattelussa tuotiin esille huomio verkkorikollisuuden kehittymisestä ja kuinka sen torjunta tulee olemaan tulevaisuudessa haaste. Kansalaiset ja eri organisaatiot tulisi pystyä suojaamaan rikollisilta verkossa ja digitaalisiin palveluihin tulisi pystyä luottamaan jatkossakin. Uusi teknologia mahdollistaa uudenlaiset ja monipuolisemmat hyökkäysmenetelmät rikollisille, minkä vuoksi kaikki uusi teknologia pitäisi hyödyntää myös tietoturvan kehittämiseen sekä suojaus-, havainnointi- ja palautumiskyvykkyyksien parantamiseen.

Eräänä tietoturvan ja varautumisen kehittämismenetelmänä haastatteluissa tuotiin esille Zero Trust -mallin yleistyminen organisaatiossa. Zero Trust käsittää yleisesti käyttäjän identiteetin varmentamisen, päätelaitteen suojaamisen, tiedon ja sovellusten suojaamisen, IT-infrastruktuurin ja verkkojen suojaamisen sekä ympäristön jatkuvan valvonnan. Näiden osalta ympäristöön luodaan toimintamallit, joissa ei suoraan luoteta käyttäjään tai laitteeseen missään tilanteessa ilman esimerkiksi sen identiteetin riittävää varmentamista. Zero Trust -ajattelumallissa oletetaan pahinta ja varaudutaan valmiiksi tilanteisiin, joissa hyökkääjä on päässyt ympäristöön tai suojattavaan tietoon käsiksi. Haastatteluissa painotettiin esimerkiksi sitä, että käyttäjän identiteetti tulisi pystyä varmistamaan eri tilanteissa kuten verkkokokouksiin liittyessä tai sähköpostin lähettämisessä. Näiden asioiden korostaminen tietoturvallisuuteen liittyvissä suosituksissa ja ohjeissa nähdään tärkeäksi.

Kyberrikollisuuden, kybervakoilun ja muiden uhkien myötä varautuminen tietoturvan häiriötilanteisiin on tunnistettu tärkeäksi kehityskohteeksi julkisessa hallinnossa ja tämä on huomioitu myös tiedonhallintalain kehittämisessä. Tiedonhallintalakiin on parhaillaan

kehitteillä lisäys, joka luo sääntelyn häiriötilanteisiin varautumisesta ja siihen liittyvästä viestinnästä. Lain muutoksen myötä nähdään tarpeelliseksi kehittää aiheeseen liittyvä suositus, joka ohjaa julkisen hallinnon organisaatioita täyttämään lain asettamat velvoitteet.

Työpajassa käsiteltiin digitalisaation kehittymisen vaikutuksia varautumiseen. Mahdollisuuksien osalta työpajassa nousivat esiin esimerkiksi riippumattomuus toimitiloista ja monenlaiset varajärjestelyt. Varautumiseen liittyvät työpajassa tunnistetut mahdollisuudet on esitetty kuviossa 9.

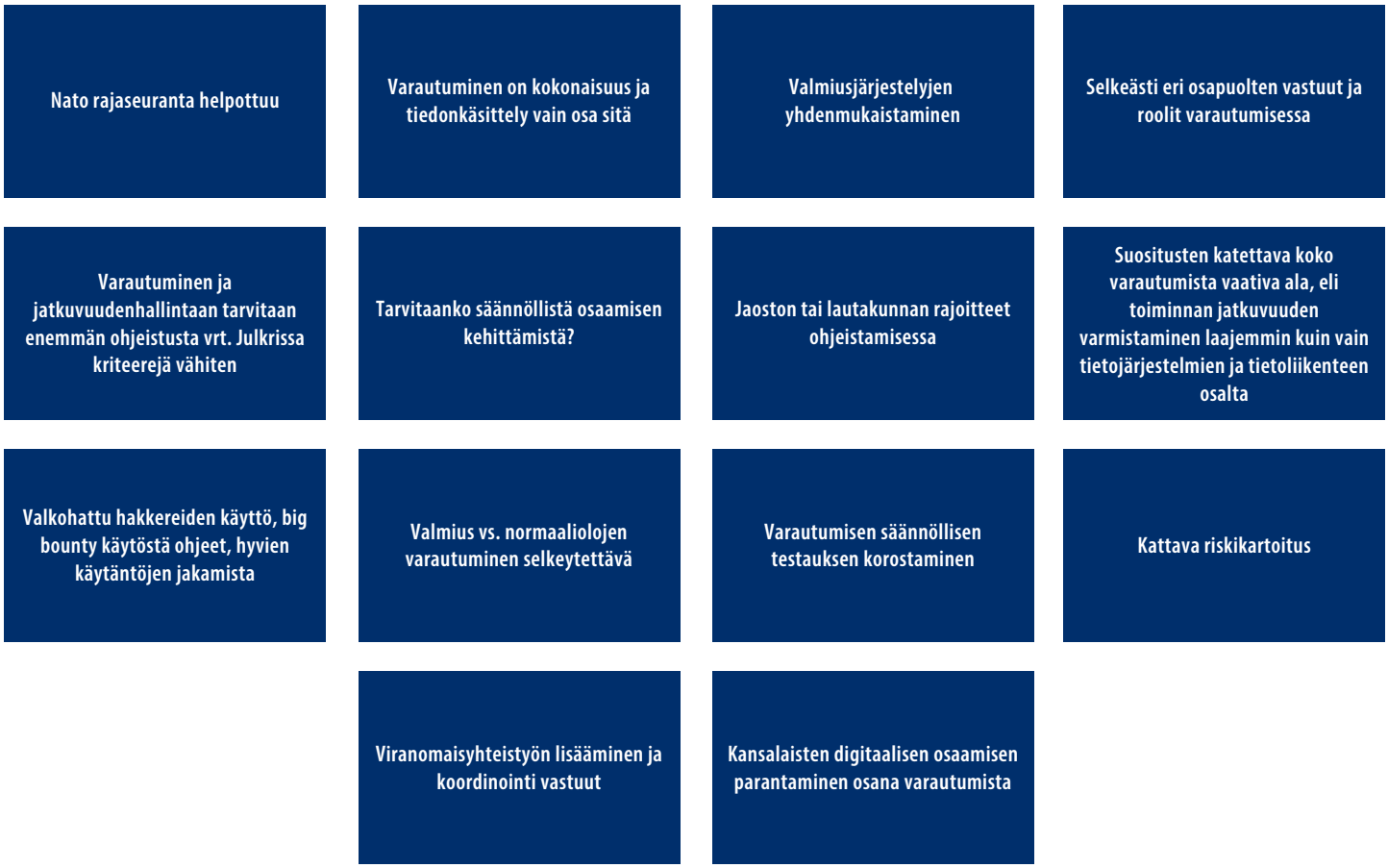
Kuvio 9. Varautumiseen liittyvät mahdollisuudet

Riskien ja haasteiden osalta vastauksissa korostuivat palveluketjujen riskit, riippuvuus ulkomaan tietoliikenneyhteyksistä ja sähkön tuotannosta sekä rikollisten uudet ja tehokkaammat hyökkäysmenetelmät esimerkiksi tekoälyn avulla. Riskien ja haasteiden tulokset on esitetty kuviossa 10.

Kuvio 10. Varautumiseen liittyvät riskit ja haasteet

Suositusten kehittämisen osalta työpajassa nousivat esille normaaliolojen ja poikkeusolojen varautumisen ohjeiden selkeyttäminen, varautumisen testauksen ja harjoittelun korostaminen sekä viranomaisyhteistyön ja koordinoinnin vastuiden ohjeistus. Kuviossa 11 on esitetty työpajassa nousseet ehdotukset suositusten kehittämiselle varautumiseen liittyen.

Kuvio 11. Varautumiseen liittyvät ehdotukset suositusten kehittämiselle



Yhteenvetona suosituksen kehittämiselle tulisi huomioida seuraava asiat:

- Toiminnan testauksen ja harjoittelun ohjeistus varautumiseen liittyvissä suosituksissa. Varautumiseen liittyvät osaamisen kehittämisen menetelmät huomioitava myös yleisesti suosituksissa.
- Viranomaisyhteistyön lisäämisen ja koordinoinnin vastuiden ohjeistaminen. Vastuiden ohjeistaminen on myös yleisesti huomioitava erilaisiin häiriötilanteisiin liittyen.
- Selkeytettävä normaaliolojen varautumisen suositukset ja poikkeusolojen ohjeistukset. Arvioitava, kuvataanko varautumisen ohjeistus molemmista näkökulmista samoissa ohjeissa vai luodaanko esimerkiksi poikkeusoloihin varautumiselle erilliset ohjeet ja suositukset.
- Julkrin varautumisen vaatimusten lisääminen yleisesti. Nykyisellään varautumisen vaatimuksia on kriteeristössä vähiten.

- Ohjeistus valkohattuhakkereiden ja bug bounty -ohjelmien hyödyntämisestä turvallisuuden kehittämisessä.
- Nato-jäsenyyden vaikutusten huomiointi varautumisen ohjeistuksessa.
- Ulkomaan tietoliikenneyhteyksien ja muun kriittisen infrastruktuurin riippuvuuksien huomiointi varautumisen suunnittelun ohjeissa.
- Palvelu- ja toimitusketjujen riskien huomioiminen varautumisen suunnittelun ohjeissa.
- Yleisesti varautumisen osalta nähdään tarve oman edellä mainittuja asioita kattavan suosituksen laadinnalle.

4.4 Uuden teknologian hyödyntäminen julkisessa hallinnossa

Jatkuvasti kehittyvä teknologia luo uusia mahdollisuuksia teknologian hyödyntämiseen, mutta myös uudenlaisia riskejä tiedon suojaamiselle. Uudella teknologialla pysytään tehostamaan toiminnan prosesseja esimerkiksi automaation toiminnoilla, joista esimerkkinä haastatteluissa nousi useasti tekoälyn teknologioiden mahdollistama automaattinen päätöksenteko.

Julkisessa hallinnossa on tunnistettu paljon teknologian hyödyntämisen mahdollisuuksia, mutta teknologian hyödyntäminen ei ole yhtä nopeaa kuin yksityisen sektorin organisaatiossa. Esimerkiksi tiedolla johtamisen ratkaisut ja menettelyt luovat paljon uusia mahdollisuuksia päätöksenteon tukemiseen, mutta haastattelujen perusteella niiden hyödyntäminen julkisessa hallinnossa on vielä melko alkuvaiheessa. Osittain teknologian hyödyntämistä jarruttavat muun muassa puuttuva teknologiaan liittyvä lainsäädäntö ja teknologiaosaamisen puute. Myös globaalit elektroniikkalaitteiden ja niiden komponenttien valmistus- ja toimitusviiveet voivat nousta joissain tapauksissa esteeksi teknologian nopealle hyödyntämiselle.

Jotta uutta teknologiaa voidaan hyödyntää uusien digitaalisten palveluiden kehittämiseen ja tietoturvan varmistamiseen, tulee organisaatiolla olla siihen riittävä osaaminen. Haastattelujen perusteella teknologian arvioinnin tulisi olla osa tiedonhallintalautakunnan tehtäviä. Uusia teknologioita syntyy jatkuvasti ja niistä pitäisi tunnistaa ne, joita voidaan hyödyntää julkisen hallinnon toiminnassa ja jotka on otettu yleisesti käyttöön muualla. Kaikkea uutta ei tule valjastaa heti julkisen hallinnon käyttöön vaan ne, joista on todistetusti hyötyä ja joita on otettu käyttöön jo esimerkiksi yksityisellä sektorilla. Tällä hetkellä koetaan, että tiedonhallintalautakunnan suositusten laatijalla ei välttämättä ole riittävää

osaamista, jotta johonkin teknologiaan liittyvää suositusta voitaisiin tehdä riittävällä tarkkuustasolla. Esimerkiksi suosituksen laadinta tekoälystä ja sen hyödyntämisestä voisi tämän myötä olla haasteellista.

Suositusten kirjoittajien pitäisi olla enemmän perillä uusista teknologioista sekä niiden tuomista mahdollisuuksista ja riskeistä. Haastattelujen mukaan eräänä keinona asian parantamiseen voisi olla lisätä julkisen hallinnon ja yksityisen sektorin toimijoiden välistä yhteistoimintaa. Tällä hetkellä välimatka yksityisen sektorin toimittajiin nähdään liian pitkänä. Tiedonhallintalautakunnan sihteeristön tulisi esimerkiksi osallistua teknologiatoimittajien ja -kehittäjien tilaisuuksiin nykyistä enemmän.

