VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Arviomuistio julkisen hallinnon tietojärjestelmien sääntelyn nykytilasta ja kehittämistarpeista

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja – 2021:54

Valtiovarainministeriön julkaisuja 2021:54

Arviomuistio julkisen hallinnon tietojärjestelmien sääntelyn nykytilasta ja kehittämistarpeista

Julkisen hallinnon tietojärjestelmiä koskevan yleislainsäädännön tarkistamista valmisteleva työryhmä

Valtiovarainministeriö Helsinki 2021

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Valtiovarainministeriö

ISBN pdf: 978-952-367-693-0
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2021

Kuvailulehti
11.10.2021

Arviomuistio julkisen hallinnon tietojärjestelmien sääntelyn nykytilasta ja kehittämistarpeista

Valtiovarainministeriön julkaisuja 2021:54		**Teema**	Julkisen hallinnon ICT
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Julkisen hallinnon tietojärjestelmiä koskevan yleislainsäädännön tarkistamista valmisteleva työryhmä		
Kieli	suomi	**Sivumäärä**	127

Tiivistelmä

Yleislainsäädännössä ei ole säädetty tietojärjestelmän olennaisista vaatimuksista asian käsittelyn asianmukaisuuden ja selvittämisvelvollisuuden toteuttamisessa. Tällaisista tietojärjestelmien olennaisista vaatimuksista voitaisiin säätää lailla. Lisäksi tietojärjestelmien kehittämisen ja käytön ohjaukseen ja valvontaan liittyviä vastuita tulisi eri viranomaisten välillä selkeyttää.

Hallinnon asiakkaan tulisi saa tiedot siitä, mihin yksilöityihin tietoihin viranomainen perustaa päätöksentekonsa niissä tilanteissa, joissa päätös voidaan tehdä täysin automatisoidusti.

Virkavastuun toteuttaminen on mahdollista kehittämällä automatisoitujen toimintaprosessien sisäistä ja ulkoista arviointi- ja varmistusmenettelyä. Viranomaisen toimintaan pitäisi kohdistaa selkeitä toimintavelvollisuuksia tietojärjestelmien kehittämisessä ja käyttöönotossa siten, että hyvän hallinnon ja oikeusturvan vaatimukset on varmistettu ennakollisesti toimintaprosesseissa.

Riittävä tiedon laatu on asianmukaisen asiankäsittelyn ja lainmukaisen hallintoasian käsittelyn edellytys. Tietovarantojen laadun, vastuiden, ja käytön osalta automaattinen päätöksenteko edellyttää nykyistä tarkempaa sääntelyä.

Olisi arvioitava, mitä vaatimuksia vasten tietojärjestelmien vaatimuksenmukaisuutta arvioidaan, ja tulisiko arviointiprosessia tarkentaa lainsäädännössä.

Asiasanat	Julkisen hallinnon ICT, tietojärjestelmät, julkinen hallinto, tietovarannot, tietoturva, tiedonhallinta, virkavastuu, hyvä hallinto		
ISBN PDF	978-952-367-693-0	**ISSN PDF**	1797-9714
Asianumero	VN/4400/2021	**Hankenumero**	VM059:00/2021
Julkaisun osoite	http://urn.fi/URN:ISBN:978-952-367-693-0		

Presentationsblad
11.10.2021

Bedömningspromemoria om de gällande bestämmelserna om informationssystem inom den offentliga förvaltningen och om utvecklingsbehoven

Finansministeriets publikationer 2021:54		**Tema**	Offentliga förvaltningens ICT
Utgivare	Finansministeriet		
Utarbetad av	Arbetsgruppen som bereder en översyn av den allmänna lagstiftningen om informationssystem inom den offentliga förvaltningen		
Språk	finska	**Sidantal**	127

Referat

Den allmänna lagstiftningen saknar bestämmelser om väsentliga krav på informationssystem vid genomförandet av ändamålsenlighet i behandlingen av ärenden och skyldigheten att lämna uppgifter. Det är möjligt att genom lagstiftning föreskriva om sådana väsentliga krav på informationssystem. Ansvaret till utveckling och styrning av och tillsyn över användningen av informationssystem mellan olika myndigheter ska klarläggas.

Det är nödvändigt att en kund till förvaltningen får information om utifrån vilka uppgifter en myndighet fattar sina beslut i situationer där beslutet kan fattas helt automatiserat.

Det är det möjligt att verkställa tjänsteansvaret genom att utveckla den interna och externa bedömnings- och kontrollpraxisen i system för automatiserade verksamhetsprocesser. Tydliga skyldigheter ska riktas till myndigheternas verksamhet i utvecklingen och införandet av informationssystem så att krav på god förvaltning och rättssäkerhet tillgodoses.

Tillräcklig kvalitet på information är en förutsättning för ändamålsenlig ärendehantering och lagenlig behandling av förvaltningsärenden. Vad gäller kvaliteten på datalager, förutsätter automatiserat beslutsfattande lagstiftning som är exaktare än den nuvarande lagstiftningen.

Det ska bedömas mot vilka krav informationssystemens överenstämmelse med krav ska bedömas och huruvida bedömningsprocessen ska preciseras i lagstiftningen.

Nyckelord offentliga förvaltningens IKT, informationssystem, offentlig förvaltning, informationsresurser, informationssäkerhet, informationshantering, tjänsteansvar, god förvaltning

ISBN PDF	978-952-367-693-0	**ISSN PDF**	1797-9714
Ärendenummer	VN/4400/2021	**Projektnummer**	VM059:00/2021
URN-adress	http://urn.fi/URN:ISBN:978-952-367-693-0		

Description sheet
11 October 2021

Assessment memorandum on the current state and development needs of information system regulation in public administration

Publications of the Ministry of Finance 2021:54		**Subject**	Public Sector ICT
Publisher	Ministry of Finance		
Group author	Working group reviewing general legislation on public administration information systems		
Language	Finnish	**Pages**	127

Abstract

There are no provisions in general legislation prescribing the essential requirements for information systems used in implementing appropriate case processing and the duty to investigate. Such essential information system requirements could be laid down by law. Responsibilities for directing and supervising the development and use of information systems should also be clarified between various public authorities.

Clients of public administration should be advised of the specified information on which the authority bases its decision in cases where the decision may be made in a wholly automated manner.

Liability for acts in office may be realised by developing an internal and external evaluation and verification procedure for automated operating processes. Official activities should be subject to clear operating responsibilities when developing and implementing information systems, with the requirements of good governance and due process ensured proactively in operating processes.

Adequate quality of information is a condition of appropriate case processing and lawful administrative procedure. Automated decision-making requires more precise regulation with respect to the quality of information pools, responsibilities, and use.

An evaluation should be made of the requirements for assessing the conformity of information systems, and of whether the assessment process should be specified in legislation.

Keywords Public administration ICT, information systems, public administration, information pools, data security, information management, liability for acts in office, good governance

ISBN PDF	978-952-367-693-0	**ISSN PDF**	1797-9714
Reference number	VN/4400/2021	**Project number**	VM059:00/2021
URN address	http://urn.fi/URN:ISBN:978-952-367-693-0		

Sisältö

KÄYTETYT LYHENTEET

akkreditointilaki	laki vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta (920/2005)
AOA	eduskunnan apulaisoikeusasiamies
AOK	valtioneuvoston apulaisoikeuskansleri
AOKS	valtioneuvoston apulaisoikeuskanslerin sijainen
arviointilaitoslaki	laki tietoturvallisuuden arviointilaitoksista (1405/2011)
arviointilaki	laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)
asiakastietolaki	laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
asiointilaki	laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
avoimen datan direktiivi	Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/1024 avoimesta datasta ja julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä
CER-direktiivi	komission ehdotus Euroopan parlamentin ja neuvoston direktiiviksi kriittisten toimijoiden häiriönsietokyvystä COM (2020) 829
CSIRT	computer security incident response teams
digipalvelulaki	laki digitaalisten palvelujen tarjoamisesta (306/2019)
ENISA	Euroopan unionin kyberturvallisuusvirasto
EOA	eduskunnan oikeusasiamies
FINAS	Suomen kansallinen akkreditointielin
hankintalaki	laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
HaVL	eduskunnan hallintovaliokunnan lausunto
HaVM	eduskunnan hallintovaliokunnan mietintö
julkisuuslaki	laki viranomaisten toiminnan julkisuudesta (621/1999)
Katakri	kansallinen turvallisuusauditointikriteeristö
KTJ-laki	laki kiinteistötietojärjestelmästä ja siitä tuotettavasta palvelusta (453/2002)
kyberturvallisuusasetus	Euroopan parlamentin ja neuvoston asetus (EU) 2019/881 Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta

maksuperustelaki	valtion maksuperustelaki (150/1992)
NIS2-direktiivi	komission ehdotus Euroopan parlamentin ja neuvoston direktiiviksi kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin 2016/1148 kumoamisesta COM (2020) 823
NIS-direktiivi	Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa
NLF-asetus	Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta
OKA	valtioneuvoston oikeuskansleri
PeVL	eduskunnan perustuslakivaliokunnan lausunto
rikosoikeudenkäyntilaki	laki oikeudenkäynnistä rikosasioissa (689/1997)
tiedonhallintalaki	laki julkisen hallinnon tiedonhallinnasta (906/2019)
tietosuoja-asetus, yleinen tietosuoja-asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)
tietoverkkorikosdirektiivi	Euroopan parlamentin ja neuvoston direktiivi 2013/40/E, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta
TrVM	eduskunnan tarkastusvaliokunnan mietintö
VAHTI	julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja keskeisten palveluiden tuottamisesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelin
YTJ-laki	yritys- ja yhteisötietolaki (244/2001)

1 Tiivistelmä

Valtiovarainministeriö asetti 30.3.2021 työryhmän ajalle 1.4.2021–30.9.2022 selvittämään julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeita sekä tekemään ehdotukset tarvittavasta lainsäädännön uudistamisesta. Työryhmän tavoitteena on tarkistaa julkisen hallinnon tietojärjestelmien sääntelyä, jolla varmistetaan hyvän hallinnon ja oikeusturvan sekä virkavastuun toteutuminen, erityisesti automaattisessa päätöksenteossa.

Tämä arviomuistio koskee tietojärjestelmiin kohdistuvaa sääntelyä ja sen kehittämistarpeita erityisesti silloin, kun tietojärjestelmää käytetään hallintoasioiden käsittelyssä tai tosiasiallisessa hallintotoiminnassa palveluja tuotettaessa, riippumatta siitä, onko toimintaprosessi automatisoitu joko kokonaan tai osittain. Arviomuistiossa tarkastellaan tietojärjestelmiä koskevan sääntelyn nykytilaa, ottaen huomioon myös Euroopan unionin sääntely, ja todetaan seuraavat sääntelytarpeet. Arviomuistiossa käsitellään myös tietojärjestelmien vaatimuksenmukaisuusarviointia koskevaa yleislainsäädäntöä.

Tietojärjestelmän käyttö ja kehittäminen

Yleislainsäädännössä ei ole säädetty tietojärjestelmän olennaisista vaatimuksista asian käsittelyn asianmukaisuuden ja selvittämisvelvollisuuden toteuttamisessa. Lainalaisuusperiaatteen kannalta sääntelyä voidaan pitää jossakin määrin puutteellisena. Työryhmän näkemyksen mukaan tällaisista tietojärjestelmien olennaisista vaatimuksista voitaisiin säätää lailla. Työryhmä pitää erityisesti tarpeellisena, että ainakin ne tietojärjestelmien osat, joissa käsitellään hallintoasioita täysin automatisoidussa toimintaprosesseissa, kuuluisivat tämän sääntelyn piiriin. Lisäksi työryhmän näkemyksen mukaan tietojärjestelmien kehittämisen ja käytön ohjaukseen ja valvontaan liittyviä vastuita tulisi eri viranomaisten välillä täsmentää tai selkeyttää yleisemminkin tietojärjestelmiä koskevassa lainsäädännössä.

Työryhmä pitää tarpeellisena, että hallinnon asiakas saa tiedot siitä, mihin yksilöityihin tietoihin viranomainen perustaa päätöksentekonsa niissä tilanteissa, joissa päätös voidaan tehdä täysin automatisoidusti. Lisäksi tulisi kertoa yleisen tietosuoja-asetuksen (EU) 2016/679 edellyttämää yksilöidymmin siitä, että asia saatetaan käsitellä täysin automaattisesti. Työryhmä ei kuitenkaan pidä tarkoituksenmukaisena, että toimintaprosessien algoritmit tulisi julkistaa tai esittää asianosaiselle. Työryhmä ehdottaa, että hallintopäätöksiin sisällytettävää asianosaisen tietosuojaa ja oikeusturvaa edistävä päätöksenteon läpinäkyvyys arvioitaisiin osana hallintolain uudistamistarpeita automatisoidun päätöksenteon mahdollistamista koskevassa valmistelussa.

Tietojärjestelmien käyttöönottovaiheeseen liittyvää sääntelyä tulisi kehittää siten, että tietojärjestelmän kelvollisuus käyttöönotettavaksi on varmistettu asianmukaisella suunnittelulla, dokumentoinnilla sekä testauksella. Teknisiin ongelmiin varautumiseen tulisi olla nykyistä selkeämmät ja täsmällisemmät toimintavelvollisuudet.

Virkavastuu

Tietojärjestelmien kehittäminen, käyttöönotto ja käyttö tulisi hahmottaa selkeämmin olennaisena osana julkisen vallan käyttöä. Työryhmän arvion mukaan virkavastuun toteuttaminen on mahdollista kehittämällä päätöksentekojärjestelmien ja automatisoitujen toimintaprosessien sisäistä ja ulkoista arviointi- ja varmistusmenettelyä. Algoritmien ja järjestelmien tekninen sekä juridinen arviointi sekä niihin liittyvät täsmälliset toimintavelvollisuudet voivat muodostaa ne virkatoimet, joihin perustuslaissa tarkoitettu virkavastuu voidaan kohdentaa henkilötasolla.

Työryhmän mukaan viranomaisen toimintaan pitäisi kohdistaa selkeitä toimintavelvollisuuksia tietojärjestelmien kehittämisessä ja käyttöönotossa siten, että hyvän hallinnon ja oikeusturvan vaatimukset on varmistettu ennakollisesti toimintaprosesseissa.

Tietovarantojen käyttö ja laatu

Työryhmä katsoo, että riittävä tiedon laatu on asianmukaisen asiankäsittelyn ja lainmukaisen hallintoasian käsittelyn edellytys. Tietovarantojen laadun, tietovarantojen vastuiden, ja tietojen käytön vastuiden osalta automaattinen päätöksenteko edellyttää nykyistä tarkempaa sääntelyä. Yleissääntelyn avulla on vaikeaa hahmottaa esimerkiksi sitä, miten tiedot tulisi tarkistaa missäkin tilanteessa, ja milloin viranomaisen voi arvioida tarkistaneen käyttämänsä tiedot riittävästi ja täyttäneensä selvittämisvelvollisuutensa.