Julkisen hallinnon organisaatioille on tiettyjä toimijoita, jotka tarjoavat ICT-palveluita, mutta näiden osalta on havaittu epäselvyyttä siitä, kuka toimija tarjoaa mitäkin palvelua ja miltä toimijalta eri hallinnon organisaatioiden tulisi ensisijaisesti hankkia teknologiapalveluita. Keskusteluissa esiin nousivat muun muassa Valtorin, in-house-yhtiöiden, valtioneuvoston kanslian ja markkinatoimijoiden väliset epäselvyydet. Haastatteluissa ehdotettiin kehittämään palvelumalli, jossa kuvataan, kuka vastaa julkisen hallinnon toimikentässä digitaalisten palveluiden toimittamisesta sekä miten niihin liittyvät tiedonhallintalain mukaiset vastuut asettuvat. Julkisen hallinnon organisaatiot ovat myös osittain riippuvaisia sen palvelutoimittajien kyvykkyyksistä tarjota moderneja teknologisia ratkaisuja.

Julkisen hallinnon käyttämään teknologiaan vaikuttaa myös se, mitä digitaalisia palveluita kansainvälinen yhteistyö tuo mukanaan. Osa teknologioista ja digitaalisista palveluista tulee esimerkiksi EU:n yhteistoiminnassa annettuna, jolloin julkisen hallinnon organisaation täytyy huomioida niiden käyttämisessä tiedonhallintalain asettamat velvoitteet. Lisäksi EU:n sääntely on huomioitava tiedonhallintalain kehittämisessä, sillä nämä eivät saa olla ristiriidassa keskenään. Lisäksi teknologioita nousee käytettäväksi yhteiskunnan ilmiöiden myötä, kuten Covid-19 pandemian aiheuttama digiloikka etätyöskentelyyn ja Ukrainan kriisin nostama digitaalisen turvallisuuden painottaminen yrityksissä ja julkisen hallinnon organisaatioissa.

Näistä johtopäätöksenä voidaan todeta, että uusien teknologioiden kehittymisen seuranta ja arviointi tulisi olla systemaattinen osa julkisen hallinnon toimintaa, jotta teknologia hyödyntämisessä ei jäädä jälkeen ja niiden vaikutukset voidaan huomioida paremmin lainsäädännön, suositusten ja ohjeistusten kehittämisessä. Kun uusi teknologia tulee saataville, toiset organisaatiot saattavat ottaa sen nopeastikin käyttöön ja soveltaa sitä omassa toiminnassaan ja toiset organisaatio pidättäytyvät sen käyttämisestä, kunnes ohjeistus tai suositus on olemassa. Mikäli teknologiaan liittyviä suosituksia ei kehitetä, riskinä on, että organisaatioiden välille muodostuu kuiluja teknologioiden hyödyntämisessä ja se aiheuttaa myös erilaisia tulkintoja muun muassa lainsäädännön vaatimusten toteuttamisessa.

On myös huomioitava, että ennen syvempää teknologiakohtaista ohjeistamista tulisi ylemmän tason perusteet esimerkiksi yhteentoimivuuden osalta olla ohjeistettu riittävällä tasolla. Haastattelussa nostettiin esille ehdotus, jossa suositukset jaoteltaisiin esimerkiksi viiteen eri portaaseen ja ohjeistusta annettaisiin eri tasoilta, alkaen ylätason linjauksista syventyen tarkempiin teknologiakohtaisiin ohjeistuksiin. Näille portaille tulisi määrittää vastuulliset eli kuka suositusten ja ohjeiden kehittäjänä toimii. Nykyisellään esimerkiksi tiedonhallintalautakunnan sivuilta löytyvästä suosituslistauksesta on vaikea nopeasti sanoa, millä tasolla aihetta eri suosituksissa ohjeistetaan. Toiset ovat hyvinkin tarkkoja ja teknisiin menetelmiin painottuvia, toiset taas ylätason linjauksia aiheeseen liittyen.

Haastatteluissa nostettiin esille erityisesti kaksi kehittyvää teknologiaa, joilla arvioidaan olevan vaikutusta julkisen hallinnon digitalisaation kehittymiseen ja tietoturvallisuuteen. Nämä olivat tekoälyn hyödyntäminen ja kvanttilaskennan tuomat mahdollisuudet ja riskit.

4.4.1 Tekoälyn hyödyntämisen yleistyminen

Tekoälyllä tarkoitetaan tietojenkäsittelyn osa-aluetta, jossa tietojärjestelmä, sovellus tai laite suorittaa älykkyyttä vaativia tehtäviä ja käyttää perinteisesti ihmisen älyyn liitettyjä taitoja, kuten päättelyä, oppimista, suunnittelemista tai luomista. [6]

Koneoppiminen on yksi tekoälyn alaluokka, jossa tekoälysovellus muodostaa koneoppimisen mallin sille opetettavan datan perusteella. Koneoppimisen malleja hyödyntävät tekoälysovellukset voivat esimerkiksi tehdä päätöksiä erikseen määritellyistä asioista dataan pohjautuen. [7] Koneoppimisen järjestelmillä ja sovelluksilla voidaan helpottaa nykypäivänä esimerkiksi prosesseja, joissa ihmisen on aiemmin pitänyt tehdä yksinkertainen päätös pohjautuen johonkin tietoon. Päätöksentekoa on nykyisellään automatisoitu muun muassa Verohallinnossa ja Kansaneläkelaitoksessa ja ilmiö on yleistymässä julkisella ja yksityisellä sektorilla. [5]

Euroopan komissio on tehnyt vuonna 2021 ehdotuksen tekoälyn sääntelemiseksi, mutta sen käsittely on vielä kesken. Tekoälyyn keskittyvää kansallista lainsäädäntöä ei myöskään Suomessa ole vielä tällä hetkellä, mutta oikeusministeriön toimesta on aloitettu automaattista päätöksentekoa koskevan hallinnon yleislainsäädännön valmistelu. Haastattelujen mukaan tekoälyn käyttämisen sääntelyn pitäisi olla riittävän salliva, mutta samalla rajata pois riittävästi ei-toivottuja lieveilmiöitä. Sääntely koetaan haastavaksi, mutta esimerkiksi tekoälyn käyttämisen kieltäminen kokonaan tai sääntely tekeminen niin monimutkaiseksi ja hankalaksi, etteivät organisaatiot hyödyntäisi tekoälyn mahdollisuuksia, olisi väärä tapa edetä.

Hallituksen esitys julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi (145/2022 vp) on annettu eduskunnalle käsittelyyn 19.9.2022. Se sisältää lisäysehdotuksia muun muassa hallintolakiin. [5] Haastattelujen perusteella tiedonhallintalakia ollaan lisäksi kehittämässä tällä hetkellä huomioimaan tiedonhallinnan automatisoinnin asiat, jotka heijastuvat myös lain luvussa 4 asetettuihin tietoturvaan liittyviin vaatimuksiin. Tiedonhallintalautakunnan kehittämä oma suositus automaattisesta päätöksenteosta nähdään tarpeelliseksi. Automaattisen päätöksenteon ongelmina nähdään päätöksentekijän vastuun muodostuminen sekä päätöksenteon jäljitettävyys ja läpinäkyvyys hallinnon asiakkaalle. Nämä ongelmat ja haasteet tulisi huomioida suositusta kehitettäessä.

Haastattelujen mukaan julkisen talouden tasapaino ja Suomen kilpailukyky nojaavat pitkälti siihen, kuinka paljon pystymme hyödyntämään tekoälyä ihmistyön automatisoinnissa. Tekoälyn käyttöönoton nopeus ja soveltamisen monipuolisuus sekä laajuus tulevat kasvamaan julkishallinnon sektorilla, minkä vuoksi aiheeseen on herätty viime vuosien aikana. Tekoälyyn liittyviä julkisen hallinnon kehittämiä julkaisuja on jo olemassa jonkin verran ja useilta eri virastoilta. Esimerkiksi Kyberturvallisuuskeskus on julkaissut vuonna 2021 Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta -ohjeen. Lisäksi tekoälyn hyödyntämiseen liittyviä hankkeita on jo käynnissä, kuten Kansallinen tekoälyohjelma Aurora AI. Ohjelmassa kehitetään teknisiä ja toiminnallisia ratkaisuja sille, miten julkinen hallinto kykenisi tulevaisuudessa tekoälyavusteisesti helpottamaan ihmisten palveluiden saamista elämän eri tilanteissa ja tapahtumissa [4].

Haastatteluissa nousi esille myös hyökkääjän näkökulma teknologian hyödyntäjänä. Tekoälyn ja koneoppimisen menetelmiä hyödyntävät verkkorikolliset ja muut vihamieliset toimijat. Hyökkääjät käyttävät automatisoituja ja oppivia järjestelmiä omassa toiminnassaan, minkä vuoksi myös julkisen hallinnon täytyy hyödyntää tekoälyn ja koneoppimisen ratkaisuja hyökkäyksiltä puolustautumiseen, havainnointiin ja palautumiseen. Eräänä esimerkkinä nostettiin esille deepfake-sisältö. Deepfake-sisällössä käytetään tekoälyn ja koneoppimisen menetelmiä esittämään esimerkiksi valheellista, mutta realistista videokuvaa ja ääntä jostain henkilöstä. Tällaista voidaan käyttää esimerkiksi informaatiovaikuttamiseen, josta esimerkkinä on Venäjän kehittämä valheellinen deepfake-video Ukrainan presidentistä, jossa hän pyytää kansalaisiaan antautumaan. Tekoälyllä ja koneoppimisella on siis merkittävä vaikutus julkisen hallinnon digitalisaation kehittymiselle ja sen mahdollisuuksia ja haasteita tutkitaan parhaillaan useissa hankkeissa.

4.4.2 Kvanttilaskennan kehittyminen

Kvanttilaskenta mahdollistaa uusia innovaatioita tulevaisuudessa, mutta tuo mukanaan myös uusia riskejä, joita on jo tänä päivänä syytä huomioida. Kvanttilaskentaan käytetään kvanttitietokoneita, jotka ovat moninkertaisesti nykyisiä supertietokoneita tehokkaampia.

Niillä voidaan ratkaista ongelmia, joiden suorittamiseen nykyisillä tietokoneilla kestäisi jopa tuhansia vuosia. Tällainen ennennäkemätön laskentateho vaikuttaa väistämättä myös kyberturvallisuuteen, esimerkiksi salaamismenetelmiin ja niiden purkumekanismeihin. Kvanttitietokoneita on ollut kehitteillä jo jonkin aikaa, mutta niiden käytön yleistymiseen voi mennä vielä useita vuosia. Tulevaisuudessa kvanttitietokoneita voidaan käyttää esimerkiksi virusten tai lääkeaineiden tarkkaan mallinnukseen tai materiaalien suunnitteluun, mikä nykyisillä menetelmillä olisi mahdotonta. [1].

Kvanttilaskennan aiheuttama uhka nykyisille salausmenetelmille tulee huomioida myös julkisessa hallinnossa. Nykyaikaisten salausten purkaminen voi aiheuttaa merkittäviä seuraamuksia yhteiskunnan turvallisuuteen. Salausten purkumenetelmien mahdollistuminen ja yleistyminen kvanttilaskennan avulla lisää salassa pidettävään tietoaineistoon kohdistuvien tietomurtojen mahdollisuutta. Nykypäivänä turvallisesti salatut tiedostot ja yhteydet eivät välttämättä ole enää tulevaisuudessa riittävän turvallisia estämään ulkopuolisten pääsyä salattuun tietoaineistoon [2]. Tämän myötä muun muassa NIST[1] on kehittänyt salausmenetelmiä, jotka kestävät tulevaisuuden kvanttilaskennan aiheuttaman uhan salauksen purkamiselle. NIST:n kehittämä standardi sisältää neljä algoritmia, joita voidaan käyttää yleiseen salaukseen ja digitaaliseen allekirjoitukseen. Standardin valmistumisen arvioidaan kestävä vielä noin kaksi vuotta. [3]

Vaikka kvanttilaskenta on vielä kehittyvä teknologia, sen uhat tulisi huomioida jo tämän päivän suosituksissa. Nykyisissä suosituksissa ei juurikaan ole käsitelty kvanttilaskennan aihetta muuta kuin yksittäisenä ilmiönä ilman tarkempaa analysointia ja ohjeistusta. Julkisessa hallinnossa kvanttilaskenta tulisi huomioida erityisesti salausmenetelmien ja sähköisen allekirjoituksen suositusten kehittämisessä. Haastatteluissa nousi esille tarve sähköisen allekirjoituksen ohjeistamisesta julkisessa hallinnossa, jossa tulisi ottaa kantaa myös kvanttilaskennan aiheuttamiin uhkiin ja mahdollisuuksiin. Eräänä riskinä tunnistettiin se, että sähköisesti allekirjoitettuja asiakirjoja voitaisiin väärentää kvanttilaskennan menetelmiä hyödyntäen.