Tietoja hyödyntävän viranomaisen on pystyttävä tarvittaessa esittämään, miten viranomaisen tiedot ovat päätöksentekoa vartan muodostuneet tietovarantoon, erityisesti niissä tilanteissa, joissa vastuu yhteiskäyttöisen tietovarannon laadusta on säädetty tietojen ilmoittajalle.

Häiriötilanteisiin varautuminen

Työryhmän näkemyksen mukaan julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, tiedonhallintalaki) tai tietojärjestelmien olennaisia vaatimuksia koskevassa säädöksessä tulisi säätää varautumiseen liittyvistä vaatimuksista. Viranomaisen on varauduttava toiminnassaan siihen, että tietojärjestelmät vikaantuvat tai niiden toiminta muusta syystä estyy. Viranomaisen on pystyttävä suorittamaan tehtävänsä myös tilanteissa, joissa tietojärjestelmää ei voida käyttää.

Työryhmä katsoo, että automaattisen päätöksenteon tukeutuminen ulkoisiin tietovarantoihin edellyttäisi varmuutta tietojen saantiin, sekä sovittuja menettelyjä, joilla häiriötilanteissa tietojärjestelmät pystyvät toimimaan, tai vähintäänkin ilmoittamaan häiriöstä.

Tietojärjestelmien vaatimusmukaisuuden arviointi

Työryhmän mukaan olisi arvioitava, mitä vaatimuksia vasten tietojärjestelmien vaatimuksenmukaisuutta arvioidaan, ja tulisiko arviointiprosessia tarkentaa lainsäädännössä.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011, arviointilaki) sekä tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, arviointilaitoslaki) nimekkeitä ja soveltamisalaa olisi tarkistettava. Yhtenä vaihtoehtona on, että viranomaisten tietojärjestelmien mahdolliset lakisääteiset arvioinnit suoritettaisiin viranomaisen toimesta arviointilakia noudattaen – mahdollisesti viranomainen voisi käyttää apunaan yksityisiä, tietyn pätevyyden omaavia yksityisiä arvioijia. Vaihtoehtoisesti arviointilaissa olisi säädettävä nykyistä laajemmin viranomaisten tietojärjestelmien vaatimustenmukaisuuden arvioinnista sekä arvioitava uudelleen arviointilaitosten pätevyysalueita ja -vaatimuksia.

Vaatimustenmukaisuuden osoittamisvelvollisuus niissä tapauksissa, kun se katsotaan tarpeelliseksi, kuuluisi säätää laissa. Osoittamisvelvollisuus sisältyisi säädettäviin tietojärjestelmän käyttöönottoa ja käyttöä koskeviin vaatimuksiin. Lisäksi tulisi harkita, missä määrin ulkopuolisen arvioijan suorittama arviointi ja hyväksyntä olisi pakollista, ja milloin riittäisi viranomaisen lakiin perustuva itsearviointi, testaus ja valvonta, tai muu vastaava. Lähtökohtaisesti teknisluonteinen arviointi, joka perustuu yleislaissa säädettyjen vaatimusten mukaisuuden arviointiin, voidaan antaa ulkopuolisen arvioijan tai viranomaisen tehtäväksi. Kuitenkin tietojärjestelmän toimintalogiikan arviointi ja varmistaminen kuuluvat kullekin asiankäsittelyssä toimivaltaiselle viranomaiselle.

Lisäksi viranomaisen ja sen tietojärjestelmien tietoturvallisuuteen liittyvästä fyysisen turvallisuuden arvioinnista olisi mahdollisesti tarpeen säätää kansallisella tasolla.

Arviointilaitoslakia tulisi muuttaa siten, että siinä asetetaan sekä arviointilaitokselle että sen palveluksessa olevalle arvioitsijalle yksilöidyt vaatimukset, joita voidaan lakitasoiseen sääntelyyn perustuen valvoa. Lisäksi arviointilaitoslakia tulisi muuttaa siten, että toimivaltaisella viranomaisella on selkeä ja perusteltu toimivalta päättää akkreditoinnista ja suorittaa kelpoisuusvaatimusten noudattamista koskevaa valvontaa.

2 Sammandrag

Den 30 mars 2021 tillsatte finansministeriet en arbetsgrupp för mandatperioden 1.4.2021–30.9.2022 för att bedöma behoven för att utveckla lagstiftningen om informationssystem inom den offentliga förvaltningen och framföra förslag om nödvändig revidering av lagstiftningen. Arbetsgruppens mål är att se över bestämmelserna om informationssystem inom den offentliga förvaltningen genom vilka man säkerställer att god förvaltning och rättssäkerhet samt tillgodoser tjänsteansvar särskilt vid automatiserat beslutsfattande.

Denna bedömningspromemoria gäller lagstiftningen om informationssystem och behovet av att utveckla den, i synnerhet då informationssystemen används vid behandling av förvaltningsärenden eller i den faktiska förvaltningsverksamheten när tjänster produceras, oberoende av ifall verksamhetsprocessen har automatiserats helt eller delvis. I bedömningspromemorian granskas även nuläget i lagstiftningen om informationssystem, även med hänsyn till regleringen inom EU, och fastställs följande behov av lagstiftning. I bedömningspromemorian behandlas även den allmänna lagstiftningen om bedömningen av informationssystemens överensstämmelse med krav.

Användning och utveckling av informationssystem

Den allmänna lagstiftningen saknar bestämmelser om väsentliga krav på informationssystem vid genomförandet av ändamålsenlighet i behandlingen av ärenden och skyldigheten att lämna uppgifter. Med hänsyn till legalitetsprincipen kan lagstiftningen i en viss mån anses bristfällig. Enligt arbetsgruppens åsikt är det möjligt att genom lagstiftning föreskriva om sådana väsentliga krav på informationssystem. Arbetsgruppen anser att det i synnerhet är nödvändigt att åtminstone de delar av informationssystemen där förvaltningsärenden behandlas i helt automatiserade verksamhetsprocesser ska omfattas av denna lagstiftning. Enligt arbetsgruppens åsikt ska dessutom ansvaret i anknytning till utveckling och styrning av och tillsyn över användningen av informationssystem mellan olika myndigheter specificeras eller klarläggas mer allmänt i lagstiftningen om informationssystem.

Arbetsgruppen anser att det är nödvändigt att en kund till förvaltningen får information om utifrån vilka uppgifter en myndighet fattar sina beslut i situationer där beslutet kan fattas helt automatiserat. Dessutom ska man enligt vad som förutsätts i dataskyddsförordningen (EU) 2016/679 redogöra mer preciserat om att det är möjligt att ärendet behandlas helt automatiserat. Arbetsgruppen anser dock inte att det är ändamålsenligt att algoritmerna för beslutsprocesser ska offentliggöras eller visas för en part. Arbetsgruppen föreslår att den transparens inom beslutsfattande som inkluderas i förvaltningsbeslut för

att främja en parts dataskydd och rättssäkerhet ska bedömas som en del av behoven att revidera förvaltningslagen i beredningen som gäller möjliggörandet av automatiserat beslutsfattande.

Lagstiftningen om fasen för införande av informationssystem ska utvecklas så att informationssystemets duglighet för att införas har säkerställts genom ändamålsenlig planering, dokumentering och testning. Tydligare och mer exakta skyldigheter att vidta åtgärder ska fastställas för beredskap inför tekniska problem.

Tjänsteansvar

Utvecklingen, införandet och användningen av informationssystem ska gestaltas tydligare som en väsentlig del av utövande av offentlig makt. Enligt arbetsgruppens bedömning är det möjligt att verkställa tjänsteansvaret genom att utveckla den interna och externa bedömnings- och kontrollpraxisen i system för beslutsfattande och automatiserade verksamhetsprocesser. Tekniska och juridiska bedömningar av algoritmer och system med tillhörande exakta skyldigheter att vidta åtgärder kan utgöra de tjänsteuppdrag till vilka det i grundlagen avsedda tjänsteansvaret riktas på personnivå.

Enligt arbetsgruppen ska tydliga skyldigheter att vidta åtgärder riktas till myndigheternas verksamhet i utvecklingen och införandet av informationssystem så att krav på god förvaltning och rättssäkerhet tillgodoses på förhand i verksamhetsprocesserna.

Användning av och kvalitet på datalager

Arbetsgruppen anser att tillräcklig kvalitet på information är en förutsättning för ändamålsenlig ärendehantering och lagenlig behandling av förvaltningsärenden. Vad gäller kvaliteten på datalager, ansvar avseende datalager och ansvar avseende användningen av uppgifter förutsätter automatiserat beslutsfattande lagstiftning som är exaktare än den nuvarande lagstiftningen. Det är till exempel svårt att med den allmänna lagstiftningen tolka hur uppgifter ska kontrolleras i en viss situation och när en myndighet kan bedömas ha kontrollerat de uppgifter myndigheten använder i en tillräcklig utsträckning och fullgjort sin utredningsskyldighet.

Myndigheten som använder uppgifterna ska vid behov kunna framföra hur myndighetens uppgifter har uppkommit i datalagret för beslutsfattande, i synnerhet i situationer där ansvaret för kvaliteten på ett gemensamt datalager har föreskrivits för anmälaren av uppgifterna.

Beredskap inför störningar

Enligt arbetsgruppens åsikt ska lagen om informationshantering inom den offentliga förvaltningen (906/2019, informationshanteringslagen) eller en förordning om väsentliga krav på informationssystem innehålla bestämmelser om krav på beredskap. Myndigheter ska i sin verksamhet vara beredda på att fel uppstår i informationssystem eller att systemens funktion förhindras av någon annan orsak. Myndigheterna ska kunna sköta sina uppgifter även i situationer där informationssystem inte kan användas.

Arbetsgruppen anser att ett på externa datalager baserat automatiserat beslutsfattande skulle förutsätta en säker tillgång till uppgifter samt överenskomna förfaranden som gör det möjligt för informationssystem att fungera under störningar eller åtminstone meddela om störningarna.

Bedömningen av informationssystemens överensstämmelse med krav

Enligt arbetsgruppen ska det bedömas mot vilka krav informationssystemens överensstämmelse med krav ska bedömas och huruvida bedömningsprocessen ska preciseras i lagstiftningen.

Beteckningar i och tillämpningsområden för lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011, bedömningslagen) och lagen om bedömningsorgan för informationssäkerhet (1405/2011, lagen om bedömningsorgan) bör kontrolleras. Ett alternativ är att en myndighet genomför eventuella lagstadgade bedömningar av myndigheternas information med beaktande av bedömningslagen – eventuellt kan myndigheten anlita privata bedömare med någon viss behörighet. Alternativt ska det i bedömningslagen i en större omfattning än för närvarande föreskrivas om bedömningen av överensstämmelse med krav i myndigheternas informationssystem och göras en ny bedömning av bedömningsorganens kompetensområden och -krav.

Skyldigheten att påvisa överensstämmelse med krav i de fall det anses nödvändigt ska föreskrivas genom lag. Påvisningsskyldigheten skulle inkluderas i de krav som föreskrivs om införandet och användningen av informationssystem. Dessutom ska man överväga i vilken mån en utomstående bedömares bedömning och godkännande ska vara obligatoriska, och när det skulle vara tillräckligt med egenbedömning, testning och tillsyn, eller något liknande. I princip kan en teknisk bedömning som grundar sig på att bedöma överenstämmelsen med de krav som ingår i den allmänna lagen överlåtas för att utföras av en extern bedömare eller myndighet. Emellertid är det respektive behörig myndighet inom ärendehantering som ansvarar för bedömningen och säkerställandet av verksamhetslogiken i informationssystemet.

Dessutom är det eventuellt nödvändigt att på nationell nivå föreskriva om bedömningen av den fysiska säkerheten hos myndigheten och dataskyddet i myndighetens informationssystem.

Lagen om bedömningsorgan ska ändras så att det i lagen både för bedömningsorgan och de av organ anställda bedömarna fastställs specificerade krav över vilka tillsyn kan utövas utifrån reglering på lagnivå. Dessutom ska lagen om bedömningsorgan ändras så att den behöriga myndigheten har en tydlig och motiverad befogenhet att fatta beslut om ackreditering och utöva tillsyn över iakttagandet av behörighetskrav.

3 Johdanto

Julkisessa hallinnossa on käytetty vuosikymmeniä tietojärjestelmiä hallintoasioiden käsittelyssä sekä muussa julkisten palvelujen tuottamisessa. Tietojärjestelmien kehittämiseen ja käyttöön vaikuttava sääntely on kuitenkin hajanaista. Tietojärjestelmä sääntelykohteena ei ole vakiintunut, vaan se esiintyy eri yhteyksissä lainsäädännössä vaihtelevilla merkityksillä. Osa sääntelystä on yleislaintasoista ja osa tiettyyn toimialaan sidottua erityislainsäädäntöä. Osa sääntelystä on uutta ja osa kymmeniä vuosia vanhaa. Sääntely voi kohdistua suoraan tietojärjestelmien kehittämiseen ja käyttöön, mutta valtaosa sääntelystä on välillistä menettelysääntelyä, joka vaikuttaa tietojärjestelmien toiminnallisuuksiin.

Valtiovarainministeriö asetti 30.3.2021 työryhmän[1] ajalle 1.4.2021–30.9.2022 selvittämään julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeita sekä tekemään ehdotukset tarvittavasta lainsäädännön uudistamisesta. Ensimmäisessä vaiheessa työryhmän tuli asettamispäätöksen mukaan arvioida hallinnon tietojärjestelmien kehittämiseen ja käyttöön liittyvän yleislainsäädännön ajantasaisuus erityisesti ottamalla huomioon automaattiseen päätöksentekoon, tekoälyn hyödyntämiseen sekä tietojärjestelmien tietoturvallisuuden varmistamiseen liittyvät sääntelytarpeet. Työryhmän tavoitteena on tarkistaa julkisen hallinnon tietojärjestelmien kehittämisen ja käytön vaatimuksia sekä vaatimuksenmukaisuuden arviointia koskevaa sääntelyä, jolla varmistetaan hyvän hallinnon ja oikeusturvan sekä virkavastuun toteutuminen hallinnon toimintaprosesseissa[2], erityisesti automaattisessa päätöksenteossa.

Euroopan unionin yleisen tietosuoja-asetuksen[3] 22 artiklassa säädetään rekisteröidyn oikeudesta olla joutumatta kokonaisuudessaan automatisoidun päätöksenteon kohteeksi, jos tällaisella käsittelyllä on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Tietosuoja-asetuksessa tarkoitettujen automatisoitujen päätösten tekeminen on kuitenkin sallittu, jos päätös perustuu rekisterinpitäjään sovellettavaan unionin oikeuteen tai jäsenvaltion lainsäädäntöön, jossa vahvistetaan asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi. Tämä käsittelyn rajoitussäännös kohdistuu suhteellisen laajaan joukkoon toimia, joilla käsitellään henkilötietoja, kun hallintoasia ratkaistaan tai palveluja tuotetaan

1 VM059:00/2021

2 Lain julkisen hallinnon tiedonhallinnasta (906/2019) 2.1 §:n 10 kohdan mukaisesti *toimintaprosessilla* tarkoitetaan arviomuistiossa viranomaisen käsittely- tai palveluprosessia.

3 Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus), jäljempänä tietosuoja-asetus.

tietojärjestelmien avulla. Rajoitussäännös kohdistuu tietojärjestelmässä niihin toiminta-prosesseihin, jotka ovat täysin automatisoituja ja joiden lopputuloksena on hallintopäätös tai muu ratkaisu, joka aiheuttaa ratkaisun kohteena olevalle oikeudellisia vaikutuksia samalla tapaa kuin esimerkiksi hallintopäätös. Tällaisia automatisoituja prosesseja voi olla myös esimerkiksi palveluihin ohjaavissa digitaalisissa palveluissa.

Työryhmän tehtävä liittyy myös eduskunnan perustuslakivaliokunnan kannanottoihin automatisoidun päätöksenteon käyttöedellytyksistä julkisen hallinnon päätöksenteossa.[4] Perustuslakivaliokunnan mukaan automaattisen päätöksenteon sääntely on henkilötietojen suojaan liittyvien kysymysten ohella merkityksellistä erityisesti perustuslain 21 §:ssä turvattujen hyvän hallinnon periaatteiden ja 118 §:ssä säädetyn virkavastuun kannalta. Myös ylimmät laillisuusvalvojat ovat kiinnittäneet viime vuosina huomiota tietojärjestelmien käyttöön liittyviin ongelmiin, kun automatisoituja toimintaprosesseja käytetään hallintoasian käsittelyssä.[5]

Euroopan komissio julkaisi 21.4.2021 ehdotuksensa COM (2021) 206 asetukseksi, jossa säädettäisiin tiettyjen tekoälyjärjestelmien käyttötarkoitusten edellytyksistä (tekoäly-asetus). Ehdotuksella on pitkällä aikavälillä vaikutuksia myös julkisen hallinnon tietojärjestelmien kehittämiseen silloin, kun tietojärjestelmässä on toiminnallisuuksia, jotka sisältyvät eurooppalaisessa sääntelyssä tarkoitettuun tekoälyjärjestelmän käsitteeseen, ja näitä toiminnallisuuksia käytetään sellaisessa tarkoituksessa, jota asetuksella säänneltäisiin.

Tämä arviomuistio koskee tietojärjestelmiin kohdistuvaa sääntelyä ja sen kehittämistarpeita silloin, kun tietojärjestelmää käytetään hallintoasioiden käsittelyssä tai tosiasiallisessa hallintotoiminnassa palveluja tuotettaessa riippumatta siitä, onko toiminta-prosessi automatisoitu joko kokonaan tai osittain. Arviomuistiossa käsitellään kuitenkin erityisesti täysin automatisoidun toimintaprosessin kehittämiseen ja käyttöönottoon liittyviä sääntelytarpeita, jolloin kysymyksenasettelu liittyy kiinteästi tietosuoja-asetuksessa tarkoitetun automatisoidun päätöksenteon käyttöönoton laillisten edellytysten arviointiin ja sääntelyn edellytyksiin.

4 PeVL 7/2019 vp, PeVL 70/2018 vp, PeVL 62/2018 vp ja PeVL 78/2018 vp.

5 AOA 3379/2018, 20.11.2019; AOA 2216/2018, 20.11.2018; AOA 2898/2018, 25.11.2019; OKA OKV/131/70/2020, 20.4.2021.

4 Tietojärjestelmät sääntelykohteena

4.1 Tietojärjestelmä

Tietojärjestelmä sääntelykohteena ei ole vakiintunut. *Tietojärjestelmän* käsite on määritelty viranomaistoiminnassa yleislain tasolla julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, tiedonhallintalaki) 2.1 §:n 3 kohdassa, jonka mukaan tietojärjestelmällä tarkoitetaan tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annetun lain (1406/2011, arviointilaki) 2.1 §:n 1 kohdan määritelmä tietojärjestelmästä vastaa tiedonhallintalaissa säädettyä. Lisäksi omana sääntelykohteenaan arviointilain 2.1 §:n 2 kohdassa on *tietoliikennejärjestelyt*, joilla tarkoitetaan tiedonsiirtoverkosta, tiedonsiirtolaitteista, ohjelmistoista ja muista tietojenkäsittelystä koostuvista järjestelyistä muodostuvaa järjestelmää. Koska tietojärjestelmien toiminta monin osin riippuu tietoliikenteen toimivuudesta ja tietojärjestelmiä käytetään pääosin tietoliikenneyhteyksien avulla, voidaan katsoa, että tietoliikennejärjestelyt ovat osa tietojärjestelmän käsitteen sisältöä. Kuitenkin tietoliikenteeseen liittyvät tekniset järjestelyt muodostavat oman kokonaisuutensa siten, että ne eivät pääsääntöisesti ole sidoksissa yksittäiseen tietojärjestelmään.

Erityislainsäädäntö sisältää jonkin verran tietojärjestelmän käsitteen määrityksiä. Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007, asiakastietolaki) 3.1 §:n 6 kohdan mukaan mainitussa laissa tietojärjestelmällä tarkoitetaan sosiaali- tai terveydenhuollon asiakastietojen sähköistä käsittelyä varten toteutettua ohjelmistoa tai järjestelmää, jonka avulla tallennetaan ja ylläpidetään asiakas- tai potilasasiakirjoja ja niissä olevia tietoja sekä kerätyistä tiedoista muodostettua automaattisen tietojenkäsittelyn avulla ylläpidettävää tiedostoa tai tietovarantoa, jonka valmistaja on erityisesti suunnitellut sosiaali- tai terveydenhuollon asiakas- tai potilasasiakirjojen ja niissä olevien tietojen käsittelyyn. Lisäksi tietojärjestelmällä tarkoitetaan välityspalvelua, jolla sosiaali- tai terveydenhuollon asiakastietoja välitetään jäljempänä 14.1 §:ssä tarkoitettuihin Kansaneläkelaitoksen ylläpitämiin valtakunnallisiin tietojärjestelmäpalveluihin.

Myös rikoslain (39/1889) 38 luvun 13 § sisältää tietojärjestelmän määritelmän, jonka mukaan tietojärjestelmällä tarkoitetaan myös tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2013/40, jäljempänä tietoverkkorikosdirektiivi, 2 artiklan a kohdassa tarkoitettua:

1. laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten; sekä

2. dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään sen tai niiden toimintaa, käyttöä, suojausta tai huoltoa varten.

Rikoslaissa tarkoitettu tietojärjestelmän määritelmä on tarkoitettu sovellettavaksi vain siinä mainittujen säännösten yhteydessä. Määritelmä on sinällään avoin ja tekniikka-neutraali.[6] Tietojärjestelmän käsite kattaa rikoslaissa myös tietojärjestelmässä olevan datan ja tietoliikennejärjestelyt.

Digitaalisten palvelujen tarjoamisesta annetun lain (306/2019, digipalvelulaki) 2.1 §:n 3 kohdan mukaan digitaalisella palvelulla tarkoitetaan verkkosivustoa tai mobiilisovellusta sekä niihin liittyviä toiminnallisuuksia. Digitaalinen palvelu voi olla itsenäinen tietojärjestelmä tai tietojärjestelmän osa, joten tietojärjestelmiin kohdistuva sääntely koskee lähtökohtaisesti myös digitaalisen palvelun toiminnallisuuksia.

Tekijänoikeuslainsäädännön näkökulmasta sääntelykohteena on *tietokoneohjelma*, mutta sitä ei ole varsinaisesti määritelty tekijänoikeuslaissa. Tietokoneohjelmien oikeudellisesta suojasta annetussa direktiivissä on varsin yleispiirteinen määritelmä tietokoneohjelmalle – tietokoneohjelmalla tarkoitetaan missä tahansa muodossa olevia ohjelmia, laitteistoon sisältyvät ohjelmat mukaan lukien. Tämä käsite sisältää myös tietokoneohjelman kehittämiseen tähtäävän valmistelevan suunnittelutyön, jos valmisteleva työ on luonteeltaan sellaista, että sen tuloksena voi myöhemmässä vaiheessa olla tietokoneohjelma.[7]

Erityislainsäädännössä käytetään myös tietojärjestelmän käsitettä yhteyksissä, joissa ei varsinaisesti säädetä tietojärjestelmästä, vaan tietojärjestelmän tietosisällöstä sekä niiden käsittelyn säännöistä. Tällaisia tietojärjestelmiä ovat muun muassa väestötietojärjestelmä[8],

6 HE 232/2014 vp, s. 38.

7 Euroopan parlamentin ja neuvoston direktiivi 2009/24/EY, annettu 23 päivänä huhtikuuta 2009, tietokoneohjelmien oikeudellisesta suojasta, resitaali 7.

8 Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (661/2009)

yritys- ja yhteisötietojärjestelmä[9], hätäkeskustietojärjestelmä[10], metsätietojärjestelmä[11], rakennerahasto-ohjelman tietojärjestelmä[12], ympäristösuojelun tietojärjestelmä[13], yrityspalvelujen asiakastietojärjestelmä[14] sekä tie- ja katuverkon tietojärjestelmä[15].

Sääntely on kuitenkin muuttumassa, sillä esimerkiksi maaseutuelinkeinohallinnon tietojärjestelmä[16] on muutettu ruokahallinnon tietovarannoksi[17] ja oikeushallinnon valtakunnallinen tietojärjestelmä on muutettu oikeushallinnon tietovarannoksi.[18]

Henkilötietojen suojaa koskevassa sääntelyssä on sääntelykohteena monissa säädöksissä automaattinen tietojenkäsittely[19] taikka tietojärjestelmää on määritelty automaattisen tietojenkäsittelyn avulla ylläpidettäväksi.[20] Jossain tilanteissa myös tietojärjestelmä ja (henkilö)rekisteri vaikuttaisivat olevan synonyymejä toisilleen.[21] Lisäksi koneellista allekirjoitusta koskevassa sääntelyssä päätöksen tuottaminen on sidottu automaattiseen tietojenkäsittelyyn.[22]

9 Yritys- ja yhteisötietolaki (244/2001)

10 Laki hätäkeskustoiminnasta (692/2010)

11 Laki Suomen metsäkeskuksen metsätietojärjestelmästä (419/2011)

12 Laki alueiden kehittämisen ja rakennerahastohankkeiden rahoittamisesta (8/2014)

13 Ympäristönsuojelulaki (527/2014)

14 Laki yrityspalvelujen asiakastietojärjestelmästä (293/2017)

15 Laki tie- ja katuverkon tietojärjestelmästä (991/2003)

16 Laki maaseutuelinkeinohallinnon tietojärjestelmästä (284/2008)

17 Hallituksen esitys laiksi ruokahallinnon tietovarannosta HE 262/2020 vp, hyväksytty eduskunnassa 26.5.2021 EV 51/2021 vp.

18 Laki oikeushallinnon valtakunnallisesta tietojärjestelmästä (372/2010) kumottiin lailla oikeushallinnon valtakunnallisesta tietovarannosta (955/2020).

19 Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) 19 §, laki kiinteistötietojärjestelmästä ja siitä tuotettavasta tietopalvelusta (453/2002) 1 §

20 Yritys- ja yhteisötietolaki (244/2001) 2 §:n 5 kohta ja laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), ulosottolaki (705/2007) 24 §

21 Esimerkiksi tietosuojalaki (1050/2018) 29.4 §, rahanpesun selvittelykeskuksesta annettu laki (445/2017) 3 § ja laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (661/2009) 3.1 §, laki hätäkeskustoiminnasta (692/2010) 16 §, Suomen metsäkeskuksen metsätietojärjestelmästä annettu laki (419/2011) 3 § sekä siviilipalveluslaki (1446/2007) 87 §.

22 Esimerkiksi rehulaki (1263/2020) 49 §, siemenlaki (600/2019) 43 § ja tavaramerkkilaki (544/2019) 104 §.

Sääntelyssä ei ole vakiintunutta *tekoälyn* tai *keinoälyn* (engl. artificial intelligence, AI) käsitettä, vaikka tätä käsitettä käytetään paljon erityisesti julkisessa keskustelussa. Tekoäly on joukko erilaisia kehittyviä ohjelmistoja ja teknologioita, joille ei voidakaan antaa ainakaan toistaiseksi yksiselitteistä määritelmää. Euroopan komissio on ehdotuksessaan tekoälyasetukseksi luonnostellut tekoälyn ja tekoälyjärjestelmän määritelmät, pohjautuen kuitenkin teknologioiden luetteloon, jota tarvittaessa myöhemmin täydennetään. Näin ehdotuksessa on tunnistettu teknologian kehittymisen asettamat haasteet sellaiselle sääntelylle, jonka soveltamisala halutaan muodostaa nimenomaan tekoälyn käsitteen kautta.[23]

Automatisoidun päätöksenteon mahdollistavien tietojärjestelmien ja ohjelmistojen sekä hallinnossa muuten hyödynnettävän automaation käsitteistö ei ole vakiintunutta.[24] Tietojärjestelmiin kohdistuvaa sääntelyä voidaan lähestyä ainakin seuraavista näkökulmista:

- tietojärjestelmä kehittämiskohteena ja tietojärjestelmän olennaiset vaatimukset
- tietojärjestelmän tarkoitus ja siinä käsiteltävät tiedot
- tietojärjestelmässä olevat toiminnallisuudet, joilla operoidaan toimintaprosesseja:
  - päätöksenteon tuki
  - automatisoitu päätöksenteko
  - tekoälyyn pohjautuva päätöksenteko
  - palveluohjaus
- tietojärjestelmä automaattisen tietojenkäsittelyn välineenä.

Tietojärjestelmät ovat osa tietoverkkojen kokonaisuutta eivätkä tietojärjestelmät pääosin toimi ilman tietoverkkoa (tietoliikennejärjestelyitä). Tässä suhteessa tietojärjestelmäsääntelyyn voidaan katsoa kuuluvaksi tietoverkkojen käyttöön kohdistuva sääntely, vaikka tietoverkkoja koskeva sääntely ei kohdistukaan tyypillisesti tiettyyn tietojärjestelmään.

4.2 Johtopäätöksiä

Voimassa olevassa lainsäädännössä käytetyistä määritelmistä ei voida muodostaa täysin yhtenäistä tietojärjestelmän sääntelykohdetta. Kussakin laissa tietojärjestelmä saa merkityssisältönsä määritelmäsäännösten kautta. Kuitenkin tietojärjestelmää koskevan

23 Ks. myös tekoälyn määrittelemisen merkityksestä, erityisesti sääntelyn tarkkarajaisuudelle, valtioneuvoston kanta ehdotukseen tekoälyasetuksesta, U 28/2021 vp, kohta 9.

24 Pöysti, Tuomas (2020): Luottamuksesta hallinnon automaattiseen päätöksentekoon teoksessa Juhlakirja Pekka Vihervuori 1950-25/8-2020, s. 347–349.

sääntelyn tulisi muodostaa yleislakien ja erityislakien systematiikassa eheä kokonaisuus siten, että käytetyt määritelmät eivät johda tulkinnanvaraisuuksiin sen suhteen, miltä osin ja miten yleislaissa säädettyä sovelletaan erityislain perusteella perustettuun tietojärjestelmään toiminnallisuuksineen.