4.4.3 Uuden teknologian riskit ja mahdollisuudet

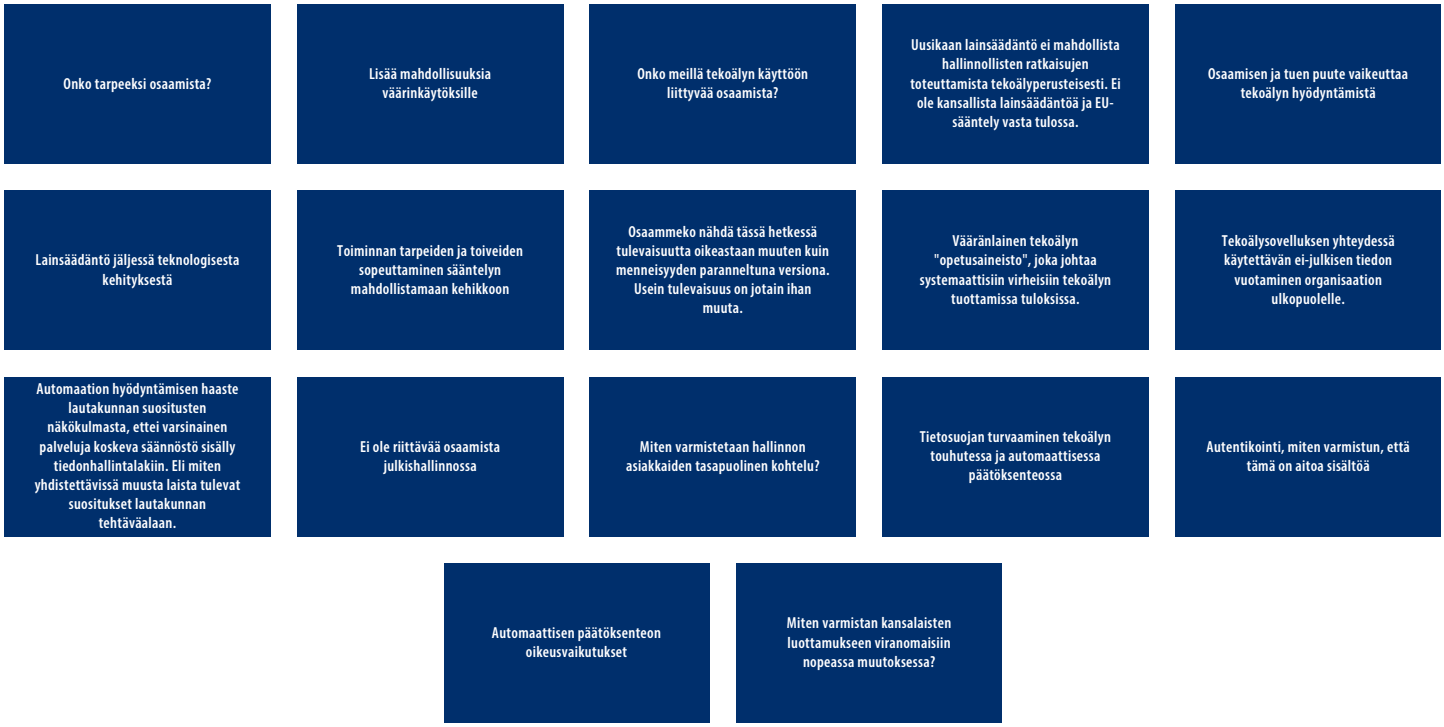
Työpajassa tunnistettiin kuviossa 12 esitetyt mahdollisuudet uuden teknologian hyödyntämiselle julkisessa hallinnossa. Mahdollisuuksista työpajassa nousi esille muun muassa tehokkaampi palveluohjaus tekoälyn avulla, sisäisen prosessien automatisointi, tuottavuuden ja tehokkuuden lisäys yleisesti sekä älykkäämmät tietoturvaratkaisut.

1 National Institute of Standards and Technology https://www.nist.gov/

Kuvio 12. Uuden teknologian hyödyntämisen mahdollisuudet

Uuden teknologian osalta riskeiksi ja haasteiksi julkisessa hallinnossa tunnistettiin kuviossa 13 esitetyt aiheet. Riskien ja haasteiden osalta työpajassa nousi esille muun muassa teknologiaan liittyvän osaamisen puutteet, puuttuva ja jälkeen jäänyt lainsäädäntö, ei-julkisen tiedon vuotaminen tekoälysovellusten kautta sekä tekoälyn vääränlaisen opetusaineiston käyttö.

Kuvio 13. Uuden teknologian tuomat riskit ja haasteet



Suositusten kehittämisen ehdotuksissa korostuivat tekoälyn käytön huomioiminen kaikissa suosituksissa ja ohjeissa, kvanttilaskennan tuomien riskien huomiointi nykyisissä salausmenetelmien ohjeissa sekä pilottityyliset ohjeet uusien teknologioiden hyödyntämisestä. Kuviossa 14 on esitetty yhteenveto työpajassa esitetyistä ehdotuksista.

Kuvio 14. Ehdotukset suositusten kehittämiseen uuden teknologian hyödyntämiseen liittyen

Yhteenvetona suosituksen kehittämiselle tulisi huomioida seuraava asiat:

- Ohjeistus salausmenetelmistä, jotka kestävät myös kvanttilaskennan tuomat riskit.
- Suosituksissa tulisi pystyä huomioimaan kaikkien lakien säädökset uuteen teknologiaan liittyen.
- Todentamiseen liittyvät ohjeistukset. Erityisesti kuinka todentamisen avulla voidaan varmistaa luotettavuus eri tilanteissa. Lisäksi lohkoketjujen hyödyntäminen todentamisessa tulisi huomioida suositusten kehittämisessä.
- Tekoälyn hyödyntämiseen liittyvät ohjeistus, jossa huomioitu myös ei-julkisen tiedon käytön rajoitteet ja riskit.
- Yleisesti se, kuinka osaamisen kehittäminen varmistetaan uuden ja kehittyvän teknologian osalta.

5 Ehdotukset suositusten kehittämiseen

5.1 Suositusten ja ohjeistusten kehittäminen yleisesti

Selvitystyön haastatteluissa ja työpajassa tuotiin esille useita ehdotuksia olemassa olevien ja uusien suosituksien kehittämiselle. Selvitystyössä kartoitettujen olemassa olevien ohjeiden ja suositusten määrä on suuri, ja niitä tuottavat useat eri julkisen hallinnon organisaatiot. Havaintona todettiin, että tarvitaan uusia menetelmiä, joilla ajantasainen ohjeistus olisi jatkossa helposti löydettävissä eri hallinnon organisaatioille esimerkiksi yhdestä keskitetystä paikasta. Tällöin esimerkiksi hyvinvointialueet voisivat löytää heitä velvoittavat tietoturvan julkisen hallinnon ohjeistukset ja muut ohjeet oman toimintansa tietoturvallisuuden kehittämiseen yhdestä paikasta. Myös toimialakohtainen ohjeistus tulisi löytyä samasta paikasta, jotta ohjeet eivät hajaantuisi useiden ohjeistavien organisaatioiden sivustoille. Menetelmän kehittämisessä on huomioitava, että suositusten ja ohjeistusten ajantasaisuutta seurataan ja ylläpidetään. Tämä edesauttaisi myös ohjeistuksia luovia organisaatiota varmistamaan, että samoja asioita ei käsitellä useissa eri ohjeissa päällekkäin.

Haastattelujen mukaan tiedonhallintalautakunnan suositusten kehittämisessä on varmistettava, että suositukset ja ohjeet soveltuvat kaikille hallinnon organisaatiolle. Eräänä konkreettisena erimerkkinä mainittiin, että tietyt turvallisuusviranomaiset voivat kokea, että heidän datansa on kriittisempää, eivätkä he sen vuoksi käytä pilvipalveluina toimitettavia julkisen hallinnon palveluita, vaikka suositukset tai ohjeistukset näin kehottaisivat. Mikäli julkisessa hallinnossa ohjeistetaan käyttämään jotain uutta teknologiaa tai menetelmää, sen pitäisi koskettaa kaikkia hallinnon organisaatioita. Suositusten avulla tulisi pyrkiä myös tehostamaan tiedonvaihtoa ja siihen liittyvää turvallisuutta esimerkiksi ohjeistamalla sähköisen allekirjoituksen käyttöä julkisessa hallinnossa ja yleisesti turvallisen tiedonvaihdon menetelmiä.

Haastattelujen mukaan tiedonhallintalautakunta on luonut eri jaostojen kautta useita suosituksia eri tiedonhallintalain kappaleista. Ongelmaksi on tunnistettu se, että useat suosituksissa ohjeistettavat asiat läpileikkaavat koko tiedonhallintalain ja sen eri luvuissa kuvatut asiat. Tämän myötä tiedonhallintalautakunnan suosituksissa tulee varmistaa, että ne huomioivat koko tiedonhallintalain eri osa-alueet jaostokohtaisuuden sijaan. Suositusjärjestelmää tulee siis yhdenmukaistaa ja arvioida, miten koko lain asiat huomioidaan jatkossa suositusten luomisessa ja päivittämisessä. Keskeistä on varmistaa, että lain soveltajat ymmärtävät suositusten perusteella huomioida kaikki tiedonhallintalain kohdat.

Haastatteluissa nousi myös kehitettäväksi asiaksi suositusten kohderyhmien arviointi. Suositusjärjestelmän kehittämisessä tulisi arvioida, olisiko suosituksia syytä tehdä enemmän toimialakohtaiseen soveltamiseen tai tuoda esimerkiksi yhteisiin suosituksiin toimialakohtaisia ohjeita tai soveltamisen esimerkkejä. Useammassa haastattelussa nousi esille erityisesti tiedonhallintalain soveltamistapojen kuvaaminen esimerkkien avulla. Suositusten kehittämisessä tulisi arvioida, kuinka hyvin ne palvelevat esimerkiksi kuntaa, ja mahdollisesti osallistaa suosituksen kohdeorganisaatioita ja hyödyntäjiä niiden kehittämiseen. Tällöin suosituksen kirjoittajalla olisi parempi ymmärrys siitä, kuinka suositusta halutaan käyttää kohdeorganisaatiossa ja millaisiin asioihin tulisi erityisesti kiinnittää huomiota. Yhteenvetona suositusten kehittämisen tulisi olla nykyistä asiakaslähtöisempää. Hyvänä esimerkkinä onnistuneesta, useat toimialat huomioivasta suosituksesta nostettiin esille Julkri.

Suositusten kehittämiseen ja kirjoittamiseen tulisi haastattelujen perusteella osallistaa myös eri yrityksistä hankittuja asiantuntijoita esimerkiksi suosituksessa käsiteltäviin teknologioihin liittyen. Tämä pienentäisi tunnistettua teknologiaosaamisen vajetta nykytilanteeseen nähden.

Haastatteluissa tuotiin ilmi, että suositusten ja ohjeiden laatijoiden roolit eivät ole täysin selviä ja että toimivaltuuksiin liittyy rajoituksia. Viranomainen voi antaa suosituksia vain sille säädettyjen tehtävien alalta. Erityisesti DVV:n rooli jäi haastattelujen perusteella epäselväksi: mistä asioista, kenelle ja mihin pohjautuen DVV:n tulisi luoda ohjeita ja suosituksia? Tämän ja muiden suositusten ja ohjeiden laatijoiden roolien ja tehtävien kirkastaminen selkeyttäisi vastuiden jakautumista ja osaltaan varmistaisi, että asioista ei ohjeisteta useampaan kertaa eri ohjeissa. Kehitysehdotusta arvioitaessa on myös huomioitava, että voi olla tarkoituksenmukaista tehdä samasta aiheesta useampi eri ohje, mikäli ne tehdään selkeästi eri näkökulmista tai kohdennettuna esimerkiksi tiettyyn toimialaan.

Digi- ja väestötietovirastolle tehdyssä haastattelussa mainittiin ehdotuksena heidän kehitteillä oleva nelimalliarviointitapa, jossa muutoksia arvioidaan aina tiedon, tiedonhallinnan, käsittelyprosessin ja tietojärjestelmien näkökulmasta. Tätä suositeltiin käytettäväksi myös uusien julkisen hallinnon suosituksien kehittämisessä, jotta suositeltavaa asiaa ohjeistettaisiin riittävissä määrin tiedonhallinnan eri näkökulmista. Suosituksissa tulisi myös huomioida tiedon kriittisyystasot. Jos kyseessä on arkaluonteista tietoa sisältävä järjestelmä, erilaisia soveltamistulkintoja ei saisi syntyä. Jos taas kyseessä on järjestelmä, joka sisältää esimerkiksi julkista tietoa, voisivat erilaiset tulkinnat olla sallittuja riskiarvioon pohjautuen. Lähtökohtaisesti riskipohjainen arviointi nähdään hyvänä käytäntönä tulkintaan.

Tietoturvallisuuteen liittyvien suositusten kehittämisessä on huomioitava, että kaikkea ei ole mahdollista suojata parhaalla mahdollisella tavalla, jolloin riskipohjaisuutta tulee korostaa. Tämän myötä tarvitaan yhteiset tulkinnat hyväksyttävistä jäännösriskeistä.

Nykyisissä suosituksissa tulisi olla valmiina esimerkkejä hyväksyttävistä jäännösriskeistä tietoturvan ja tietosuojan osalta. Tämä mahdollistaisi ohjeiden paremman tulkinnan ja tekisi niistä konkreettisempia. Erääksi ongelmaksi haastatteluissa mainittiin se, että eri organisaatiolla on käytettävissä eritasoiset resurssit ja rahat, jonka myötä riskiarvioiden tuloksetkin ovat erilaiset ja päätökset teknologian käytöstä poikkeavat organisaatioiden välillä.

Suositusten laadinnassa on huomioitava tarkkaan sanasto ja se, mitä eri käsitteillä tarkoitetaan. Jos esimerkiksi suosituksessa puhutaan tekoälystä tai pilvipalvelusta, tulisi määritellä selkeästi mitä sillä ohjeessa tarkoitetaan, koska käsitteet itsessään ovat laajoja ja voivat aiheuttaa erilaisia tulkintoja. Tietyt käsitteet koettiin ongelmallisiksi senkin vuoksi, että ne jakavat suosituksia liikaa tiettyihin näkökulmiin, esimerkiksi jaotteluun pilvipalveluiden ja ei-pilvipalveluiden välillä.

Työpajassa arvioitiin, mitkä ovat keskeisimmät ongelmat nykyisissä suosituksissa ja niiden vaikuttavuudessa. Työpajan tulokset tähän kysymykseen on esitetty kuviossa 15. Työpajassa nousivat esille suositusten ongelmista niiden päällekkäisyydet, jaoston toiminnan rajallisuus, suositusten tunnettavuuden haasteet, valmisteluun tarvittavien resurssien vajaukset ja käyttäjälähtöisyyden puute. Keskustelussa ehdotettiin myös muita muotoja suositusten viestimiseen ja kouluttamiseen, kuten esimerkiksi videokoulutuksia.

Kuvio 15. Nykyisissä suosituksissa koetetut ongelmat

5.2 Suositusten vaikuttavuuden kehittäminen

Haastattelussa selvitettiin eräänä teemana suositusten vaikuttavuuden kehittämistä. Vastausten perusteella suosituksien ja ohjeistuksien tulisi helpottaa ja yksinkertaistaa toimintaa eikä tehdä siitä vaikeampaa. Suositusten tulisi ohjeistaa selkeästi soveltajaa toteuttamaan tiedonhallintalaissa esitetyt velvoitteet niin, että se on kyseiselle organisaatiolle helppoa, tehokasta ja selkeää. Viranomaisen harkintavalta mahdollistaa lain soveltamisen useilla eri tavoilla, jonka vuoksi esimerkkien käyttäminen ohjeissa voisi selkeyttää, helpottaa ja yhtenäistää soveltamista sekä vähentää erilaisia tulkintoja. Suositusten tulisi olla helppolukuisia ja niitä lukemalla pitäisi pystyä soveltamaan lakia ja hoitamaan lain velvoitteet omassa organisaatiossa. Haastatteluissa korostuivat termit täsmällisyys, selkeys, helppous, konkreettisuus ja esimerkeillä kuvaaminen sekä käyttötapausten kuvaaminen. Tarvittaessa toimiala- ja tyyppikohtainen sovitus nähtiin suositeltavaksi menetelmäksi.

Useammassa haastattelussa mainittiin keväällä 2022 julkaistu Julkri, joka koettiin hyvänä ja laajana ohjeena tietoturvan ja tietosuojan vaatimusten määrittelyyn. Suositus käsittelee tietoturvan lisäksi muun muassa jatkuvuuden, varautumisen ja tietosuojan vaatimuksia, mikä vaikuttaa olevan harvinaista tiedonhallintalautakunnan toimintakenttä huomioiden. Tiedonhallintalautakunnan tehtävänä on ohjeistaa tiedonhallintalakiin liittyviä asioita eikä esimerkiksi tietosuojan asioita. Tämä rajaus nähtiin useammassa haastattelussa ongelmaksi, koska tiedonhallintalain soveltamisessa tulisi huomioida myös muita lakeja ja ohjeistuksia. Toisin sanoen suositusten tulisi olla jatkossa laaja-alaisempia ja esimerkiksi tietoturvallisuusjaoston kehittämien suositusten tulisi kattaa koko tiedonhallintalain asiat sekä muu asiaan liittyvä lainsäädäntö.

Tiedonhallintalautakunnan suositusten ongelmaksi nähtiin yleisesti niiden tunnettavuus ja vaikuttavuus. Tiedonhallintalautakunnan suositusten vaikuttavuutta tulisi yleisesti parantaa ja esimerkiksi Julkrin käyttämistä julkisen hallinnon organisaatiossa pyrkiä aktiivisemmin edistämään. Haukka-hankkeessa tehdyssä selvityksessä tutkittiin kahden Vahti-ohjeen ja kahden tiedonhallintalautakunnan suosituksen vaikuttavuutta. Näiden vaikuttavuuden pisteet olivat 2.2–4.3, kun 10 oli paras arvo [20].

Huonon vaikuttavuuden syihin lukeutui muun muassa se, että ohjetta ei tunneta riittävästi tai organisaatiolla oli jo olemassa oma ohjeistus aiheeseen. Uusien suosituksien luomisen ohella tulisi siis yleisesti edistää jo olemassa olevien suositusten tunnettavuutta ja vaikuttavuutta. Suositusten vaikuttavuuden arvioinnin pitäisi olla säännöllistä ja selkeä osa tiedonhallintalautakunnan toimintaa. Suositusten vaikuttavuutta arvioitaessa tulisi myös pohtia, vastataanko suosituksilla oikeasti merkittävimpiin tietoturvan uhkiin ja riskeihin.

Työpajassa arviointiin, kuinka suositusten vaikuttavuutta voidaan kehittää. Kuviossa 16 on esitetty työpajassa esille nousseet ajatukset. Tulosten mukaan suositusten kehittämistä voitaisiin edistää lisäämällä niihin liittyviä koulutusmuotoja, luomalla niistä selkeämpiä, osallistamalla käyttäjäorganisaatioita vahvemmin niiden kehittämiseen, hyödyntämällä palvelumuotoilua, testaamalla ohjeistuksia ja suosituksia joissain organisaatiossa sekä yleisesti paremmalla viestinnällä.

Kuvio 16. Ehdotukset suositusten vaikuttavuuden kehittämiselle

5.3 Kehitysehdotukset olemassa oleviin suosituksiin

Työn yhtenä tavoitteena oli tunnistaa kehittämisehdotuksia luvussa 2 kuvattuihin tietoturvallisuusjaoston laatimiin suosituksiin. Seuraavissa alikappaleissa on kuvattu suositus-kohtaisesti tunnistettuja kehittämistoimenpiteitä näihin liittyen. Ehdotukset pohjautuvat selvitystyön haastatteluihin, työpajaan ja muihin työssä syntyneisiin havaintoihin.

5.3.1 Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta, VM 2021:65

Suosituskokoelma kattaa laaja-alaisesti tiedonhallintalain luvun 4 säädökset ja useita tietoturvallisuuden osa-alueita, minkä vuoksi siihen kohdentui eniten kehittämisehdotuksia. Tämän selvityksen haastattelujen, työnpajan ja muiden työn tulosten pohjalta tunnistettiin seuraavat suosituksen kehittämisehdotukset.

1. **Toimitilaturvallisuuden ohjeistuksen lisääminen.** Nykyiset toimitilaturvallisuuden ohjeet eivät huomioi riittävissä määrin nykyaikaisia työskentelymalleja kuten etätyöskentelyä ja monipaikkaista työskentelyä. Suosituksen luvussa 11.3 ”Vahingoilta suojaaminen ”viitataan VAHTI 2/2013 Toimitilojen tietoturvaohjeeseen, joka sisältää osittain vanhentunutta tietoa. Tässä selvitystyössä ehdotetaan myös uuden suosituksen, jossa etätyöskentelyn ja monipaikkaisen työskentelyn mallit on huomioitu, luomista toimitilaturvallisuuden asioille. Mikäli kyseinen suositus luodaan, tulee suosituskokoelmassa viitata siihen ja poimia sieltä keskeisimmät asiat. Uuden toimitilaturvallisuuden suosituksen tulisi kuvata, kuinka etätyöskentelymalli tai monipaikkaisen työn malli otetaan käyttöön tiedonhallintayksikössä, ja sisältää tarkastuslistat eri työskentelymallien ympäristöille. Tässä on syytä kuvata myös teknisiä tietoturvan kontrolleja esimerkiksi väärinkäytösten ehkäisemiseen nykyaikaisiin työskentelymuotoihin liittyen.
2. **Riippuvuudet kriittisestä infrastruktuurista.** Suosituksessa tulisi ohjeistaa tiedonhallintayksiköitä ottamaan huomioon riippuvuudet kriittisen infrastruktuurin palveluista varautumisen näkökulmasta. Näistä selvitystyön aikana esille nousivat erityisesti ulkomaan tietoliikenneyhteyksien riippuvuudet. Luvussa 11.5 ”Saatavuuden ja käyttökelpoisuuden varmistaminen” kuvataan saatavuuteen liittyviä huomioita, mutta sisältöä voisi päivittää ohjeistamalla arvioimaan kriittisen infrastruktuurin palveluiden tarpeellisuutta eri skenaarioissa. Kansainvälisten tietoliikenneyhteyksien riippuvuudesta ja merkityksestä voisi ohjeistaa myös luvussa 9 ”Tietojen siirtäminen yleisessä tietoverkossa”.
3. **Palvelu- ja toimitusketjuhyökkäysten huomiointi.** Suosituksessa tulisi ohjeistaa huomioimaan vahvemmin palvelu- ja toimitusketjuihin liittyvien riskien arviointia. Näistä tulisi kuvata, mitä kyseiset riskit yleisesti ovat, ja muodostaa ohjeistuksia sille, kuinka niiltä voidaan suojautua ja kuinka riskit otetaan huomioon tiedon elinkaaren eri vaiheissa sekä esimerkiksi hankinnoissa. Päivitys tulisi kohdentaa lukuihin 5 ”Tiedon elinkaaren huomioiminen tietojärjestelmissä” ja lukuun 8 ”Tietoturvallisuus tietojärjestelmähankinnoissa”.