Tietojärjestelmät ja niiden toiminnallisuudet ovat olennainen osa viranomaisissa hallintoasioiden käsittelyä. Kuitenkin tietojärjestelmien käyttö erilaisissa hallintoasioissa ja toimintaprosesseissa vaihtelee, samoin kuin automatisoinnin aste jopa samassa asiankäsittelyn asiaryhmässä. Tähän voivat vaikuttaa muun muassa asiankäsittelyyn liittyvät kontrollit, jotka ohjaavat käsittelyyn joko automaattisessa prosessissa tai manuaaliseen prosessiin, josta käsittely voi edelleen palata automaattiseen prosessiin.

Siten määriteltäessä hallinnon tietojärjestelmille olennaisia vaatimuksia, ei sääntelyä voida kohdentaa kaikilta osin yleisesti tietojärjestelmään, vaan tietojärjestelmässä käsiteltäviin, tiedonhallintalaissa tarkoitettuihin toimintaprosesseihin. Työryhmän näkemyksen mukaan hallinnon tietojärjestelmien sääntelyä kehitettäessä on arvioitava vaatimuskohtaisesti, milloin vaatimus voidaan kohdistaa yleisesti tiedonhallintalaissa tarkoitetun tietojärjestelmän toiminnallisiin ja teknisiin vaatimuksiin ja milloin vaatimukset kohdistuvat tietojärjestelmän sellaisiin toiminnallisuuksiin, joilla on merkitystä esimerkiksi asianosaisen oikeuksien turvaamiseksi ja viranomaisen toiminnan asianmukaisuuden varmistamiseksi.

Koska tekoäly on teknologiana vielä muuttuva ja kehittyvä, ja koska tekoälystä ei olisi mielekästä säätää kansallista määritelmää ainakaan tässä yhteydessä, ei sääntelyä olisi tarkoituksenmukaista kohdistaa nimenomaan tekoälyyn tai tekoälyksi tulkittavia teknologioita käyttäviin järjestelmiin. Sen sijaan sääntelyn olisi oltava mahdollisimman teknologiariippumatonta ja siten aikaa kestävää. Kunhan tietojärjestelmä täyttää sille laissa asetetut vaatimukset, ei sillä, millä teknologialla vaatimukset täytetään, ole merkitystä. Sääntelyä valmistellessa on kuitenkin tärkeää ottaa huomioon erilaisten teknologioiden ja niiden ympärillä käytävän keskustelun vaikutukset muun muassa julkisen hallinnon luotettavuuteen ja läpinäkyvyyteen.

5 Tietojärjestelmien kehittämiseen kohdistuvat vaatimukset

5.1 Suunnitteluvelvollisuus

Tietojärjestelmien kehittämistä ohjaa talouden suunnittelua, julkisia hankintoja, tietosuojaa ja tiedonhallintaa koskeva lainsäädäntö.

Valtion viranomaisissa talouden suunnittelua koskevista perusteista säädetään valtion talousarviosta annetussa laissa (423/1988) ja valtion talousarviosta annetussa asetuksessa (1243/1992) sekä määrätty valtiovarainministeriön määräyksessä toiminta- ja taloussuunnittelusta, julkisen talouden suunnitelman valmisteluun liittyvien kehys- ja muiden ehdotusten sekä valtion talousarvioehdotusten laadinnasta (VN/4842/2020) ja valtioneuvoston päätöksessä valtion talousarvion soveltamismääräyksistä (TM 9509). Kuntien ja kuntayhtymien talouden suunnittelu perustuu kuntalakiin (410/2015) ja sen nojalla annettuihin sisäisiin määräyksiin. Muiden viranomaisiksi rinnastuvien toimijoiden talouden suunnittelu perustuu erityislainsäädäntöön, joskin osalla talouden suunnittelu on osittain sidoksissa valtion talousarvioon. Tässä arviomuistiossa ei työryhmän toimeksiannon puitteissa arvioida tarkemmin tietojärjestelmien kustannusten kattamiseen tarkoitetun talouden suunnittelun sääntelyä.

Julkisista hankinnoista ja käyttöoikeussopimuksista annetussa laissa (1397/2016, hankintalaki) säädetään laissa tarkoitettujen kynnysarvojen ylittävissä hankinnoissa noudatettavista säännöistä. Hankintalain säännökset eivät sääntele hankinnan kohteen määrittämisestä, mutta hankinnan kohteella on vaikutus hankintalajin valintaan, hankintamenettelyyn sekä hankintailmoituksessa julkaistaviin tietoihin, kuten CPV-koodiin. Oikeuskäytännön mukaan hankintayksiköllä on laaja harkintavalta esimerkiksi tietojärjestelmähankinnoissa sen suhteen, miten se määrittelee hankinnan kohteen ja millaisia ominaisuuksia se hankinnan kohteelta edellyttää.[25] Tätä harkintavaltaa kuitenkin rajoittavat hankintalaissa säädetyt hankintoja koskevat periaatteet avoimuudesta, suhteellisuudesta sekä tasapuolisesta ja syrjimättömästä kohtelusta. Teknisten vaatimusten määrittämiseen esimerkiksi tietojärjestelmiä hankittaessa vaikuttavat muualla lainsäädännössä säädetyt vaatimukset muun muassa tietoturvallisuusvaatimusten täyttämisestä.

25 Esim. MAO 298/20, 25.6.2020, MAO 843/17, 22.12.2017 ja MAO 147/17, 23.3.2017

Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 4.2 §:n mukaan tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on asianmukaiset työvälineet tiedonhallintaa koskevien velvollisuuksien toteuttamiseksi. Säännöksen perustelujen mukaan asianmukaisten työvälineiden vaatimuksen tarkoituksena on huolehtia siitä, että viranomaiset voivat hoitaa tiedonhallintaan liittyvät tehtävänsä hyvän hallinnon edellyttämällä tavalla tehokkaasti ja tuloksellisesti. Säännöksellä korostetaan sitä, että tiedonhallinnassa tarvittavat työvälineet, kuten päätelaitteet, palvelimet ja ohjelmistot ovat tehtävien edellyttämällä tavalla ajantasaisia ja riittävän suojattuja siten, että työvälineiden käyttö tukee viranomaisten tehtävien hoitamista hyvän hallinnon edellyttämällä tavalla. Asianmukaisten työvälineiden hallinnointia varten tiedonhallintayksikköjen tulisikin suunnitella laitteistojen ja tietojärjestelmien elinkaaret siten, että näiden avulla viranomainen voi hoitaa tiedonhallintayksikössä sille laissa kuuluvat tehtävät asianmukaisesti. Säännöksellä on siten sidoksensa siihen, että viranomaisten on jo hankintoja valmisteltaessa otettava huomioon muun muassa perustuslain 21 §:stä lähtevät vaatimukset asianmukaisesta asiankäsittelystä ja käsittelyn viivytyksettömyydestä käsiteltäessä viranomaisen toimivaltaan kuuluvia asioita.

5.2 Toimintaprosessin automatisoinnin määritteleminen

Lainsäädäntö, viranomaisten määräykset ja ohjeet sekä muut lain soveltamisessa käytettävät lähteet on laadittu nk. luonnollisella kielellä. Tietoja ei ole ainakaan nykyisellä teknologialla mahdollista käsitellä automaattisesti tietojärjestelmässä antamalla sille käskyjä ainoastaan luonnollisella kielellä, vaan käskyt on jollain tasolla muunnettava tietojärjestelmän toimintalogiikan mukaiseksi kieleksi, ohjelmointikieleksi.[26]

Tyypillinen tapa toisintaa ihmisen suorittamaa toimintaprosessia, kuten asian käsittelyä ja ratkaisemista, tietojärjestelmän sisällä on kuvata toimintaprosessi erilaisina toimintasääntöinä, eli algoritmeina. Koko toimintaprosessi alusta loppuun voi olla toteutettavissa algoritmeina, tai prosessi voidaan toteuttaa osin algoritmien avulla ja osin virkamiehen toimesta. Erikseen määritellyt algoritmit eivät ole kuitenkaan ainoa mahdollinen tapa toteuttaa automaattista tietojenkäsittelyä. Tietokoneohjelma voi esimerkiksi matkia ihmiskäyttäjän toimintaa niin, että se pystyy toistamaan samat liikkeet ja toimet graafisen

26 On olemassa luonnollista kieltä ymmärtäviä chatbotteja ja muita vastaavia, koneoppivia malleja tai muita teknologioita käyttäviä tietojärjestelmiä tai ohjelmistoja, ja on mahdollista, että teknologian kehittyessä ohjelmointikielten merkitys vähenee tietojärjestelmien kehittämisessä ja käyttämisessä. Lisäksi on olemassa ns. Rules as a Code -malli, jossa lainsäädäntö laaditaan suoraan koneluettavaan ja ymmärrettävään muotoon. Kirjoitettuja säädöksiä ja ohjeita ilman ihmisen osallisuutta lukevaa ja tulkitsevaa tietojärjestelmää ei kuitenkaan pidetä tässä arviomuistiossa realistisena lähitulevaisuuden mahdollisuutena.

käyttöliittymän kautta ja luomaan toiminnan pohjalta algoritmin itse. Erilaisia ihmiskäsittelyä jäljitteleviä toteutustapoja kutsutaan ohjelmistorobotiikaksi tai robotisoiduksi prosessiautomaatioksi (Robotic Process Automation, RPA).

Nykyisessä sääntelyssä ei oteta kantaa siihen, kuka muuntaa lain soveltamisessa käytettävät lähteet tietojärjestelmän käsiteltävissä olevaan muotoon, millaisella prosessilla tämä tehdään, tai miten lopputulos olisi testattava ja varmistettavissa. Lain soveltamisen automatisoinnin toteuttamista ulkoistettaessa on myös otettava huomioon, mitä perustuslain 124 §:ssä säädetään julkisen hallintotehtävän antamisesta muulle kuin viranomaiselle. Onkin analysoitava tarkemmin, missä määrin automatisoinnin toteuttaminen on julkisen hallintotehtävän hoitamista tai jopa merkittävää julkisen vallan käyttöä, ja missä määrin on kyse pelkästä teknisestä toimenpiteestä. Automatisoinnin toteuttamisessa saatetaan myös tarvita erityisen laaja-alaista ja syvällistä asiantuntemusta, jota ei välttämättä ole edes mahdollista saada viranomaisen ulkopuolelta. Olisi siis hyvän hallinnon periaatteiden, lainalaisuusperiaatteen, virkamieshallinnon periaatteen sekä virkavastuun toteutumisen kannalta ongelmallista, jos toimintaprosessin automatisoinnin määritteleminen, toteuttaminen, testaaminen, käyttö ja valvonta tapahtuisi yksityisen toimesta muutoin kuin pelkkien teknisluontoisten toimenpiteiden osalta.

5.3 Testaus- ja varmistamisvelvollisuus

Yleislainsäädännössä ei ole säädetty selkeästi siitä, miten viranomaisten tietojärjestelmissä asianmukainen asiankäsittely varmistetaan tai miten viranomaisen tulisi osoittaa, että asianmukaisen asiankäsittelyn edellytykset on varmistettu tietojärjestelmän käytössä. Hallintolaissa omaksuttu virkamieshallintoperiaate ohjaa asiankäsittelyä prosessimaisesti ihmisen tekemänä työnä. Tilanteissa, joissa hallintoasioita käsitellään tietojärjestelmissä automatisoiduissa prosesseissa, merkitystä on ennakollisella sääntelyllä ja siihen liittyvillä menettelyillä, joilla voidaan varmistaa hyvän hallinnon, oikeusturvan, yhdenvertaisuuden, virkavastuun sekä muiden perustuslaista lähtevien vaatimusten toteutuminen hallintoasioiden käsittelyssä. Tällainen ennakolliseen kontrolloitavuuteen ja kehittämistyöhön kohdistuva sääntely on nykytilassa vähäistä ja välillistä.

Tiedonhallintalaissa on eräitä säännöksiä, jotka velvoittavat tietojenkäsittelyssä varmistamaan osana tietoturvallisuustoimenpiteitä käsittelyn asianmukaisuus sekä muiden perusoikeuksien toteuttaminen. Tiedonhallintalain 13.1 §:n mukaan tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Käytännössä säännös tarkoittaa tietojärjestelmien kehittämisessä sitä, että tiedonhallintayksikössä toimivien viranomaisten on suunniteltava tietoturvallisuustoimenpiteet ja mitoitettava ne riskiarvioinnin mukaisesti.

Tiedonhallintalain 13.2 §:n mukaan viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti. Säännös ei kohdenna sitä, milloin vikasietoisuutta ja toiminnallista käytettävyyttä on testattava, mutta tyypillisesti testaus tapahtuu tietojärjestelmän kehittämisen tai käyttöönoton yhteydessä hyväksymistestauksessa. Säännöksessä kuitenkin edellytetään säännöllisesti tapahtuvaa vikasietoisuuden ja toiminnallisen käytettävyyden testausta, joten sitä on tehtävä muulloinkin kuin tietojärjestelmän kehittämisvaiheessa. Säännöksessä vikasietoisuuden ja toiminnallisen käytettävyyden varmistamisvelvollisuus koskee olennaisia tietojärjestelmiä, joita ovat tyypillisesti viranomaisten hallintoasioiden käsittelyyn ja palvelujen tuottamiseen liittyvät tietojärjestelmät. Yleislainsäädännössä ei ole säädetty testauksen tai muun laadunvarmistamisen dokumentoinnista eikä kohdennetusti, millaiset tietojärjestelmät kuuluvat erityisen laadunvarmistamisen piiriin jo tietojärjestelmän kehittämisvaiheessa.

Tiedonhallintalain 13.3 §:n mukaan viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa. Suunnitteluvelvollisuuden tarkoituksena on varmistaa tietojärjestelmien toiminnallisuuksissa hyvän julkisuus- ja salassapitorakenteen avulla asiakirjajulkisuuden tehokas ja tosiasiallinen toteutuminen.

Tiedonhallintalain 13.4 § sisältää tietoturvallisuustoimenpiteiden varmistamisvelvollisuuden tietojärjestelmähankintoja toteutettaessa. Varmistamisvelvollisuus tarkoittaa tietoturvallisuustestausta ja/tai tietoturvallisuusarvioinnin tekemistä hankintavaiheessa. Tämä puolestaan edellyttää sitä, että hankintayksikkö on määritellyt laissa säädetyt tietoturvavaatimukset tarjouspyyntöasiakirjoihin riittävän yksiselitteisesti.

Digitaalisten palvelujen tarjoamisesta annetun lain 4.1 §:ssä on säädetty yleisesti digitaalisten palvelujen suunnitteluvelvollisuuden täyttämisestä. Säännöksen mukaan viranomaisen on suunniteltava ja ylläpidettävä digitaaliset palvelunsa siten, että niiden tietoturvallisuus, tietosuoja, löydettävyys ja helppokäyttöisyys on varmistettu. Lisäksi viranomaisen on varmistettava digitaalisten palvelujensa yhteensopivuus yleisesti käytettyjen ohjelmistojen ja tietoliikenneyhteyksien kanssa. Varmistamisvelvollisuus tarkoittaa paitsi näiden eri vaatimusten huomioimista digitaalisen palvelun suunnittelussa, mutta myös varmistamista tarvittavilla testauksilla ja muilla laadunvarmistustoimenpiteillä näiden vaatimusten toteuttaminen. Säännös ei sisällä konkreettisia vaatimuksia mm. tietoturvallisuuden tai tietosuojan osalta, vaan nämä vaatimukset perustuvat muuhun sääntelyyn.