4. **Salausmenetelmien huomiointi tiedon säilytyksessä.** Suosituksen luvussa 4.3 ”Tiedon säilytys” on kuvattu hyvin yleisesti tiedon tallentamisen salausmenetelmiä. Luvussa olisi syytä huomioida nykyisiin salausmenetelmiin liittyvät riskit ja ohjeistaa käyttämään sellaisia salausmenetelmiä, jotka kestävät esimerkiksi kvanttilaskennan tulevaisuudessa tuomat uhat. Vaikka kvanttilaskennan vaikutukset realisoituvat vasta tulevaisuudessa, on sen salausten purkumahdollisuudet huomioitava jo tämän päivän tiedon salaamisessa. Suosituksessa viitataan VAHTI 2/2015-ohjeeseen salauskäytännöistä, jonka lisäksi voisi olla hyödyllistä viitata Kyberturvallisuuskeskuksen hyväksymään salausratkaisujen ohjeeseen.
5. **Vastaanottajan tunnistamiseen ja todentamiseen liittyvät ohjeistukset**. Vastaanottajan tunnistamiseen liittyvää ohjeistusta on kuvattu suosituksen luvussa 10. Selvityksen aikana nostettiin useamman kerran esille haasteet käyttäjän luotettavassa tunnistamisessa esimerkiksi videoneuvotteluyhteyksissä. Suosituksen päivittämisessä tulisi huomioida tämä haaste ja ohjeistaa, kuinka videoneuvotteluissa osallistujien identiteetti varmistetaan sekä kuinka esimerkiksi tekoälyn tuomilta uhkilta (esimerkiksi deepfake-videokuvan käyttö) voidaan suojautua. Lisäksi suosituksen päivittämisessä tulisi arvioida lohkoketjuteknologioiden tuomien mahdollisuuksien käyttöä todentamisen kehittämisessä.
6. **Ohjeistus yleisimmiltä tietoturvahyökkäyksiltä suojautumiseen**. Suosituksessa ei oteta kantaa siihen, kuinka tiedonhallintayksiköiden tulisi suojautua yleisimmiltä kyberhyökkäyksiltä. Ehdotuksena on lisätä suositukseen ohjeita erilaisiin hyökkäyksiin ja tietomurtoyrityksiin, joita ovat esimerkiksi kiristyshaittaohjelmat, palvelunestohyökkäykset, tietojen kalastelu ja muut yleisesti käytettävät hyökkäysmenetelmät, varautumiseen ja niiltä suojautumiseen. Lisäksi on syytä arvioida, tulisiko ohjeistuksen olla osa tätä suositusta vai tulisiko tehdä mahdollisesti oma erillinen suositus aiheesta ja viitata siihen tässä suosituksessa. Mikäli uusi suositus luodaan, tulisi siinä ottaa kantaa myös Zero Trust -mallin, joka nousi selvitystyön aikana useamman kerran esille, käyttämiseen. Lisäksi on syytä harkita valkohattuhakkereiden ja bug bounty -ohjelmien hyödyntämisen ohjeistamista tai viitata näihin liittyviin Kyberturvallisuuskeskuksen ohjeisiin.

5.3.2 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä, VM 2021:5

Turvallisuusluokiteltavien tietojen käsittely etätyössä ja monipaikkaisessa työskentelytilassa nousi keskeisimmäksi haasteeksi suositukseen liittyen. Seuraavassa on kuvattu tunnistetut ehdotukset suosituksen kehittämiselle.

1. **Etätyön ja monipaikkaisen työn huomiointi.** Suosituksen luvussa 6 käsitellään asiakirjojen käsittelyä turvallisuusalueiden avulla. Suosituksessa ei ohjeisteta, kuinka turvallisuusluokiteltua tietoaineistoa käsitellään etätyön tai monipaikkaisen työskentelyn malleissa. Suositukseen tulisi kuvata näihin liittyvät toimintatavat ja vaatimukset. Tässä selvitystyössä suositellaan myös erillisen toimitilaturvallisuuteen keskittyvän suosituksen laatimista. Mikäli tällainen luodaan, tulee tähän suositukseen poimia siitä keskeiset huomioitavat asiat.
2. **Auditointien ja arviointien huomiointi suosituksessa.** Työpajassa nostettiin esille auditoinnin haasteet erityisesti pilviympäristöihin liittyen. Vaikka huomio kohdentui pilviympäristöihin, on syytä harkita, tulisiko suosituksessa turvallisuusluokiteltavien asiakirjojen käsittelystä ohjeistaa myös auditointeihin ja arviointeihin liittyvistä asioista. Ohjeistettavia asioita voisivat olla esimerkiksi, milloin ja missä tapauksessa tietojenkäsittely-ympäristöt tulee auditoida ja missä muodossa ja laajuudessa sekä kenen toimesta näitä tulee toteuttaa. Suosituksessa tulisi vähintään viitata Katakriin ja PiTuKriin sekä kuvata, missä tilanteissa niitä hyödynnetään.

5.3.3 Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa, VM 2022:4

Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa -suosituksen kehittämisehdotukset pohjautuvat selvitystyön haastatteluissa ja työpajassa nousseisiin huomioihin. Koske aihe on ajankohtainen, kehittämisehdotuksia nousi esille useita ja valtaosa niistä kohdentui ohjeiden ja suosituksen konkretian kehittämiseen. Seuraavassa on kuvattu ehdotukset suosituksen kehittämiselle.

1. **Ohjeistukset sopimusten laadinnasta julkisten pilvipalvelutarjoajien kanssa.** Suosituksen luvussa 5 käsitellään pilvipalveluihin liittyviä palvelusopimusasioita. Selvityksen aikana nousi esille useita tarpeita suosituksille ja ohjeille sopimusten laadinnasta julkisten pilvipalveluiden tarjoajien kanssa. Nykyinen ohjeistus kuvaa sopimuksissa huomioitavia asioita ylätasolla, mutta sitä voisi tuoda nykyistä konkreettisemmalle tasolle ja tuoda esille mahdollisesti tähän liittyviä esimerkkejä sopimusten

laadinnan tueksi. Suosituksessa voisi myös viitata valtiovarainministeriön julkaisemaan pilvipalvelujen soveltamisohjeeseen, Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille (VM 2020:73), jossa on lisää ohjeistusta sopimusten laadintaan. On hyvä arvioida, olisiko aiheesta syytä tehdä myöhemmin oma erillinen suositus, jossa voisi olla mukana esimerkiksi sopimuspohjia tukemaan julkisten pilvipalveluiden käyttöönottoa. Suosituksessa tulee myöhemmin huomioida myös valtiovarainministeriön Cirrus-hankkeen lopputulokset, jotka ovat odotettavissa vuoden 2023 loppuun mennessä hankkeen päättyessä.

2. **Konkreettiset työvälineet pilvipalveluiden arviointiin.** Selvityksen aikana nykyisten pilvipalveluiden ohjeistuksien keskeiseksi haasteeksi mainittiin konkretian puute. Suosituksen kehittämisessä tulisi arvioida, voidaanko sen osaksi tuoda selkeitä työvälineitä pilvipalveluiden turvallisuuden arvioinnin tueksi. Näitä voisivat olla esimerkiksi tarkastuslista palvelun turvallisuuden varmistamiseksi, riskiarviointipohja ja esimerkit hyväksytyistä jäännösriskeistä. Valtiovarainministeriön julkaisu Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille (VM 2020:73) kuvaa osittain näitä työvälineitä, joten siihen viittaaminen on suositeltavaa. Konkreettisena työvälineenä pilviympäristöjen käyttöönotolle voisi olla esimerkki referenssiarkkitehtuurista, jossa täyttyvät turvallisuusluokka IV-tason vaatimukset.
3. **Tiedonhallintayksikön ja pilvipalvelutarjoajan vastuiden ohjeistus.** Eräänä suositusten kehittämiskohteena nousi esille ohjeistaminen vastuista tiedonhallintayksikön ja pilvipalvelutarjoajan välillä. Suosituksessa tulisi kuvata, mitkä ovat kunkin osapuolen vastuut yleisesti ja kuinka nämä tulee huomioida pilvipalvelun käyttöönotossa. Ohjeistuksissa voisi viitata julkisten pilvipalvelutarjoajien ”shared responsibility model” -malleihin, joissa asiakkaan ja palvelutoimittajan väliset vastuut kuvataan eri pilvipalveluiden tasoilla.
4. **Auditointien ja arviointien huomiointi suosituksessa.** Työpajassa nostettiin esille auditoinnin haasteet erityisesti pilviympäristöihin liittyen. Suosituksessa tulisi antaa ohjeita siitä, miten pilvipalvelun tarjoajaa ja sen palvelua tulisi auditoida ja millaisissa tilanteissa auditointi on tarpeellinen.

5.3.4 Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), VM 2022:43

Selvitystyössä tunnistettiin muutamia kehittämiskohteita Julkrin kehittämiseen, vaikka suositus oli melko tuore ja kattoi laajasti eri kriteeristöjen vaatimuksia. Keskeisimmät havaitut kehittämiskohteet liittyvät varautumisen vaatimuksiin ja fyysisen turvallisuuden vaatimuksiin.

1. **Varautumisen ja jatkuvuudenhallinnan vaatimukset.** Julkrin vaatimuksissa on tällä hetkellä 12 varautumisen ja jatkuvuudenhallinnan vaatimusta. Muihin vaatimusryhmiin verrattuna vaatimuksia on selkeästi vähemmän, minkä vuoksi on syytä arvioida, onko nykyinen vaatimusmäärä riittävä kaikkien varautumiseen liittyvien asioiden huomioinnille kriteeristössä. Tässä selvitystyössä ehdotetaan uuden suosituksen laadintaa varautumiseen ja jatkuvuudenhallintaan. Mikäli suositus luodaan, tulee Julkrissa viitata siihen ja poimia sieltä kriteeristöön uudet varautumisen ja jatkuvuudenhallinnan vaatimukset.
2. **Etätyön ja monipaikkaisen työn vaatimusten huomiointi.** Julkrissa on laajasti vaatimuksia fyysisen turvallisuuden osa-alueelle. Vaatimukset eivät kuitenkaan suoraan ota kantaa etätyön ja monipaikkaisen työskentelyn ehtoihin. Julkrin päivittämistä suunniteltaessa on pohdittava, tuodaanko kriteeristöön vaatimuksia, joissa huomioidaan etätyöpisteen tai monipaikkaisen työskentely-ympäristön turvallisuusvaatimukset.

5.4 Ehdotukset uusille tiedonhallintalautakunnan suosituksille

Selvitystyössä nousi esille useita ehdotuksia ja tarpeita uusille suosituksille. Näitä olivat muun muassa suositus sähköisestä allekirjoituksesta, suositus automaattisesta päätöksenteosta ja suositus häiriötilanteiden hallintaan. Työpajan yhtenä pääaiheena oli suositusten kehittäminen yleisesti, ja osallistujilta kysyttiin tarpeita uusille suosituksille. Työpajassa nousseet ajatukset uusista suosituksista on esitetty kuviossa 17.

Kuvio 17. Tarpeet uusien suositusten kehittämiselle

Työpajan huomioissa korostuivat eheyteen ja saatavuuteen keskittyvät suositusehdotukset sekä suosituskokonaisuuden käytön ohjeistaminen. Uusia suositusehdotuksia on osittain kuvattu myös luvun 4 aihealuekohtaisissa kappaleissa, jotka käsittelevät työpajassa esille nousseita ajatuksia. Seuraavissa kappaleissa on kuvattu tarkemmin ehdotukset uusista suosituksista.

5.4.1 Suositus toimitilaturvallisuudesta

Selvitystyön yhtenä pääaiheena oli etätyö ja monipaikkainen työskentely julkisessa hallinnossa. Haastatteluissa ja työpajassa nousi esille useita huomioita nykyaikaisten työskentelymallien haasteista ja ohjeistuksen puutteista. Aiheeseen liittyviä ohjeita on olemassa muiden organisaatioiden julkaisemina, mutta tiedonhallintalautakunnan ohjeissa ja suosituksissa aihetta ei ole käsitelty. Työn aikana todettiin myös, että nykyään suosituksissa ja ohjeissa viitataan edelleen usein vuonna 2013 julkaistuun VAHTI:n toimitilojen tietoturvaohjeeseen. Ohje on osittain vanhentunut, minkä vuoksi on suositeltavaa luoda uusi ajantasainen toimitilaturvallisuuden ohje, joka käsittelee laajasti myös nykyaikaisten työskentelymuotojen huomiot ja vaatimukset. Ohjeessa huomioitava asioita ovat muun muassa etätyö ja monipaikkaisen työn mallit yleisesti, varautumisen näkökulmat etätyön osalta ja turvakopit sekä niiden hyödyntäminen monipaikkaisessa työskentelyssä. Selvitystyön aikana tuli myös esille ehdotus oman toimitilaturvallisuuden asioiden kehittämiseen ja suositusten laadintaan keskittyvän jaoston perustamisesta tiedonhallintalautakuntaan.