5.4 Muutosvaikutusten arviointivelvollisuus

Tietojärjestelmien kehittämisprosessiin vaikuttaa tiedonhallintalain 5.3 §:ssä tiedonhallintayksikölle säädetty velvollisuus tehdä tiedonhallinnan muutosvaikutusarviointi otettaessa tietojärjestelmä käyttöön. Muutosvaikutusarviointi on käytännössä tehtävä jo tietojärjestelmän hankintaa suunniteltaessa. Muutosvaikutusarvioinnin tarkoitukseksi ei ole säännöksen perusteluissa nostettu hyvän hallinnon vaatimusten toteuttamista, vaan säännöksen lähtökohtina ovat olleet tietojärjestelmien hanketoiminnan taloudellisten ja toiminnallisten riskien ennakointi ja suunnitelmien saattaminen realistiselle pohjalle sekä yhteentoimivuuden ja tietoturvallisuuden toteuttaminen.[27]

Yleisen tietosuoja-asetuksen 35 artiklassa on puolestaan säädetty tietosuojan vaikutustenarvioinnista muun muassa uutta teknologiaa käyttöönotettaessa. Tietosuoja-asetuksen vaikutustenarviointia koskevaa velvollisuutta on tarkennettu tietosuojavaltuutetun päätöksessä, jossa on määritelty, missä tilanteissa vaikutustenarviointi on pakollista. Tällaisia tilanteita ovat muun muassa automaattisten päätöksenteon käyttöönotto, rekisteröityjen järjestelmällinen valvonta, erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely ja laajamittainen tietojenkäsittely.

Tietosuojan vaikutustenarviointia koskeva sääntely jää yleiselle tasolle, mutta vaikutustenarviointiin kuuluu riskien tunnistaminen rekisteröidyn oikeuksille ja vapauksille sekä rekisterinpitäjälle velvollisuus ryhtyä toteuttamaan asianmukaisia teknisiä ja organisatorisia toimia henkilötietojen suojaamiseksi. Rekisteröidyn oikeuksien ja vapauksien sisältöä ei ole yksiselitteisesti määritelty tietosuoja-asetuksessa, mutta asetuksen tarkoituksena on eri perusoikeuksien turvaaminen henkilötietojen käsittelyssä. Tässä suhteessa myös oikeusturvan varmistaminen henkilötietojen käsittelyn eri vaiheissa kuuluu teknisiin ja organisatorisiin toimiin, joiden suunnittelu perustuu riskiperusteiseen arviointiin, josta on säädetty tietosuoja-asetuksen 35 artiklan lisäksi 5 ja 25 artiklassa. Tietosuoja-asetuksessa on säädetty rekisterinpitäjän vastuulle suunnitella ennakkoon henkilötietojen käsittelytoimet siten, että rekisteröidyn oikeudet ja vapaudet toteutuvat henkilötietoja käsiteltäessä. Tietosuoja-asetuksen 25 artiklassa on säädetty käytännössä sisäänrakennetun ja oletusarvoisen tietosuojan suunnitteluvelvollisuudesta. Tietosuoja-asetuksen resitaalin 78 mukaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet olisi huomioitava julkisten tarjouskilpailujen yhteydessä. Sisäänrakennetun ja oletusarvoisen tietosuojan osoittamiseen voidaan käyttää tietosuoja-asetuksen 42 artiklassa tarkoitettuja sertifiointimekanismeja.

27 HE 284/2028 vp, s. 78.

5.5 Tietojärjestelmien käyttöönotto

Tietojärjestelmien käyttöönottovaiheesta ei ole varsinaisesti säädetty yleislainsäädännön tasolla mitään. Sen sijaan erityislainsäädännössä, esimerkiksi sosiaali- ja terveydenhuollon asiakastietolaissa, on säädetty käyttöönoton edellytykseksi vaatimustenmukaisuuden arviointi joko arviointilaitoksen tekemänä tai eräissä tapauksissa itsearviointina.

Tiedonhallintalain 5.3 §:ssä on säädetty tiedonhallinnan muutosvaikutusarvioinnin tekemisestä suunniteltaessa tietojärjestelmien käyttöönottoa, jolla on vaikutusta tiedonhallintayksikön tiedonhallintamallin sisältöön. Laissa tarkoitettu käyttöönotto ei varsinaisesti ohjaa käyttöönottovaihetta, vaan tietojärjestelmän käyttöönottoon tähtäävää suunnittelua, joka alkaa jo tietojärjestelmien vaatimusmäärittelystä ja hankinnan valmistelusta.

Laillisuusvalvonnassa on noussut esiin varsin runsaasti ongelmia tietojärjestelmien käyttöönottovaiheissa. Tietojärjestelmien käyttöönottoon keskeneräisenä liittyy yksilön perusoikeuksiin liittyviä riskejä. Eräissä tapauksissa asiankäsittelyajat ovat voineet pitkittyä[28], viranomaisen velvollisuuksien toteuttaminen pitkittyä[29] tai palvelujen saatavuus on voinut estyä.[30] Käyttöönottoon liittyneiden ongelmien laillisuusvalvonnallisten arviointien yhteydessä on toistuvasti ja vakiintuneesti todettu, että tietojärjestelmiin liittyvillä syillä ei voida perustella poikkeamista hyvän hallinnon ja oikeusturvan viranomaismenettelyille asettamista vaatimuksista.[31] Edelleen laillisuusvalvonnassa on todettu, että aikataulusyillä ei voida perustella järjestelmän käyttöönottoa, jos siihen liittyy yksilön perusoikeuksien kannalta merkittäviä puutteita. Laillisuusvalvonnan näkökulmasta asiassa on olennaista se, että tämänkaltaisia tietojärjestelmiä ei oteta käyttöön perusoikeuksien näkökulmasta keskeneräisinä.[32] Käyttöönottovaiheeseen liittyy viranomaistoiminnassa asianmukaisuusvaatimuksia sen varmistamiseksi, että viranomainen pystyy käyttöönoton yhteydessä selviytymään lakisääteisistä velvollisuuksistaan.

28 AOK 226/1/96, 14.5.1997, EOA 2071/4/05, 19.10.2005, AOA 1137/4/04, 31.5.2006 AOA 645/4/04, 31.5.2006, AOA 33/2/06 ja 34/2/2006, 31.5.2006.

29 OKA 949/1/90, 03.04.1992 ja OKV/3/50/2018, OKV/1453/1/2018, 301.2019.

30 EOA 206/4/11, 31.5.2012.

31 EOA 537/4/10,12.8.2010; EOA 2523/4/08, 8.11.2010; AOA 3951/4/09/21.6.2010; AOA 3718/4/07, 17.12.2008; AOA 750/2019, 19.8.2019.

32 EOA 2523/4/08, 8.11.2010.

5.6 Johtopäätöksiä

Lainsäädännössä ei ole säädetty tietojärjestelmien kehittämismenetelmistä. Kehittämismenetelmiä on useita erilaisia eikä ole tarkoituksenmukaista säännellä kehittämisestä niin, että vain tietyt menetelmät ja lähestymistavat sallittaisiin. Olennaista on se, että kehittämismenetelmä tuottaa riittävän laadukkaan lopputuloksen, ja että virkamiehet ovat kehittämisessä mukana niin, että automaattisessa hallinnossa lainmukaisuus ja asianmukaisuus toteutuvat.

Viranomainen voi ottaa tietojärjestelmän käyttöönsä joko tuottamalla sen alusta asti itse, tai ulkoistamalla toimittajalle yhden tai useamman vaiheen. Viranomainen saattaa kuitenkin tapauksesta ja tietojärjestelmän luonteesta riippuen osallistua enemmän tai vähemmän myös ulkoistettuihin vaiheisiin. Tärkeää on, että viranomaisella ja toimittajalla on selkeä työnjako siitä, kuka mistäkin vaiheesta vastaa.

Työryhmä katsoo, että lainsäädännössä ei ole säädetty yhtenäisesti tai kattavasti siitä, minkälaisia kontrolleja ja dokumentaatiota pitäisi vaatia hallinnon tietojärjestelmien kehittämisestä, joilla voidaan todentaa, että tietojärjestelmän toiminnallisuudet täyttävät asianmukaiselle asiankäsittelylle ja hyvälle hallinnolle asetettavat vaatimukset. Koska sääntely jää yleiselle tasolle ja osin sääntelemättömäksi, ei myöskään voida osoittaa selvästi, kenellä on virkavastuu miltäkin osin tietojärjestelmän kehittämisestä ja sen toiminnallisuuksien varmistamisesta. Työryhmän näkemyksen mukaan kehitettävän sääntelyn pitäisi sisältää säännökset tietojärjestelmien kehittämiseen liittyvistä riittävistä kontrolleista ja dokumentoinnista.

Kehittämisessä olisi myös varmistuttava siitä, että tietojärjestelmien käytöstä aiheutuvat virheet ovat mahdollisimman tehokkaasti jäljitettävissä ja korjattavissa, esimerkiksi niin että automaattisesti tehdyt virheelliset merkinnät on mahdollista löytää ja korjata automaattisin toimin sen sijaan, että korjaukset joudutaan tekemään käsin. Tällaisten automatisoitujen korjaamistoimenpiteiden mahdollistaminen edellyttäisi kuitenkin hallintolain hallintopäätössä olevien asia- ja kirjoitusvirheen korjaamista koskevien säännösten arviointia sekä samanaikaisesti sen selvittämistä, miltä osin korjaamista voidaan tehdä jo voimassa olevan tietosuojasääntelyn perusteella.

Työryhmä pitää tarpeellisena, että tietojärjestelmien käyttöönottovaiheeseen liittyvää sääntelyä kehitetään siten, että tietojärjestelmän kelvollisuus käyttöönotettavaksi tarkoitukseensa on varmistettu riittävän huolellisella testauksella, tietojärjestelmän käytön koulutuksella ja käyttöönoton suunnittelulla. Myös teknisiin ongelmiin varautumiseen käyttöönottovaiheessa on syytä kiinnittää huomiota sääntelyä kehitettäessä.

6 Tietojärjestelmille laissa säädetyt toiminnalliset ja tekniset vaatimukset

6.1 Yleistä

Tietojärjestelmien toiminnallisia ja teknisiä vaatimuksia määritellään tyypillisesti viranomaisten omissa ohjeissa, hankinta-asiakirjoissa sekä tietylle alalle kohdennetuissa standardeissa. Lainsäädännössä on voitu säätää yleisellä, abstraktilla tasolla toiminnallisista ja teknisistä vaatimuksista. Sääntelyä ei voida kiinnittää tiettyyn tekniseen ratkaisuun, koska silloin sääntely voi rajata markkinoita, estää tietojärjestelmien innovatiivisen ja joustavan kehittämisen, sekä vanhentua nopeasti teknisen ympäristön kehittymisen myötä.

Sääntelykohteena tietojärjestelmissä käytettävä tieto- ja viestintäteknologia on nopeasti muuttuvaa, joten sääntelynkin on oltava joustavaa, teknologianeutraalia ja tietyltä osin abstraktilla tasolla. Tietojärjestelmien vaatimuksien yhdenmukaistamisessa ovat tärkeitä laissa säädetyn lisäksi lakia alemman tasoinen sääntely sekä alan soft law -tyyppinen itse- tai myötäsääntely.[33] Tieto- ja viestintäteknologiaan kohdistuvaa, teknisluonteista ja laissa säädettyä tarkentavaa sitovaa sääntelyä ovat antaneet määräyksenantovaltuuksien puitteissa esimerkiksi Terveyden ja hyvinvoinnin laitos[34] sekä Liikenne- ja viestintävirasto[35]. Myötäsääntelyyn viittaavia suosituksia on puolestaan antanut julkisen hallinnon tiedonhallintalautakunta, jonka tehtävänä on tiedonhallintalain 10.1 §:n 2 kohdan perusteella tiedonhallintalaissa säädettyjen vaatimusten ja menettelytapojen edistäminen. Itsesääntelyä puolestaan voidaan katsoa tapahtuvan IT-alan standardien laatimisen ja antamisen kautta.

33 Voutilainen, Tomi (2009): ICT-oikeus sähköisessä hallinnossa – ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely, s. 115–116 ja 123–124.

34 Määräyksenantovaltuudesta säädetään sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 19 a §:n 3 momentissa.

35 Määräyksenantovaltuudesta säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 42 §:ssä sekä sähköisen viestinnän palveluista annetun laissa (917/2014), mm. sen 244 §:ssä.

6.2 Lähtökohtana asianmukaisuuden varmistaminen tietojärjestelmissä

Perustuslain 21.1 §:n mukaan jokaisella on oikeus saada asiansa käsitellyksi *asianmukaisesti* ja *ilman aiheetonta viivytystä* lain mukaan toimivaltaisessa viranomaisessa. Jokaisen oikeus saada asiansa käsitellyksi asianmukaisesti viranomaisessa on yksi hyvän hallinnon keskeisimmistä vaatimuksista.

Perustuslaissa säädetty asianmukaisuus tarkoittaa hallintolaissa (434/2003) viranomaisen tuottaman palvelun ja asiankäsittelyssä noudatettavan menettelyn asianmukaisuutta. Hallintolain 7.1 §:n mukaan asiointi ja asian käsittely viranomaisessa on pyrittävä järjestämään siten, että hallinnossa asioiva saa asianmukaisesti hallinnon palveluita ja viranomainen voi suorittaa tehtävänsä tuloksellisesti. Säännöksen perustelut keskittyvät asianmukaisuuden arvioinnissa hallinnon palvelujen asianmukaisuuden järjestämiseen ja asiakasnäkökulman korostamiseen palveluja tuotettaessa. Sen sijaan perusteluissa ei avata asian käsittelyn ja tuloksellisuuden vaatimuksia tarkemmin.[36] Säännös ja sen perustelut viittaavat siihen, että asianmukaisuusvaatimus on huomioitava viranomaisten toimintaprosessien[37] näkökulmasta kokonaisuutena riippumatta siitä, liittyykö toimintaprosessi asianosaisaloitteisen tai viranomaisaloitteisen asian käsittelyyn taikka palvelun tuottamiseen ilman erillistä asian käsittelyä, eli tosiasiallisena hallintotoimintana.

Asianmukaisuuteen liittyy myös hallintolain 9 §:ssä säädetty hyvän kielenkäytön vaatimus siitä, että viranomaisen on käytettävä asiallista, selkeää ja ymmärrettävää kieltä. Viranomaisen on myös käytettävä harkintavaltaansa asianmukaisesti. Tästä harkintavallan käytössä sekä muuten viranomaisten toiminnassa on huomioitava yleiset hallinnon oikeusperiaatteet, joista säädetään hallintolain 6 §:ssä. Sinällään hallintolaki ohjaa menettelysäännöksillään käsittelyn asianmukaisuuteen kokonaisuudessaan samoin kuin hallinnon muut yleislait, kuten laki sähköisestä asioinnista viranomaistoiminnassa (13/2003, asiointilaki) ja digipalvelulaki.