5.4.2 Suositus automaattisesta päätöksenteosta julkisessa hallinnossa

Haastattelujen perusteella tiedonhallintalakia ollaan kehittämässä vuoden 2023 aikana niin, että siinä huomioidaan säädökset automatisoidusta tiedonhallinnasta ja päätöksenteosta (luku 6a). Tämän myötä nousee esille tarve luoda suositus, jossa ohjeistetaan hallinnon organisaatioita soveltamaan tiedonhallintalaissa kuvattuja säädöksiä automaattisen päätöksenteon osalta.

Suositusta kehitettäessä on arvioitava mahdolliset muut lainsäädännön esteet. Suositus pohjautuu tiedonhallintalain automaattisen päätöksenteon sääntelyyn, mutta on arvioitava myös muiden lakien vaikutus automaattisen päätöksenteon käytön soveltamiseen. Lisäksi on huomioitava, että EU-tasolta puuttuu tällä hetkellä sääntely tekoälyn hyödyntämiselle.

5.4.3 Suositus häiriötilanteiden hallinnasta

Haastattelujen perusteella tiedonhallintalakia kehitetään vuoden 2023 aikana niin, että siinä säädetään jatkossa velvoitteista tietoturvaan liittyvien häiriötilanteiden tiedottamisesta ja ilmoittamisvelvollisuuksista sekä häiriötilanteihin varautumisesta (13a §). Tämän myötä syntyy tarve luoda suositus, joka ohjeistaa hallinnon organisaatioita soveltamaan tiedonhallintalain velvoitteita omaan toimintaansa.

Suosituksessa tulee kuvata yhteistoiminnan menetelmät ja velvoitteet eri organisaatioiden välillä häiriötilanteissa. Useammassa haastattelussa nousi esille tiedonsaantioikeus ja tiedon luovuttamisen haasteet viranomaisten välillä esimerkiksi tietomurtotilanteessa. Haasteeksi koetaan esimerkiksi tulkinnat siitä, mitä tietoa kunta saa valtiolta tai mitä tietoa esimerkiksi tietomurtotapauksessa suojelupoliisi saa Kyberturvallisuuskeskukselta. Tietomurtotapaukseen voi liittyä useita toimijoita kuten poliisi, Kyberturvallisuuskeskus, hyökkäyksen kohteeksi joutunut organisaatio, asiakas, jonka tietoa on vuodettu, sekä useita palveluntoimittajia, jotka esimerkiksi tuottavat ja ylläpitävät tietojärjestelmiä. Näiden toimijoiden välinen tiedonvaihto koetaan tällä hetkellä epäselväksi, minkä vuoksi aiheeseen liittyvää sääntelyä ja suosituksia tulisi kehittää. Suosituksen kehittämisessä tulisi huomioida myös yksityisyyden suojaan liittyvät näkökulmat.

Häiriötilanteiden hallinnan suosituksen kehittämisessä tulisi arvioida, kuvataanko siinä myös haavoittuvuuksien hallintaan liittyviä menetelmiä ja toimintamalleja sekä CSIRT-toiminnan käytäntöjä vai tulisiko näistä luoda erilliset suosituksensa. Molemmat aiheet ovat sidoksissa häiriötilanteisiin varautumiseen.

5.4.4 Suositus varautumiseen ja jatkuvuudenhallintaan

Selvitystyössä käsiteltiin digitalisaation vaikutusta varautumiseen, minkä myötä syntyi useita ajatuksia varautumiseen liittyvistä riskeistä ja suositusten kehittämisehdotuksista. Tiedonhallintalautakunnalla ei ole omaa suositusta varautumiseen ja jatkuvuudenhallintaan, mutta VAHTI-työryhmä on julkaissut vuonna 2016 ohjeen toiminnan jatkuvuuden hallintaan. Ohje on melkein seitsemän vuotta vanha, minkä vuoksi aihetta on syytä tarkastella uudelleen ja luoda ajantasainen ohjeistus tiedonhallintayksiköille.

Kehittyneen digitalisaation yleisten huomioiden lisäksi suosituksessa on hyvä huomioida pilviympäristöjen tuomat mahdollisuudet ja riskit varautumisen näkökulmasta, viranomaisyhteistyön nykyiset käytännöt ja linjaukset, etä- ja monipaikkaisen työn tuomat mahdollisuudet, viestinnän ja tiedottamisen vastuut sekä toiminnan testauksen ja harjoittelun näkökulmat. Esimerkiksi toimintakriittisten palveluiden hajauttaminen pilvipalveluihin omien konesalien lisäksi kriisitilanteessa on yksi näkökulma, joka tuli useasti esille selvitystyön aikana. Työpajassa nousi esille myös huomio Nato-jäsenyyden vaikutuksista varautumiseen – niitä on syytä arvioida suositusta kehitettäessä. Lisäksi varautumiseen liittyvät osaamisen kehittämisen menetelmät on syytä ohjeistaa suosituksessa. Suositusta kehitettäessä on tärkeää arvioida, tehdäänkö suosituksen ohjeet normaaliolojen varautumisen lisäksi poikkeusolojen varautumisen näkökulmasta.

Varautumisen ohjeistukseen voisi sisällyttää myös käytännön esimerkkejä siitä, miten esimerkiksi keskeisiltä kyberhyökkäyksiltä voidaan suojautua ja miten tapahtuneesta hyökkäyksestä voidaan toipua mahdollisimman pian. Kappaleessa 5.4.3 kuvattu ehdotus suosituksesta häiriötilanteiden hallintaan voisi myös olla osa tätä laajempaa varautumisen suositusta.

5.4.5 Suositus sähköisestä allekirjoituksesta julkisessa hallinnossa

Haastatteluiden perusteella kävi ilmi, että sähköisen allekirjoituksen käyttöönotto on osittain vielä keskeneräistä julkisen hallinnon organisaatioissa. Tarvetta nähtiin sähköisen allekirjoituksen suositukselle, joka ohjeistaisi siihen liittyvistä toimintamalleista ja menetelmistä ja siten tukisi käyttöönottoa. Suosituksessa tulisi kuvata, millaisiin tapauksiin sähköinen allekirjoitus on hyväksyttävä tapa ja millaisiin tilanteisiin se ei sovellu. Suositus helpottaisi tiedonhallintayksiköitä hyödyntämään sähköisen allekirjoituksen käyttöä laajemmin, mikä voisi nopeuttaa julkisen hallinnon organisaatioiden eri prosesseja. Suosituksen kehittämisessä tulee huomioida EU:n eIDAS-asetuksen säädökset ja Kyberturvallisuuskeskuksen ohjeet esimerkiksi hyväksytyistä ja ei-hyväksytyistä luottamuspalveluista.

5.4.6 Suositus tekoälyn hyödyntämisestä julkisessa hallinnossa

Tekoälyyn liittyvä ohjeistus nousi esille haastatteluissa ja työpajan tuloksissa useamman kerran. Tekoälyn soveltamisen mahdollisuudet kasvavat jatkuvasti ja niitä on tarpeellista ottaa käyttöön julkisessa hallinnossa esimerkiksi kyberturvallisuuden kyvykkyyksien kehittämisen osalta. Suositus auttaisi tiedonhallintayksiköitä arvioimaan tekoälyyn liittyviä riskejä ja mahdollisuuksia ja sitä kautta tekemään päätöksiä erilaisten ratkaisujen käyttöönotosta. Suosituksen haasteena on puuttuva tekoälyyn kohdennettu lainsäädäntö, joten suositus pitäisi tehdä huomioiden tiedonhallintalain säädökset ja päivittää siinä vaiheessa, kun EU:n tai kansallisen tason lainsäädäntö tekoälylle astuu voimaan.

Suositusta laadittaessa on arvioitava, missä määrin siinä puhutaan tekoälystä, koneoppimisesta tai esimerkiksi laajemmin kehittyneistä järjestelmistä, joka kattaisi tekoälyn lisäksi muita moderneja teknologioita. Tekoälyn ja esimerkiksi koneoppimisen termien välillä on eroja, joten termistön auki kirjoittaminen ja niiden käyttö tulee pohtia tarkkaan tulkintaerojen välttämiseksi. Suosituksen laadinnassa voisi hyödyntää Kyberturvallisuuskeskuksen vuonna 2021 julkaisemaa Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta -ohjetta.

5.4.7 Suosituskokonaisuuden käytön ohjeistus

Vaikutusten arvioinnista järjestetyssä työpajassa tuotiin esille ehdotus suosituskokoelman käytön ohjeistamisesta. Tähän liittyen myös haastatteluissa tuli esille ehdotuksia suositusten yleiselle kehittämiselle; näitä on kuvattu kappaleissa 5.1 ja 5.2. Suosituskokonaisuuden käytön oheistus voisi kuvata esimerkiksi sitä, mitä suositukset yleisesti sisältävät, mikä suositusten tarkoitus on ja miksi niitä luodaan, miten suosituksia tulee hyödyntää tiedonhallintayksiköiden toiminnassa, millä tasolla suosituksia on laadittu, ketkä ovat vastuullisia kehittämään niitä eri tasoilla ja kuinka uusista suosituksista viestitään. Suosituksessa voisi ohjeistaa myös, kuinka suosituksen soveltamiseen saa tukea ja koulutusta.

Suosituksen kehittämisessä on arvioitava, koskettaako se vain tiedonhallintalakiin liittyviä suosituksia vai otetaanko siinä huomioon myös muut julkisen hallinnon suositukset ja niiden hyödyntämisen ohjeistaminen. Yleisesti selvitystyön tulosten pohjalta on tunnistettu, että eri julkisen hallinnon organisaatioiden tuottamat ohjeet, suositukset ja niiden kehittäminen ovat hajautuneet ja ne sisältävät paljon päällekkäisyyksiä, minkä vuoksi suosituskokonaisuuden käytön ohjeistus voisi luoda tähän selkeämpää mallia jatkossa.

6 Yhteenveto

Selvitystyön aikana muodostui useita ehdotuksia tietoturvallisuuden suositusten kehittämiselle ja uusien suositusten luomiselle. Yhteenvetona voidaan todeta, että tuloksissa korostuvat suositusten käytännönläheisyyden ja konkreettisuuden kehittämistarpeet. Haasteeksi yleisesti havaittiin myös osaamisen puutteet erityisesti uusien teknologioiden osalta. Uusi teknologia tuo tarpeita uusille suosituksille, ja sen tuomat riskit on huomioitava tietoturvallisuuden ohjeiden ja suositusten päivittämisessä. Suositusten laadinnan prosesseja ja toimintamalleja on syytä tarkastella kokonaisuutena havaintojen pohjalta ja arvioida, mitkä ehdotetut kehittämistoimenpiteet tuovat suosituksille parempaa vaikuttavuutta sekä kehittävät niiden käytännönläheisyyttä, jotta suositusten lukija pystyy paremmin soveltamaan niitä omaan toimintaansa.

Olemassa olevien suositusten kehittämiseen tunnistettiin useita lisäysehdotuksia. Erityisesti suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta on hyvä kooste erilaisia ohjeista tiedonhallintalain säädöksiin liittyen, jota on mahdollista kehittää laajemmaksi selvitystyön tulosten pohjalta. Vaikutusten arvioinnin työpajan tuloksista ja haastatteluista tunnistettiin ehdotuksia uusien suositusten kehittämiselle. Vastaavaa arviointia voisi tehdä jatkossa säännöllisesti esimerkiksi jaostojen kokousten yhteydessä.

6.1 Kooste ehdotetuista kehittämistoimenpiteistä

Taulukossa 1 on esitetty kokoelma ehdotetuista kehitystoimenpiteistä Tiedonhallintalautakunnan suositusten kehittämiselle.