Asianmukaisuutta virkatehtävien hoidossa on myös korostettu valtion virkamieslain (750/1994) 14 §:ssä ja kunnallisesta viranhaltijasta annetun lain (304/2003) 17.1 §:ssä. Virkamieslainsäädännön asianmukaisuusvaatimus kohdistuu kaikenlaisiin virkaan liittyviin tehtäviin – ei pelkästään asiankäsittelyyn ja tosiasialliseen hallintotoimintaan. Siten virkamieslainsäädännön näkökulmasta katsottuna tietojärjestelmien kehittämisessä virkamiesten ja viranhaltijoiden on hoidettava siihen liittyvät tehtävät asianmukaisesti.

---

36 HE 72/2002 vp, s. 56–57.

37 Toimintaprosessilla tarkoitetaan tiedonhallintalain 2 §:n 10 kohdan mukaan viranomaisen asiankäsittely- tai palveluprosessia.

6.2.1 Asianmukaisuus digitaalisissa palveluissa ja palveluautomaatiossa

Hallintolain 7 §:ssä säädetty palveluperiaate sisältää palvelun asianmukaisuuden vaatimuksen. Palveluperiaatetta koskevassa säännöksessä ei varsinaisesti ole viranomaisten palvelujen tuottamista koskevia yksilöityjä vaatimuksia, vaan säännös saa – ehkä ongelmallisesti – sisältönsä perustelujen kautta. Hallituksen esityksen hallintolaiksi (HE 72/2002 vp) 7 §:n perusteluissa palveluperiaatteen sisällössä korostetaan asiakasnäkökulmaa. Pykälässä hallinnossa asioivalla tarkoitetaan viranomaispalvelujen käyttäjiä. Asioinnilla puolestaan tarkoitetaan kaikkea julkisen tehtävän hoitamiseen liittyvien palvelujen käyttöä. Palvelun ja viranomaisen toiminnan tuloksellisuuden näkökulmasta asioinnin tulisi olla sekä hallinnossa asioivan että viranomaisen kannalta mahdollisimman nopeaa, joustavaa ja yksinkertaista, sekä kustannustehokasta. Palvelun asianmukaisuudelle ei ole hallintolaissa säädetty laatuvaatimuksia, mutta säännöksen perustelut antavat näille laadullisille vaatimuksille suuntaa-antavaa pohjaa. Toisaalta mitään yksiselitteistä velvollisuutta asianmukaisuuden minivaatimuksistakaan ei ole, joten viranomaisella ei ole ehdotonta toimintavelvollisuutta asiointipalvelujen asianmukaiseksi järjestämiseksi, vaan se jää erityissääntelyn varaan. Palvelun asianmukaisuuteen liittyviä kriteerejä palveluperiaatesäännöksen perusteluissa ovat:[38]

- Asiointi olisi pyrittävä järjestämään siten, että hallinnossa asioiva voi helposti muodostaa kokonaiskäsityksen asiansa hoitamiseen tarvittavan palvelun sisällöstä ja siihen liittyvistä toimista.
- Julkisia palveluja järjestettäessä tulisi erityisesti kiinnittää huomiota palvelujen riittävyyteen ja saatavuuteen sekä hallinnossa asioivan valinnanvapauteen.
- Palvelujen saatavuutta ei tulisi rajoittaa ilman asiallisesti hyväksyttäviä perusteita.
- Hallinnossa asioivan itsemääräämisoikeutta ja toimintaedellytyksiä viranomaisasioinnissa olisi mahdollisuuksien mukaan pyrittävä edistämään. Tähän liittyvät yhteistyö ja vuorovaikutus palvelujen käyttäjien kanssa, kuten palautteen kerääminen palveluista ja asiakaslähtöisten arviointimenetelmien käyttö.
- Asioinnin järjestämisen keinoja ja laajuutta tulisi pyrkiä arvioimaan erityisesti palvelujen käyttäjinä olevien henkilöiden ja yhteisöjen tarpeiden kannalta.
- Kaikille palveluja tarvitseville olisi pyrittävä turvaamaan yhtäläinen mahdollisuus asiansa hoitamiseen palvelun laadusta riippumatta.

38 HE 72/2002 vp, s. 56–57.

- Asiointimahdollisuuksien olisi myös vastattava mahdollisimman hyvin yhteiskunnallisten erityisryhmien tarpeisiin. Näitä erityisryhmiä ovat esimerkiksi vanhukset, sairaat ja vammaiset.
- Asioinnin järjestämisessä olisi kiinnitettävä huomiota myös kohteena olevan palvelun erityispiirteisiin. Julkisen sektorin on huolehdittava siitä, että hallinnossa asioivien kannalta tärkeät palvelut ovat saatavilla kaikkialla maassa ja välttämättömät tehtävät tulevat tehokkaasti hoidetuiksi.

Näille palveluperiaatteen sisällöllisille tavoitteille ja luonnehdinnoille on annettu painoa erityisesti laillisuusvalvonnan ratkaisukäytännössä, kun valvonnan kohteena on ollut viranomaisen palvelujen järjestäminen ja sen asianmukaisuus.[39] Palvelun asianmukaisuutta on myös arvioitu suhteessa palveluperiaatteen taustalla oleviin tavoitteisiin, kun laillisuusvalvonnassa on arvioitu erilaisten palvelumuotojen saatavuutta sekä sähköisen asioinnin mahdollistavien digitaalisten palvelujen käytön korostamista viranomaisten viestinnässä.[40]

Hallinnon palveluperiaatetta täsmennetään hallintolain 8 §:ssä viranomaisen neuvontavelvollisuudella, jossa säädetään neuvonnan vähimmäisvaatimuksista. Viranomaisen on toimivaltansa rajoissa annettava asiakkailleen tarpeen mukaan hallintoasian hoitamiseen liittyvää neuvontaa. Lisäksi viranomaisen on vastattava asiointia koskeviin kysymyksiin ja tiedusteluihin. Neuvonnan on oltava maksutonta. Lisäksi viranomaisella on velvollisuus opastaa asiakas toimivaltaiseen viranomaiseen, jos asia ei kuulu viranomaisen toimivaltaan. Viranomaisen neuvonnan asianmukaisuuteen palveluperiaatteen mukaisesti kuuluu, että se on oikeansisältöistä ja selkeää.[41] Tällä on vaikutuksensa myös siihen, millä tavalla ja minkälaista tietosisältöä neuvontatarkoituksessa hallinnon asiakkaille annetaan erilaisissa digitaalisissa palveluissa.[42]

Asiointilaissa on menettelyllistä sääntelyä siitä, kun viranomainen vastaanottaa sähköisiä asiakirjoja, esimerkiksi vastaanottokuittauksesta ja sähköisten asiakirjojen vastaanottotoimista. Asiointilaki sisältää myös menettelyllisiä vaatimuksia tietojärjestelmille, kun tiedoksianto tehdään sähköisesti. Asiointilaki sallii lisäksi päätösasiakirjan allekirjoittamisen sähköisesti. Säännös on mahdollistava, eikä velvoita päätösasiakirjojen sähköiseen allekirjoittamiseen.

---

39 Ks. esimerkiksi OKV/135/10/2020, 19.11.2020, OKV/ 138/10/2020, 29.10.2020, OKV/89/10/2020, 3.9.2020, AOA 6525/2018, 4.11.2019, EOAK/502/2019, 31.7.2020 ja OKV/1124/1/2012, 9.6.2014.

40 AOA 39/4/11, 13.9.2012, AOA 3661/4/08 ja AOA 3999/4/08, 9.11.2010, AOA 4192/4/10, 21.3.2012 sekä AOA 4653/4/14, 31.12.2015

41 OKV/1011/10/2020, 21.4.2021

42 Ks. esimerkiksi OKV/2092/1/2017, 13.3.2018, EOA 2149/4/13, 4.4.2014 ja AOA 1468/4/11, 17.2.2012.

Digipalvelulaissa säädetään digitaalisten palvelujen asianmukaisuutta määritteleviä vaatimuksia. Digipalvelulain 2 luvussa säädetään viranomaisille digitaalisten palvelujen järjestämiseen liittyviä yleisiä vaatimuksia palvelujen suunnitteluun ja ylläpitoon, digitaalisten palvelujen tarjoamiseen sekä palvelujen käyttäjien tunnistamiseen. Sääntely sisältää digitaalisten palvelujen toiminnallisuuksiin lähinnä sähköisen tunnistamisen osalta yksilöityjä vaatimuksia. Lisäksi sääntely sisältää digitaalisten palvelujen sisältöihin ja tukeen liittyviä vaatimuksia. Laissa säädetään myös palvelun sisällön saavutettavuusvaatimuksista, jotka ovat osa perusoikeutena turvatun yhdenvertaisuuden toteuttamista koskevia toimia. Saavutettavuusvaatimuksilla pyritään edistämään jokaisen mahdollisuuksia käyttää digitaalisia palvelujen siten, että palvelujen sisältö on esitetty muodossa, joka on saatavissa selville erilaisilla päätelaitteilla erilaisille käyttäjäryhmille.

Viranomaisten digitaalisiin palveluihin on viime vuosien aikana luotu erilaisia palveluun ohjaamiseen ja asiakkaiden neuvontaan sekä opastamiseen liittyviä toiminnallisuuksia, joissa asiakkaan antamien vastausten avulla edetään neuvonnassa tai palveluohjauksessa automaattisesti. Lisäksi viranomaisten digitaalisissa palveluissa on otettu käyttöön chatbot-sovelluksia, jotka antavat automaattisesti vastauksia asiakkaan luonnollisella kielellä esittämiin kysymyksiin. Tällaisista hallinnon asiakkaan suuntaan täysin automatisoiduilta näyttävistä ja tekoälyä muistuttavista toiminnallisuuksista tai niiden käyttöönoton edellytyksistä ei ole erityistä sääntelyä. Viranomaisen neuvontavelvollisuuden toteuttamiseen liittyy niin asianmukaisuusvaatimus, hyvän kielenkäytön vaatimus, julkisen hallintotehtävän kuin virkavastuukin toteuttaminen tietyn tyyppisissä neuvontatilanteissa. Neuvontaa ei ole pidetty yleisesti julkisen vallan käyttämisenä[43], mutta neuvonnan sisältö ja asiayhteys voivat vaikuttaa tähän arvioon.[44] Hallintolaissa säädetyn neuvontavelvollisuuden toteuttamista on pidetty perustuslain 124 §:ssä tarkoitettuna julkisena hallintotehtävänä.[45]

Voimassa oleva hallinto- ja kielilainsäädäntö muodostavat tällaiselle automaation hyödyntämiselle yleiset puitteet, mutta esimerkiksi vastuun määrittämiseen ja neuvonta-automaation sisällön tuottamiseen ei ole selkeitä säännöksiä, esimerkiksi suhteessa perustuslain 124 §:ään.

43 PeVL 11/2006 vp, 2, PeVL 20/2006 vp, KKO 2009:24 ja AOA 1806/2/05, 3.11.2005.

44 KKO 1989:50.

45 PeVL 11/2006 vp, PeVL 20/2006 vp.

6.2.2 Asianmukaisuus asiankäsittelyssä

Asiankäsittelyn asianmukaisuudesta säädetään hallintolain 31.1 §:ssä, jonka mukaan viranomaisen on huolehdittava asian riittävästä ja asianmukaisesta *selvittämisestä* hankkimalla asian ratkaisemiseksi tarpeelliset tiedot sekä selvitykset. Säännöksen perustelujen mukaan asian riittävällä selvittämisellä tarkoitetaan sitä, että viranomainen hankkii sellaiset tiedot ja selvitykset, joilla se arvioi olevan merkitystä asian ratkaisemiselle. Selvittämisen asianmukaisuus puolestaan korostaa viranomaiselle kuuluvaa menettelyjohtovaltaa ja huolellisuutta selvitysten hankkimisessa.[46] Asianmukaisuus asian selvittämisessä tarkoittaa menettelyvaatimusten ja konkreettiseen asiaan liittyvien erityisvaatimusten noudattamista.[47] Selvittäminen on tehtävä perusteellisesti erityisesti etuja ja oikeuksia koskevan käsittelyn yhteydessä.[48] Viranomaisen ratkaisunsa perusteeksi hankkiman tietopohjan on oltava luotettavaa ja objektiivista.[49] Myös automatisoituihin toiminnallisuuksiin on sisällytettävä kontrollit, joilla voidaan varmistaa tietojärjestelmän tekemien oikeudellisesti merkittävien toimintojen perusteiden ja käytettävien tietojen oikeellisuus.[50] Tietojärjestelmissä olevien kontrollien puute ei puolestaan poista virkamiehen vastuuta asianmukaisesta ja huolellisesta asiankäsittelystä.[51]

Asianmukaisuus asian selvittämisessä tarkoittaa viranomaisen valtaa virallisperiaatteen mukaisesti johtaa selvittämistä koskevaa menettelyä sekä hankkia selvityksiä ja muita tietoja asianosaiselta, muilta viranomaisilta sekä muilta tahoilta. Asian selvittämisen asianmukaisuuteen liittyy viranomaisen velvollisuus tehdä se huolellisesti muun muassa tietoja ja selvityksiä hankittaessa.[52] Hallinnon asianmukaisuus edellyttää myös asioiden ja asiakkaan kanssa käytyjen keskustelujen huolellista kirjaamista tietojärjestelmään.[53] Asianmukaisuuteen sisältyy myös vaatimus siitä, että asiankäsittely dokumentoidaan sekä tarvittavilta osin esitetään hallintopäätöksessä. Päätöksestä on ilmettävä, mitkä seikat ovat

46 HE 72/2002 vp, s. 86.

47 Mäenpää, Olli (2016): Hallintolaki ja hyvän hallinnon takeet (5. uudistettu painos), s. 232.

48 Ks. esimerkiksi OKV/663/1/2019, 31.3.2020 ja OKV/357/1/2019, 12.3.2020

49 Mäenpää (2016), s. 232.

50 Ks. tästä esimerkiksi OKV/1166/1/2016, 12.10.2017 ja EOAK/5372/2019, 22.6.2020. Käytettävien tietojen laatua käsitellään tarkemmin arviomuistiossa jäljempänä.

51 OKV/20/31/2017, 1.2.2018.

52 Ks. esimerkiksi laillisuusvalvonnan kannanottoja huolellisuusvelvollisuudesta osana asianmukaisuusvaatimusta OKV/430/10/2020, 10.9.2020 ja OKV/663/1/2019, 31.3.2020 sekä oikeuskirjallisuudesta esimerkiksi Kulla, Heikki (2018): Hallintomenettelyn perusteet, s. 232.

53 OKV/610/1/2019, 25.3.2020.

johtaneet asianosaista koskevan ratkaisun tekemiseen. Perustelujen täsmällisyydellä ja selkeydellä on merkitystä viranomaistoiminnan yleisen luottamuksen kannalta.[54] Perustelujen puutteita ei voida perustella tietojärjestelmien teknisillä ominaisuuksilla.[55]

Asianosaisella on oikeus saada häntä koskevan ratkaisun perusteet, jotta hän voi arvioida käsittelyn, kuten automatisoitujen käsittelyvaiheiden, asianmukaisuutta sekä omaa oikeusturvaansa. Myös tieto siitä, että asianosaisen asia on ratkaistu täysin automaattisesti, tulisi olla asianosaisen tiedossa selkeästi yksilöitynä viranomaisen päätöksessä.[56] Laillisuusvalvonnassa on pidetty tarpeellisena, että asianosaiselle kerrotaan tietojärjestelmien automaation hyödyntämisestä asiankäsittelyssä.[57]

Asiankäsittelyn asianmukaisuutta dokumentoidaan myös asiarekisteriin, jonka tietosisällöstä säädetään tiedonhallintalain 26 §:ssä. Tiedonhallintalain 25 §:ssä säädetään asiakirjojen rekisteröintivelvollisuudesta asiarekisteriin. Asiarekisteristä ilmenevät käsittelyssä olevat ja käsittelyssä olleet asiat sekä niiden vaiheet ja niihin kuuluvat asiakirjat. Asianmukaisuuden jälkikäteistä kontrollia ja todennettavuutta sääntelee myös tiedonhallintalain 17 §:ssä säädetty velvollisuus viranomaiselle kerätä tietojärjestelmien käytöstä lokitietoja, joiden tarkoituksena on muun muassa tietojen käytön ja luovutuksen seuranta. Säännöksen perustelujen mukaan käyttölokien keräämisen perusteena toimii muun muassa virkavastuun todentaminen.[58] Laillisuusvalvonnassa on todettu, että kaikkien asiaan vaikuttavien seikkojen ja asian menettelyvaiheiden tulee selkeästi ilmetä asiakirjoista ja tietojärjestelmistä.[59] Tätä dokumentointivelvollisuutta voidaan pitää yhtenä konkreettisena asianmukaiseen asiankäsittelyyn liittyvänä vaatimuksena.

Asianmukaisuusvaatimuksen tarkkaa sisältöä ja vaatimuksia ei siis ole säädetty hallintolaissa, vaan se jää osittain paitsi erityislainsäädännön, myös oikeuskäytännön ja laillisuusvalvontakäytännön varaan. Toisaalta tiedon hankkiminen asian selvittämistä varten voi edellyttää erillisiä tiedonsaantioikeuksia salassapitosäännösten estämättä, jos selvittämisessä on tarvetta saada toiselta viranomaiselta salassa pidettäviä tietoja. Tiedonsaannista yksityiseltä, joka ei ole asianosainen, on säädettävä myös erikseen.

54 EOAK/1187/2020, 21.4.2021.

55 KHO 19.11.2014 t. 3613.

56 Ks. tästä myös AOA EOAK/3379/2018, 20.11.2019, s. 36.

57 AOA EOAK/2216/2018, 20.11.2019

58 HE 284/2018 vp, s. 96.

59 EOA 86/4/06, 26.6.2008.

Asianmukaisuuden näkökulmasta automatisointia voidaan perustella käsittelyn tehostumisella ja nopeutumisella, mikä edistää asiankäsittelyn viivytyksettömyyttä. Vaikka menettely muuten täyttäisikin vaatimuksen asiankäsittelyn viivytyksettömyydestä, perustuslain 21.1 §:n ja hallintolain 31.1 §:n vaatimus asianmukaisuudesta ei välttämättä täyty summaarisessa, riittämättömään tai varmistamattomaan tietopohjaan perustuvassa käsittelyssä, tai epäasiallisia keinoja käyttäen hankitun tiedon perusteella.[60] Hyvään hallintoon sinänsä kuuluvien asiankäsittelyn nopeuden ja tehokkuuden perusteella ei siis voida poiketa asiankäsittelyn asianmukaisuudelle säädetystä vaatimuksesta.[61]

6.2.3 Asianmukaisuus hallinnon tietojärjestelmien käytössä

Käytettäessä digitaalisia palveluja ja muita tietojärjestelmiä asioinnissa sekä asiankäsittelyssä siten, että käsittely on joko kokonaan tai osittain automaattista, joudutaan hallinnon palvelujen ja asiankäsittelyn asianmukaisuus varmistamaan ennalta, kun kehitettävälle tietojärjestelmälle määritellään vaatimuksia. Vaatimuksia määriteltäessä on otettava huomioon yleis- ja erityissääntely, käsittelykohteeseen vaikuttavat säännökset, sekä menettelysääntely. Kuitenkin tällainen sääntely jää monissa tilanteissa yleiselle tasolle, jolloin säännösten soveltamiselle jää kussakin soveltamiskontekstissa varsin laaja tulkintamahdollisuus.

Hallintolaki ei sisällä varsinaisesti ja kohdennetusti tietojärjestelmien toiminnallisuuksiin liittyvää sääntelyä. Hallintolaki perustuu virkamieshallintoon, jossa virkamies selvittää ja ratkaisee asian.[62] Julkisen hallinnon tietojärjestelmien kehittämiseen ei ole kohdistettu varsinaisesti yleisiä säännöksiä, jotka velvoittaisivat todentamaan tietojärjestelmän toiminnallisuuksien lainmukaisuuden ja asianmukaisuuden. Yleislainsäädännössä ei ole myöskään esitetty kehittämisen vastuisiin ja dokumentointiin liittyviä vaatimuksia. Tällaisen sääntelyn voidaan kuitenkin katsoa olevan tarpeen viranomaisen asianmukaisen palvelun ja asiankäsittelyn varmistamiseksi sekä hallinnon toimintaan kohdistuvan luottamuksen vahvistamiseksi.[63] Asianmukaisuuden vaatimus koostuu erilaisista laatuvaatimuksista sen mukaan, missä yhteydessä asianmukaisuutta arvioidaan viranomaisen toiminnassa.[64]

60 Miettinen, Tarmo – Kuosmanen, Elisa (2006): Hallintolaki oikeus- ja laillisuusvalvontakäytännössä. Oikeusministeriön julkaisuja 2006:10, s. 70.

61 Väätänen, Ulla (2011): Oikein ja joutuisasti, s. 87.

62 AOA EOAK/3379/2018, 20.11.2019, s. 33

63 Ks. luottamuksen merkityksestä hallinnossa Pöysti 2020, s. 346–347.

64 Väätänen (2011), s. 87.

Jotta asianmukaisuus voisi olla velvoittavaa, esimerkiksi virkavastuun näkökulmasta, tulisi se määritellä esimerkiksi tietojärjestelmien kehittämisen yhteydessä tarkemmin säätämällä laissa kehittämiseen liittyvistä asianmukaisuusvaatimuksista (laatuvaatimuksista).

Hallintolaissa tai muuallakaan yleislainsäädännössä ei ole yleisiä säännöksiä siitä, miten hyvä hallinto ja oikeusturva toteutuvat käytettäessä tietojärjestelmiä hallintoasioiden käsittelyssä, riippumatta siitä, millainen automaatioaste toimintaprosessilla on. Tiedonhallintalaissa on jossakin määrin tietojärjestelmiin kohdistuvia säännöksiä, jotka liittyvät myös hyvän hallinnon toteuttamiseen.

Perustuslain 2.3 §:n mukaan julkisen vallan käytön on perustuttava lakiin. Kaikessa julkisessa toiminnassa on tarkoin noudatettava lakia. Perustuslain 21.2 §:n mukaan hyvän hallinnon takeet turvataan tarkemmin lailla. Nämä julkisen vallan käytölle ja hallinnon toiminnalle säädetyt perusvaatimukset eivät täyty pelkästään yleisluonteista ja kaikkeen asiankäsittelyyn sovellettavan ja leimallisesti henkilötyöhön viittaavan sääntelyn perusteella. Lainsäädännössä ei ole säädetty selkeästi hyvän hallinnon takeiden toteuttamisesta, kun tietojärjestelmiä käytetään hallinnon toiminnassa. Lain tarkka noudattaminen julkisen hallinnon tietojärjestelmiä kehitettäessä ja käytettäessä ei toteudu yleisluonteisella sääntelyllä, joka ei sisällä selkeitä toimintavelvoitteita.

Onkin ilmeistä, että julkisen hallinnon hallintoasioiden käsittelyyn ja muuhun hallintotoimintaan liittyvien tietojärjestelmien kehittämistä ja käyttöä koskevaa sääntelyä on täsmennettävä sekä hyvän hallinnon periaatteiden että hallinnon lainalaisuus- ja lakisidonnaisuusvaatimusten vuoksi.

6.3 Tekoälyn käyttöön liittyvät eettiset periaatteet ja niiden soveltaminen tietojärjestelmiin

Viranomaisten toimintaprosessien automatisointi, muun muassa algoritmipohjaisesti, voi muuttaa viranomaiskäytäntöjä tavoilla, joista saattaa seurata tarve tarkastella viranomaiskäytännön arvo- ja normipohjaa ns. tekoälyn eettisten periaatteiden näkökulmasta. Näillä periaatteilla viitataan suosituksiin, joita eri toimijat ovat ehdottaneet tekoälyn eettisesti hyväksyttävän kehittämisen ja soveltamisen perustaksi[65].

Ns. ensimmäisen sukupolven (2015–2019) suosituksissa ”luotettavuus” (engl. ”trustworthy”) ja ”luottamus” nähdään usein keskeisimpinä algoritmipohjaisten järjestelmien kehittämistä ja käyttöä ohjaavina tavoitteina. Viranomaisten käyttämien tietojärjestelmien kohdalla tämä edellyttää, että tietojen käsittelyyn käytettävät järjestelmät ovat teknisesti vakaita, ja järjestelmiä käytettäessä määritellään vastuuketjut selkeästi sekä turvataan yksityisyyden- ja tietosuojan tapaiset perusoikeudet.

Luotettavuudesta seuraa myös vaatimus ymmärrettävyydestä ja selitettävyydestä. Jotta yksilö voisi aidosti kokea esimerkiksi algoritmiavusteisesti tehdyt päätökset luotettavina, hänen tulisi voida hahmottaa, kuinka ne on tehty. Yksilöllä on siis oikeus ymmärrettävään selitykseen. Tietojen käsittelystä vastaavalla viranomaisella on puolestaan velvollisuus kuvata ymmärrettävällä tavalla, kuinka tietojen käsittely algoritmisten sovellusten avulla tosiasiallisesti tapahtuu.

Selitettävyys ja ymmärrettävyys ovat yhteydessä läpinäkyvyyteen. Vaikka näitä käsitteitä käytetään usein synonyymeina, ne tarkoittavat hiukan eri asioita. *Ymmärrettävyys* (engl. ”comprehensibility”) määritellään usein yksilön kyvyksi hahmottaa, kuinka järjestelmät toimivat. *Selitettävyys* (engl. ”explainability”) puolestaan viittaa kykyyn kuvata, miksi ja miten järjestelmä tuottaa alkutilasta lopputilan. ”Läpinäkyvyys” (engl. transparency”) kuvataan esimerkiksi tietojenkäsittelytieteessä kysymyksenä, missä määrin mallin tai neuroverkon toimintaa voidaan kuvata tai simuloida[66]. Malli on (täydellisen) läpinäkyvä

65 Laskutavasta riippuen ohjeistuksia on jo yli 160. Tekijöiden joukossa ovat niin kansalliset toimijat (Iso-Britannian parlamentin ylähuone, Kanada), EU (Euroopan komission High Level Expert Group), kuin muutkin kansainväliset toimijat (mm. OECD) ja uskonnolliset yhteisöt (The Rome Call for AI Ethics). Myös yleishyödylliset toimijat (IEEE, AI4people, EGE), akateemiset yhteisöt (Future of Life Institute) ja useat yritykset (mm. Microsoft, Google, IBM, Tieto) ovat julkaisseet omia periaatesuosituksiaan.

66 Tulkittavuus, läpinäkymättömyys tai selitettävyys voivat viitata (i) koko mallin tai järjestelmän ominaisuuksiin, (ii) yksittäisten järjestelmän komponenttien (kuten noodien tai parametrien) ominaisuuksiin tai (iii) järjestelmän ytimenä olevan algoritmin ominaisuuksiin (Lipton, Zachary (2016). The Mythos of Model Interpretability. arXiv:1606.03490v3).

ainoastaan silloin, kun syöteaineiston ja mallin parametrien avulla pystytään käymään läpi askel askeleelta mallin suorittama laskenta siten, että lopputuloksena on sama vaste kuin minkä malli tuottaa.

Usein todetaan, että oikeus selitykseen ei toteudu, jos esimerkiksi tietojen käsittelyssä käytetään sovelluksia, jotka ovat ns. mustia laatikoita. Nykyalgoritmeista jotkin ns. syväoppivat verkot (DNN, DCNN) ovatkin lähtökohtaisesti tässä mielessä läpinäkymättömiä. Tällä hetkellä ei ole menetelmiä, joiden avulla voitaisiin tarkastella, miten ne toimivat syvempien kerrosten tasolla. Niiden toiminnan selittäminen askel askeleelta on nykyisillä menetelmillä mahdotonta, ja siksi ne saattavat olla olemuksellisesti läpinäkymättömiä[67]. Monien nykyalgoritmien kohdalla läpinäkyvyys on kuitenkin tiedollista, ei olemuksellista. Tällöin läpinäkymättömyyden syy ei ole arkkitehtuurin syvyys tai prosessoinnin kompleksisuus, vaan se, että sovellus käyttää suurta määrää dataa. Tämän datan läpikäyminen on liian vaativaa ihmisen kaltaisille, rajallisille kognitiivisille toimijoille. Tällöin läpinäkyvyys johtuu pohjimmiltaan ihmisen kognitiivisten kykyjen rajoituksista, ei olemuksellisista tekijöistä.

Mustien laatikkojen ongelma on synnyttänyt paljon keskustelua. On esimerkiksi ehdotettu, että oikeus selitykseen pitäisi uudelleen muotoilla oikeutena kontrastiiviseen oikeutukseen[68]. Ehdotuksen ydin on, että hyvän hallinnon toteutuminen ei välttämättä edellytä yksilön näkökulmasta selitystä tai läpinäkyvyyttä, vaan riittävää *oikeutusta* yksilöä koskeville päätöksille. Oikeutus tarkoittaa, että yksilölle kerrotaan, kuinka häntä koskeva päätös perustellaan esimerkiksi kertomalla ne lakipykälät, joihin päätös perustuu, eikä niinkään kuvaamalla järjestelmien suorittamaa laskentaa syiden ja seurausten välisten riippuvuuksien tasolla. Jos esimerkiksi sosiaaliviranomainen tekee yksilöä koskevan hallintopäätöksen, ja toteaa, ettei yksilö ole oikeutettu sosiaalietuuteen, päätöksen oikeuttaminen edellyttää, että yksilölle kerrotaan, mihin asetuksiin tai muihin tekijöihin päätös perustuu. Keskeistä on, että perustelu on kontrastiivinen, toisin sanoen yksilölle kerrotaan lisäksi, missä olosuhteissa päätös olisi ollut toisenlainen. Esimerkiksi jos tulot olisivat pienemmät, sosiaalietuus voitaisiin myöntää.