Taulukko 1. Yhteenveto suositusten kehittämistoimenpiteistä

Toimenpiteen nimi	Toimenpiteen kuvaus
Suosituskokoelman tiettyjen tietoturvallisuussäännösten soveltamisesta päivittäminen	Luvussa 5.3.1 kuvatut toimenpiteet
Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä päivittäminen	Luvussa 5.3.2 kuvatut toimenpiteet

Toimenpiteen nimi	Toimenpiteen kuvaus
Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa päivittäminen	Luvussa 5.3.3 kuvatut toimenpiteet
Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) päivittäminen	Luvussa 5.3.4 kuvatut toimenpiteet
Suositus toimitilaturvallisuudesta	Uuden suosituksen kehittäminen toimitilaturvallisuudelle. Suosituksessa huomioitava erityisesti nykyaikaiset työskentelymuodot.
Suositus automaattisesta päätöksenteosta julkisessa hallinnossa	Uuden suosituksen laadinta automaattisen päätöksenteon hyödyntämiseen. Kehitettävä kun tiedonhallintalakiin tehdään aihetta koskeva päivitys.
Suositus häiriötilanteiden hallinnasta	Uuden suosituksen laadinta häiriötilanteiden hallintaan. Kehitettävä kun tiedonhallintalakiin tehdään aihetta koskeva päivitys.
Suositus varautumiseen ja jatkuvuudenhallintaan	Uuden suosituksen laadinta varautumiseen ja jatkuvuudenhallintaan. Kehitettävä konkreettinen ohjeistus siihen, kuinka tiedonhallintayksiköissä kehitetään varautumista normaali- ja poikkeusoloihin. Huomioitava erityisesti digitalisaation vaikutukset varautumiseen ja modernit työskentelymuodot.
Suosituskokonaisuuden käytön ohjeistus	Uuden suosituksen laadinta suosituskokoelman käytön ohjeistamiseen. Suosituksessa huomioitava toimintamallit erilaisten ohjeiden ja suositusten kehittämiselle ja arvioitava, kuinka vaikuttavuuden kehittäminen saadaan osaksi prosessia. Suosituksen tarkoituksena on selkeyttää, kuinka tiedonhallintayksikkö voi parhaiten hyödyntää ohjeita ja suosituksia omassa toiminnassaan.
Suositus tekoälyn hyödyntämisestä julkisessa hallinnossa	Uuden suosituksen laadinta tekoälyn hyödyntämiselle. Suositus antaa ohjeita siihen, millaisia asioita on huomioitava, kun tekoälypohjaisia ratkaisuja otetaan käyttöön julkisessa hallinnossa.

Toimenpiteen nimi	Toimenpiteen kuvaus
Julkisen hallinnon suositusten ja ohjeistusten keskittäminen	Kehitettävä keskitetty sijainti, josta erilaiset suositukset ja ohjeet löytyvät helposti julkisen hallinnon organisaatiolle. Tästä tulisi käydä ilmi myös se, ketä kukin suositus koskettaa, jotta organisaation on helppo tunnistaa siihen kohdistuvat ohjeet ja suositukset.
Olemassa olevien suositusten ajantasaisuuden tarkastaminen ja päivittäminen	Useat julkisesti saatavilla olevat suositukset ja ohjeet ovat vanhoja ja niiden ajantasaisuus tulee tarkistaa. Nykyisellään lukijalle ei käy selkeästi selväksi, mitkä ovat ajantasaisia ja mitkä sisältävät vanhentunutta tietoa. Asian kehittämiseen tulisi luoda toimintamalli, joka varmistaa, että ohjeet ja suositukset pysyvät ajantasaisina.
Esimerkkien lisääminen suosituksiin toimialakohtaisesta soveltamisesta ja hyväksytyistä jäännösriskeistä	Yleinen kehittämisehdotus, joka koskettaa kaikkia suosituksia. Työn aikana nostettiin useamman kerran esille tarve konkreettisille esimerkeille suosituksen tai ohjeen soveltamisesta.
Suositusten vaikuttavuuden arviointi ja kehittäminen osaksi tiedonhallintalautakunnan suositusten yleistä kehittämisprosessia	Määriteltävä, kuinka suosituksen vaikuttavuutta mitataan, arvioidaan ja kehitetään sen luomisen aikana ja julkaisemisen jälkeen. Vaikuttavuuden arvioinnin ja kehittämisen tulisi olla kiinteä osa suositusten yleistä kehittämisprosessia.
Vaikutusanalyysi viranomaisten tehtäviin liittyvistä rakennemuutoksista	Haastatteluissa nostettu tarve luoda vaikutusanalyysi tulevista viranomaisten tehtäviin liittyvistä rakennemuutoksista. Vaikutusanalyysissa huomioitava erityisesti tiedonhallintalain säädösten vaikutukset organisaatioihin ja esimerkiksi yhteisiin tietovarantoihin liittyen.
Suositusten hyödyntäjien osallistaminen suositusten kehittämiseen	Haastatteluissa useasti esille tuotu tarve osallistaa vahvemmin suositusten hyödyntäjiä niiden kehittämiseen. Tämän osalta pohdittava, mitkä ovat parhaat keinot lisätä kohdeorganisaatioiden osallistumista suositusten kehittämiseen ja arviointiin ennen niiden julkaisua.

Toimenpiteen nimi	Toimenpiteen kuvaus
Suositusten ja ohjeiden tasojen ja niiden vastuiden määrittäminen	Konkreettisena kehitysehdotuksena esitetty malli, jossa suositukset ja ohjeet jaetaan eri tasoille niiden sisällön tarkkuustason mukaisesti. Ehdotuksena on luoda tasot ja määrittää, mikä organisaatio vastaa niiden suositusten ja ohjeiden laadinnasta. Toimenpidettä kannattaa tarkastella tiedonhallintalautakuntaa laajemmin, mielellään niin, että se huomioi myös esimerkiksi DVV:n ja KTK:n ohjeistustoiminnan.
Ohjeistus tai suositus digitaalisten palvelujen dokumentaatiosta ja mitä tietoa käyttäjille on luovutettava	Yksittäisenä tarpeena esille nostettu ohjeistus siitä, millainen dokumentaatio tulee luoda julkisen hallinnon tarjoamasta palvelusta. Ohjeessa huomioitava myös se, mitä tietoa tulee luovuttaa palvelun käyttäjälle, jotta se voi varmistaa esimerkiksi tiedonhallintalain vaatimusten toteutumisen palvelussa.

6.2 Jatkoselvityksen aiheet

Selvitystyön aikana tunnistettiin useita muita teknologioita ja julkisen hallinnon digitalisaation ilmiöitä, jotka rajautuivat työstä pois. Näiden ilmiöiden tutkimista ja vaikutusten julkiseen hallintoon arviointia on syytä harkita jatkotyönä. Tunnistetut aiheet on listattu taulukossa 2.

Taulukko 2. Selvitystyöstä pois rajatut aihealueet

Aihe	Kuvaus
Tiedonsaantioikeus	Haastattelun mukaan tähän liittyvää sääntelyä ja mahdollista suositusta tulisi kehittää, jotta tiedonsaantiin liittyvät jäykkyydet saataisiin poistettua ja teknologian hyödyntäminen digitaalisten ratkaisujen kehittämiseen mahdollistettua.

Aihe	Kuvaus
Tunnistautumisen menetelmät	Vastaanottajan tunnistaminen ja tunnistautuminen nousivat esille haasteena esimerkiksi videokokouksissa. Vastapuoli pitäisi pystyä verifioimaan kaikissa tilanteissa. Jatkotutkimuksessa arvioitava, mikä on riittävä taso vastaanottajan tunnistamiselle, ja tuotava linjaukset osaksi olemassa olevia suosituksia.
Sosiaalisen median alustojen omien selainten käyttö	Selvitettävä sosiaalisen median omien selainten tietoturvallisuusriskit, esimerkiksi niiden keräämä tieto käyttäjän toiminnasta. Aihe tulee huomioida julkisen hallinnon tietoturvan ohjeistuksissa.
Mobiililaitteiden ja -sovellusten tuomat riskit verrattuna perinteisiin työasemiin.	Julkisen hallinnon tietoturvan ohjeistuksissa huomioitava mobiililaitteiden ja niiden sovellusten riskit verrattuna perinteisiin työasemiin ja niiden sovelluksiin.
Tietosuojan lainsäädännön tulkintaerot	Tietosuojan osalta haastatteluissa tunnistettiin, että useat organisaatiot tekevät erilaisia tulkintoja tietosuojan sääntelystä. Yleisenä esimerkkinä esiin nostettiin henkilötietojen käsittely ja säilyttäminen julkipilvipalveluissa. Tulkintaa tehdään monesti vaikeimman kautta ja tähän liittyvää suositusta tai tarkempaa ohjeistusta tarvitaan. Konkreettinen ja selkeä ohjeistus mahdollistaisi paremmin pilvipalveluiden käyttämisen. Ohjeen taustaksi tulisi tutkia, millaisia erilaisia tulkintoja on tähän asti tehty ja mistä tulkintaerot johtuvat.
Tietoturvateknologioiden kehitys	Ehdotettu jatkotutkimusaiheeksi sitä, millaisia tietoturvateknologioita voidaan nykyään ja tulevaisuudessa hyödyntää tiedon suojaamiseen.
OECD:n digiturvan standardit ja niiden vaikutuksen arviointi	Ehdotettu jatkotutkimusaiheeksi sitä, millaisia vaikutuksia OECD:n digiturvan standardit ja suositukset tuovat julkisen hallinnon organisaatioille.
Kybervakoilun vaikutus ja huomioiminen suosituksissa	Arvioitava, millaisia vaikutuksia kybertiedustelulla ja kybervakoilulla on julkiseen hallintoon sekä kuinka aiheesta tulisi ohjeistaa julkisen hallinnon organisaatioita.

Aihe	Kuvaus
EU-sääntelyn aiheuttamat vaikutukset	Arvioitava kokonaisuutena, millaisia digitaalisen turvallisuuden vaikutuksia Euroopan unionin säädökset tuovat Suomen julkiseen hallintoon. Haastatteluissa on nostettu esille NIS2 (Network and Information Systems), CER (Resilience of Critical Facilities) ja CRA (Cyber Resilience Act) -säädökset.
Tiedonhallintalain tavoitteiden arviointi	Haastatteluissa esille nostettu tarve. Tiedonhallintalakia kehitettäessä tulisi pohtia, mikä sen alkuperäinen tavoite on ollut, onko tavoitteiden saavuttamisessa onnistuttu ja ovatko tavoitteet edelleen valideja nykypäivänä vai pitäisikö niitä kenties päivittää.
Vanhojen tietojärjestelmien turvaaminen	Kuinka vanhojen tietojärjestelmien turvaaminen pitää toteuttaa, kun siirrytään uusiin moderneihin palveluihin ja ympäristöihin? Tämä koskettaa esimerkiksi järjestelmiä, joita on pakko pitää yllä tiedon arkistointiin liittyen. Aihe huomioitava julkisen hallinnon ohjeistuksissa.
5G-teknologian aiheuttavat vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia 5G-teknologian yleistyminen aiheuttaa julkisen hallinnon organisaatioille.
Lohkoketjuteknologian aiheuttamat vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia lohkoketjuteknologian yleistyminen tuo julkisen hallinnon organisaatioille.
Metaversumin ja AR/VR-teknologioiden aiheuttamat vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia VR- ja AR-teknologioiden sekä metaversumin yleistyminen aiheuttaa julkisen hallinnon organisaatioille.
IoT-teknologian aiheuttamat vaikutukset ja muutokset	Arvioitava millaisia vaikutuksia IoT teknologian yleistyminen aiheuttaa julkisen hallinnon organisaatioille.
Ohjelmistorobotiikan (RPA) aiheuttamat vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia ohjelmistorobotiikan yleistyminen aiheuttaa julkisen hallinnon organisaatioille.
Älyautojen teknologioiden aiheuttamat vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia älyautojen teknologioiden yleistyminen aiheuttaa julkisen hallinnon organisaatioille.
Wearables-laitteiden käytön yleistyminen ja niiden aiheuttamat vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia puettavien laitteiden kuten älykellojen yleistyminen aiheuttaa julkisen hallinnon organisaatioille.

Aihe	Kuvaus
Puheentunnistussovellusten ja -palveluiden aiheuttamat vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia puheentunnistussovellusten ja niihin liittyvien palveluiden yleistyminen aiheuttaa julkisen hallinnon organisaatioille.
Digitaalisten asiointipalveluiden yleistymisen vaikutukset ja muutokset	Arvioitava syvemmin, millaisia vaikutuksia digitaalisten asiointipalveluiden yleistyminen aiheuttaa julkisen hallinnon organisaatioille.
Digitaalisen henkilöllisyystodistuksen käyttöönoton vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia digitaalisen henkilöllisyystodistuksen käyttöönotto aiheuttaa julkisen hallinnon organisaatioille.
Nato-jäsenyyden vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia Nato-jäsenyys aiheuttaa julkisen hallinnon organisaatioille erityisesti kyberturvallisuuden näkökulmasta.
Informaatiovaikuttamisen ja disinformaation vaikutukset	Arvioitava syvällisemmin vaikutuksia, joita informaatiovaikuttaminen aiheuttaa julkisen hallinnon organisaatioille, sekä huomioitava nämä julkisen hallinnon turvallisuuden ohjeistuksissa.
Hyvinvointialueiden näkökulma tietoturvallisuuden sääntelyyn	Tutkimuksen tarkempana kohteena voisivat olla hyvinvointialueet ja niiden tietoturvaan liittyvät riskit ja mahdollisuudet. Tulisi myös selvittää, millaista yhteistoimintaa tarvitaan hyvinvointialueille ja kuinka alueiden tietoturvan sääntelyä tulee kehittää.
Tiedolla johtaminen, data-analytiikka ja big data	Arvioitava, millaisia vaikutuksia tiedolla johtamisen ratkaisut, data-analytiikka ja big data -ilmiöt aiheuttavat julkisen hallinnon organisaatioille erityisesti kyberturvallisuuden näkökulmasta.
Paikkatiedon hyödyntäminen ja sen vaikutukset ja muutokset	Arvioitava, millaisia vaikutuksia paikkatiedon hyödyntäminen aiheuttaa julkisen hallinnon organisaatioille erityisesti kyberturvallisuuden näkökulmasta.

SANASTO

Sana	Määritelmä
5G-teknologia	5G (fifth generation) -teknologia tarkoittaa viidennen sukupolven datayhteyttä mobiilitekniikassa.
Augmented reality (AR)	Lisätty todellisuus, augmented reality (AR) on reaaliaikaista tiedon käyttöä tekstin, grafiikan, äänen ja muiden virtuaalisten formaattien muodossa, joka on integroitu reaalimaailman objekteihin.
CER	CER (Critical Entities Resilience Directive) on EU-laajuinen lainsäädäntöohje, joka luo puitteet kriittisten palvelujen tarjoajien digitaaliselle ja fyysiselle turvallisuudelle ja kestävyydelle. Direktiivi keskittyy fyysiseen turvallisuuteen ja kriittisten prosessien, kuten juomaveden ja energian, turvallisuuteen ja suojaamiseen.
CRA	Euroopan unionin asetusehdotus digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusvaatimuksista, joka tunnetaan nimellä Cyber Resilience Act (CRA).
Deepfake	Deepfake-sisällössä käytetään tekoälyn ja koneoppimisen menetelmiä esittämään esimerkiksi valheellista, mutta realistisen näköistä videokuvaa ja ääntä jostain henkilöstä.
Informaatiovaikuttaminen	Informaatiovaikuttaminen on toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn.
IoT	Internet of Things (IoT) kuvaa verkkoa, joka koostuu fyysisistä objekteista, jotka sisältävät antureita, ohjelmistoja ja muita tekniikoita, joiden tarkoituksena on yhdistää ja vaihtaa tietoja muiden laitteiden ja järjestelmien kanssa Internetin kautta.
Julkinen pilvipalvelu	Pilvipalveluilla tarkoitetaan digitaalisia palveluita, jotka pilvipalvelutarjoaja tuottaa keskitetystä ja jaetusta laskenta-, -muisti ja tallennuskapasiteetista. Yleisiä julkisia pilvipalveluita ovat Microsoft Azure, Amazon Web Services ja Google Cloud Platform.
Koneoppiminen	Koneoppiminen on yksi tekoälyn alaluokka, jossa tekoälysovellus muodostaa koneoppimisen mallin sille opetettavan datan perusteella. Koneoppimisen malleja hyödyntävät tekoälysovellukset voivat esimerkiksi tehdä päätöksiä erikseen määritellyistä asioista dataan pohjautuen.

Sana	Määritelmä
Kvanttilaskenta	Kvanttilaskentaan käytetään kvanttitietokoneita, jotka ovat moninkertaisesti nykyisiä supertietokoneita tehokkaampia. Niillä voidaan ratkaista ongelmia, joiden suorittamiseen nykyisillä tietokoneilla kestäisi jopa tuhansia vuosia.
Kybervakoilu ja -tiedustelu	Kybervakoilulla tarkoitetaan toimintaa, jonka avulla voidaan hankkia salaisia tietoja esimerkiksi yksityisiltä ihmisiltä, yritysmaailman kilpailijoilta tai oman tai vieraan valtion organisaatiosta Internetistä tai siihen tarkoitetuilla ohjelmistoilla ja laitteilla.
Lohkoketjuteknologia	Lohkoketjuteknologia on edistynyt tietokantamekanismi, joka mahdollistaa läpinäkyvän tiedon jakamisen yritysverkossa.
Metaversumi	Metaversumilla tarkoitetaan virtuaalitodellisuuden (VR) kautta koettua, jaettua virtuaalista ympäristöä, jossa käyttäjät ovat vuorovaikutuksessa keskenään ja voivat esimerkiksi ostaa tavaroita tai palveluita, joista osa olisi olemassa vain verkkomaailmassa.
NIS2-direktiivi	NIS2 (Network and Information System) -direktiivi on EU-laajuinen lainsäädäntöohje kyberturvallisuuden hallintaan. Se asettaa perustan kyberturvallisuusriskien hallintatoimenpiteille ja raportointivelvoitteille kaikilla direktiivin kattamilla aloilla, kuten energia, liikenne, terveys ja digitaalinen infrastruktuuri.
Ohjelmistorobotiikka (RPA)	Ohjelmistorobotiikka, Robot Process Automation (RPA), tarkoittaa teknologiaa, jonka avulla voidaan automatisoida esimerkiksi rutiininomaisia töitä eri prosesseissa ja toiminnoissa.
SaaS	Ohjelmisto palveluna -malli (Software as a Service) on palvelumalli, jossa pilvipalvelun tarjoaja tuottaa palvelut kokonaisuudessaan.
Tekoäly	Tekoälyllä tarkoitetaan tietojenkäsittelyn osa-aluetta, jossa tietojärjestelmä, sovellus tai laite suorittaa älykkyyttä vaativia tehtäviä ja käyttää perinteisesti ihmisen älyyn liitettyjä taitoja, kuten päättelyä, oppimista, suunnittelemista tai luomista.

Sana	Määritelmä
Tiedonhallintalautakunta	Julkisen hallinnon tiedonhallintalautakunta on monialaiseen asiantuntijayhteistyöhön perustuva viranomainen, joka toimii valtiovarainministeriön yhteydessä. Tiedonhallintalautakunnan tehtävänä on edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista.
Tiedonhallintayksikkö	Viranomainen, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti
Tietoturvallisuusjaosto	Tietoturvallisuusjaosto kehittää tiedonhallintalain säännösten toteuttamista konkretisoivia tietoturvallisuussuosituksia ja seuraa ja arvioi niiden ajantasaisuutta ja kattavuutta.
Todentaminen	(autentikointi) menettely, jolla varmistetaan tunnisteen aitous ja oikeellisuus (Tiivis tietoturvasanasto (TSK 31, 2004)
Virtual reality (VR)	Virtuaalitodellisuus, virtual reality (VR) on termi, jota käytetään kuvaamaan kolmiulotteista, tietokoneella luotua ympäristöä, jota ihminen voi tutkia ja jonka kanssa hän voi olla vuorovaikutuksessa esimerkiksi sen käyttöön tarkoitetuilla VR-laseilla ja ohjaimilla.
Zero Trust	Zero Trust yleisesti käsittää käyttäjän identiteetin varmentamisen, päätelaitteen suojaamisen, tiedon ja sovellusten suojaamisen, IT-infrastruktuurin ja verkkojen suojaamisen sekä ympäristön jatkuvan valvonnan. Näiden osalta ympäristöön luodaan toimintamallit, jossa ei suoraan luoteta käyttäjään tai laitteeseen missään tilanteessa ilman esimerkiksi riittävää varmentamista sen identiteetistä. Zero Trust -ajattelumallissa oletetaan pahinta ja varaudutaan valmiiksi tilanteisiin, joissa hyökkääjä on päässyt ympäristöön tai suojattavaan tietoon käsiksi.

LIITTEET

Liite 1 Listaus tietoturvallisuuden ohjeista ja suosituksista – Olemassa olevat suositukset ja ohjeet.xlsx

Liite on tallennettu omana tiedostonaan osoitteeseen

https://urn.fi/URN:ISBN:978-952-367-437-0

Liite 2 Haastattelun kysymysrunko – Haastattelun pohja.docx

Liite on tallennettu omana tiedostonaan osoitteeseen

https://urn.fi/URN:ISBN:978-952-367-437-0

LÄHTEET

[1] Teknologian tutkimuskeskus VTT. Suomen ensimmäinen kvanttitietokone on valmis käyttöön. Lehdistötiedote 30.11.2021. https://www.vttresearch.com/fi/uutiset-ja-tarinat/suomen-ensimmainen-kvanttitietokone-valmis-kayttoon

[2] Puolustusvoimat. Puolustustutkimuksen vuosikirja 2021. PVTUTKL+Puolustustutkimuksen+vuosikirja+2021.pdf (puolustusvoimat.fi)

[3] National Institute of Standards and Technology. NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. Tiedote 5.7.2022. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[4] Valtiovarainministeriö. Kansallinen tekoälyohjelma AuroraAI. https://vm.fi/tekoalyohjelma-auroraai

[5] Eduskunnan kirjasto. Yleislainsäädäntö automaattiselle päätöksenteolle. 14.10.2022. https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/yleislainsaadanto-automaattiselle-paatoksenteolle.aspx

[6] Euroopan parlamentti. Mitä tekoäly on ja mihin sitä käytetään? https://www.europarl.europa.eu/news/fi/headlines/society/20200827STO85804/mita-tekoaly-on-ja-mihin-sita-kaytetaan

[7] Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta. 2.11.2021. https://www.traficom.fi/sites/default/files/media/publication/Teko%C3%A4lyn%20soveltamisen%20kyberturvallisuus%20ja%20riskienhallinta.pdf

[8] Valtiovarainministeriö. Yhteistyötä palveluissa ja toimitiloissa. https://vm.fi/yhteistyota-palveluissa-ja-toimitiloissa

[9] Valtiovarainministeriö. Monipaikkainen työ ja sen potentiaali – kysely. 22.3.2021. https://vm.fi/documents/10623/302994/Monipaikkainen+-ty%C3%B6+ja+sen+potentiaali+%E2%80%93virastokyselyn+tulokset.pdf/d18f3777-d6a8-de56-f1f2-c5344fb9d555/Monipaikkainen+ty%C3%B6+ja+sen+potentiaali+%E2%80%93virastokyselyn+tulokset.pdf?t=1616596283400

[10] Valtiovarainministeriö. Valtioneuvoston periaatepäätös valtion toimitilastrategiaksi. 16.12.2021. https://vm.fi/documents/10623/68097244/Valtioneuvoston+periaatep%C3%A4%C3%A4t%C3%B6s+valtion+toimitilastrategiaksi.pdf/9adb45e9-f7d1-90ce-511b-e53bbaee3e71/Valtioneuvoston+periaatep%C3%A4%C3%A4t%C3%B6s+valtion+toimitilastrategiaksi.pdf?t=1658140212929

[11] Valtiovarainministeriö. Digitalisaation edistämisen ohjelma. https://vm.fi/digitalisaation-edistamisen-ohjelma

[12] Valtiovarainministeriö. Julkisen hallinnon pilvipalvelulinjaukset. 18.1.2019. http://urn.fi/URN:ISBN:978-952-251-982-5

[13] Valtiovarainministeriö. Tiedonhallintalaki. https://vm.fi/tiedonhallintalaki

[14] Valtiovarainministeriö. Tiedonhallintalautakunta. https://vm.fi/tiedonhallintalautakunta

[15] Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2021:65). Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. http://urn.fi/URN:ISBN:978-952-367-897-2.

[16] Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2021:5). Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. http://urn.fi/URN:ISBN:978-952-367-500-1.

[17] Tiedonhallintalautakunnan suositus – Valtiovarainministeriö (2022:4). Suositus turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. http://urn.fi/URN:ISBN:978-952-367-906-1.

[18] Tiedonhallintalautakunnan suositus - Valtiovarainministeriö (2022:43). Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) : Suositus ja kriteeristö. http://urn.fi/URN:ISBN:978-952-367-275-8.

[19] Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

[20] Valtiovarainministeriö, Haukka-hanke. Ohjeiden ja suositusten vaikuttavuuden arvioinnin pilotointi https://www.vm.fi/documents/10623/31227348/Haukka+ohjeiden+-suositusten+vaikuttavuuden+arviointi.pdf/c698197a-4df7-6521-69b8-af6d67c8c7bc/Haukka+ohjeiden+suositusten+vaikuttavuuden+arviointi.pdf?t=1650893980407

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-437-0 (pdf)

Toukokuu 2023