Tätä ehdotusta on kritisoitu muun muassa toteamalla, että tapauksissa, joissa järjestelmät tekevät virheitä, saattaa virheiden yksilöiminen edellyttää kuitenkin viittaamista algoritmien tekemään laskentaan. Tällöin palataan takaisin läpinäkyvyyden tematiikkaan.

---

67 Humphreys erottelee olemuksellisen ja tiedollisen läpinäkymättömyyden. Ks. Humphreys, Paul (2004). Extending Ourselves: Computational Science, Empiricism and Scientific Method. Cambridge University Press.

68 Wachter, Sandra, Mittelstadt, Brent ja Russell, Chris (2018). "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR", Harvard Journal of Law and Technology. 31 (2) 841–887.

Vastaavasti on epäselvää, että vaikka oikeus kontrastiiviseen oikeutukseen täyttäisi yksilön oikeuden häntä koskevan tietojen käsittelyn ymmärrettävyyteen, voidaanko saman logiikan nojalla ratkaista viranomaispäätöksiin liittyvien vastuiden tiedolliset edellytykset. Jos viranomaispäätöksiin liittyvien vastuiden tulkitaan edellyttävän nimenomaan riittävää tiedollista pääsyä algoritmeihin ja niiden tekemään laskentaan, tulee viranomaisella olla riittävä ymmärrys laskennallisesta prosessista, jolla päätös on tuotettu. Siten vastuukysymysten kohdalla pelkkä velvollisuus tarjota kontrastiivinen oikeutus ei riittäne.

Tarkasteltaessa viranomaisten tietojärjestelmiä ja ylipäänsä algoritmista tietojenkäsittelyä erilaisissa hallintotehtävissä myös muut tekoälyn eettisissä suosituksissa mainitut periaatteet voivat olla merkityksellisiä. Esimerkiksi viime vuosina eettisissä ohjeistuksissa ja periaatekokoelmissa on otettu voimakkaasti kantaa itse periaatteiden normatiivisista tavoitteista. Eettisten periaatteiden keskeisin päämäärä on lähinnä riskien ja harmien, kuten syrjinnän tai yksityisyydenloukkausten, ennaltaehkäisyssä ja minimoinnissa (non-maleficance), ei niinkään positiivisten vaikutuksien tukemisessa tai mahdollistamisessa (beneficence).

Tietojen käsittelyyn kohdistuvien asianmukaisuuden tai tarkoituksenmukaisuuden kaltaisten edellytysten kohdalla nouseekin esiin vastaava kysymys: tulkitaanko asianmukaisuus tai tarkoituksenmukaisuus ensisijaisesti haittavaikutusten minimoinnin vaiko mahdollisten positiivisten vaikutuksien tukemisen tai mahdollistamisen näkökulmasta? Jos ne tulkitaan negatiivisten seurausten minimoimisena, niin tietojärjestelmiin kohdistuvan sääntelyn tehtävä on estää tietojen asianmukaisen käsittelyn vaarantuminen käytettyjen algoritmien tai muun automatiikan vuoksi. Jos taas asian- tai tarkoituksenmukaisuus tulkitaan positiivisten seurausten näkökulmasta, keskeiseksi nousee, missä määrin sääntelyllä voidaan tukea algoritmien avulla tapahtuvaa viranomaistoimintaa siten, että tietojen käsittelyn asian- tai tarkoituksenmukaisuus toteutuisi tosiasiallisesti aiempaa paremmin.

Ylipäänsä eettisten periaatteiden näkökulmasta keskeistä on, kuinka tietojärjestelmien ja tietojen käyttöön liittyvässä viranomaistoiminnan sääntelyssä nähdään yhdenvertaisuuden, yksityisyydensuojan, itsemääräämisoikeuden, turvallisuuden ja koskemattomuuden kaltaiset eettiset periaatteet. Olennaista on, pyritäänkö sääntelyllä tukemaan automaattista tietojen käsittelyä siten, että se parantaa kaikkien kansalaisten oikeuksia yhdenvertaiseen kohteluun, vai onko kyse pelkästään algoritmeihin sisältyvien mahdollisen syrjinnän ennaltaehkäisystä. Kehitetäänkö tietojen viranomaiskäyttöä tavalla, joka tukee inklusiivisuutta tai myönteistä demokratiakehitystä, vai pyritäänkö estämään eriarvoistumista tai digitaalista polarisaatiota? Tuetaanko sääntelyllä tietosuojaa, itsemääräämisoikeuksia tai turvallisuutta, vai ennaltaehkäistään niiden vaarantamista?

6.4 Tietojen siirtäminen yleisessä tietoverkossa

Tiedonhallintalain 14.1 §:n mukaan viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.

Tiedonsiirtoon liittyvässä sääntelyssä ei ole tarkemmin säädetty, minkälaisia menettelyjä ja menetelmiä käyttäen salassa pidettävää tietoa voidaan siirtää Internetissä. Lainkohdassa ei ole myöskään säädetty, miten vastaanottajan varmistaminen tai tunnistaminen pitäisi toteuttaa. Sääntelyn tarkempi toteuttaminen jääkin viranomaisen vastuulle sekä alan muun soft law-tyyppisen sääntelyn varaan. Tämä on myös teknologianeutraaliuden kannalta perusteltua.

Tietojen siirtämistä yleisessä tietoverkossa koskevan sääntelyn tarkoituksena on asettaa yleiset vaatimukset sille, miten viranomaisten on suojattava salassa pidettäviä aineistojaan. Toteutustapaan vaikuttaa myös se, minkälaista aineistoa yleisessä tietoverkossa siirretään. Esimerkiksi turvallisuusluokitelluille asiakirjoille säädetään erityisiä käsittelyvaatimuksia tiedonhallintalain nojalla annetulla asetuksella asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Tietojen siirtoon liittyvät tietoturvallisuusvaatimukset ovat osa tietosuoja-asetuksessa tarkoitettuja teknisiä toimia henkilötietojen suojaamiseksi.

6.5 Tunnistaminen ja käyttöoikeudet

Kirjautumisesta tai käyttäjien tunnistamisesta tietojärjestelmiin ei ole varsinaisesti säädetty yleislainsäädännössä. Erityislainsäädännössä esimerkiksi asiakastietolain (159/2007) 8 §:n mukaan asiakastietojen sähköisessä käsittelyssä asiakas, sosiaalihuollon ja terveydenhuollon palvelujen antaja, muu asiakastietojen käsittelyn osapuoli ja näiden edustajat sekä tietotekniset laitteet tulee tunnistaa luotettavasti. Potilastietoja käsittelevien henkilöiden, palvelujen antajien, tietoteknisten laitteiden sekä valtakunnallisten tietojärjestelmäpalvelujen tunnistaminen edellyttää lisäksi todentamista.

Digipalvelulain 6 §:ssä säädetään digitaalisen palvelun käyttäjän sähköisestä tunnistamisesta. Pykälän 1 momentissa säädetään, missä tilanteessa digitaalisen palvelun käyttäjän sähköinen tunnistaminen on sallittua. Säännöksen mukaan viranomainen voi vaatia digitaalisessa palvelussa käyttäjältä sähköistä tunnistamista vain, jos se on tarpeen palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi tai palvelussa tehtävään toimeen liittyvien oikeusvaikutusten vuoksi. Pykälän 2 momentissa säädetään puolestaan

velvollisuudesta tunnistaa vahvaa sähköistä tunnistuspalvelua tai perustellusta syystä muuta vastaavaa tietoturvallista tunnistuspalvelua käyttämällä digitaalisen palvelun käyttäjä, jos palvelusta on mahdollista saada salassa pidettäviä tietosisältöjä nähtäväksi ja käytettäväksi.

Tietojärjestelmiin kirjautumisen yhteydessä käyttäjä yksilöidään jollakin menetelmällä (tunnistetaan). Tämän perusteella tietojärjestelmä määrittelee käyttäjällä käyttöoikeudet tai pyytää käyttäjän yksilöimään, missä roolissa hän käyttää tietojärjestelmää. Pääsyn- ja käyttöoikeuksien hallinnan avulla käytännössä määritellään käyttäjän oikeudet tehdä tietojärjestelmällä niitä toimia tai toimenpiteitä, joihin hänellä on toimivaltuus/toimivalta. Tällä on merkitystä muun muassa virkavastuun yksilöimiseksi sekä tehtyjen oikeudellisesti merkityksellisten toimien todentamiseksi.

Tiedonhallintalain 16 §:ssä säädetään käyttöoikeuksien määrittelystä ja ylläpidosta tietojärjestelmissä. Säännöksen mukaan tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina. Käyttöoikeuksilla määritellään muun muassa tietojärjestelmän käyttäjien oikeuksia tehdä erilaisia toimia ja toimintoja tietojärjestelmissä.

Käyttöoikeuksien tarkoituksena on myös rajata tiedonsaantia tietojärjestelmästä. Laillisuusvalvonnassa on myös kiinnitetty huomiota siihen, että viranomainen ei voi tehdä tietojärjestelmiin esimerkiksi tiedonsaantioikeuksia rajaavia määrityksiä ilman, että viranomaisella olisi laissa säädettyä toimivaltaa tällaiseen rajaamiseen, erityisesti hallinnon asiakkaan oikeuksia toteutettaessa.[69] Tällaiset lakitasoiseen sääntelyyn perustuvat rajaukset on tehtävä laissa, jonka jälkeen ne voidaan panna täytäntöön viranomaisen tietojärjestelmissä.

6.6 Lokitietojen kerääminen

Tiedonhallintalain 17 §:n mukaan viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.

69 OKV/31/50/2019, 13.5.2020 ja OKV/2057/1/2017, 18.12.2018.

Säännöksen perustelujen mukaan, jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, tulee luovuttavassa järjestelmässä kerätä luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen perusteensa. Lisäksi käyttölokitiedot tulee kerätä ainakin tietojärjestelmistä, joissa käsitellään salassa pidettäviä tietoja. Käyttölokitietojen keräämisen tarvearviointi perustuu siihen, tarvitaanko niitä virheselvittelyjä varten tai yksilön etujen, oikeuksien ja velvollisuuksien sekä oikeusturvan toteuttamiseksi taikka virkavastuun todentamiseksi.

Käyttölokitiedot ovat merkityksellisiä myös täysin automatisoiduissa prosesseissa. Tietojärjestelmää voidaan valvoa ja mahdolliset virheet voidaan havaita tietojärjestelmän toimintaa kattavasti kuvaavien lokitietojen avulla. Lokitietojen avulla voidaan jäljittää automaattisen käsittelyn kulku ja siinä käytetyt tiedot sekä se, missä määrin, jos ollenkaan, virkamies on osallistunut asian käsittelyyn. Näin voidaan varmistaa automaattisen toiminnan lainmukaisuus, asianosaisen oikeusturva, sekä virkavastuun kohdentuminen. Tiedonhallintalain 17 §:ssä on sinällään huomioitu käyttölokien kerääminen, mutta se jättää viranomaisille tarveharkintaa lokien keräämisen laajuuden osalta.

Tiedonhallintalain 17 §:ää tulisi kehittää siten, että siinä tarkennetaan, mitä lokitietojen tulee kuvata tietojärjestelmän toiminnasta. Automaattisten toimintaprosessien kannalta kyse olisi siis enemmänkin teknisen lokitiedon keräämisestä kuin käyttölokeista.

6.7 Tekninen rajapinta ja katseluyhteys

Tiedonhallintalain 22 ja 24 §:ssä säädetään teknisten rajapintojen käytön edellytyksistä silloin, kun tietoja luovutetaan viranomaisten tietojärjestelmien välillä tai viranomainen luovuttaa tietojärjestelmästään tietoja muulle kuin viranomaiselle. Tekniset rajapinnat mahdollistavat tietojen keräämisen eri viranomaisten tietovarannoista esimerkiksi asian selvittämisvaiheessa. Automatisoiduissa prosesseissa tekniset rajapinnat ovat merkityksellisiä käytettäessä prosessissa toisen viranomaisen teknisiä rajapintoja.

Teknisiä rajapintoja koskevassa sääntelyssä ei ole säädetty, miten ja missä tilanteessa teknisten rajapintojen avulla saatuja tietoja voidaan käyttää, vaan edellytyksistä, joilla teknisten rajapintojen avulla tietoja voidaan luovuttaa. Osa teknisistä rajapinnoista on voitu toteuttaa ainoastaan viranomaisen kontrolli- ja valvontatarkoituksiin, jolloin tietoja ei käytetä suoraan päätöksenteossa, vaan saatujen tietojen tarkoituksena voi olla esimerkiksi asianosaisen antamien tietojen oikeellisuuden tarkistaminen. Toisaalta viranomaiset keräävät tietoja teknisten rajapintojen avulla siten, että saadut tiedot voivat toimia pohjana viranomaisaloitteisten asioiden käsittelylle. Tilanteissa, joissa teknisten rajapintojen avulla saatuja tietoja käytetään suoraan ja mahdollisesti automatisoidusti yksilön etuja,

oikeuksia ja velvollisuuksia koskevassa päätöksenteossa, voidaan asettaa korkeita tietojen laatuun liittyviä vaatimuksia, koska näillä tiedoilla voi olla välitön vaikutus käsittelyn kohteena olevan asianosaisen (rekisteröidyn) oikeudelliseen asemaan.

Tietojen käytön, myös teknisten rajapintojen avulla saatavien tietojen käytön, edellytyksiä koskevaa sääntelyä on syytä täsmentää. Olisi täsmennettävä, millaisia vaatimuksia teknisten rajapintojen avaamiselle eri käyttötarkoituksiin on tarvetta säätää yksilön oikeusturvan varmistamiseksi automatisoiduissa toimintaprosesseissa. Tietojen laatua ja käyttöä koskevia sääntelytarpeita käsitellään tarkemmin arviomuistiossa jäljempänä.

Katseluyhteyksiä koskeva sääntely asettaa vaatimuksia katseluyhteyden tekniselle toteuttamiselle tietojärjestelmässä. Katseluyhteyksiä käytetään kuitenkin toimintaprosesseissa, joissa tietoja katselee tietojärjestelmän käyttäjä. Siten katseluyhteydet eivät toimi tietojen luovutustapana tilanteissa, joissa toimintaprosessi on automatisoitu.

6.8 Asianhallinta ja palvelujen tiedonhallinta

Tiedonhallintalain 25.1 §:ssä säädetään asiakirjojen rekisteröintivelvollisuudesta. Lainsäädäntö ei aseta estettä sille, että asiakirjat rekisteröidään asiarekisteriin automaattisesti, kunhan rekisteröinnissä voidaan tuottaa lain 26 §:ssä säädetyt asiakirjoihin ja asioihin liittyvät kuvailutiedot (metatiedot).

Tiedonhallintalain 26 §:ssä säädetään asiarekisteriin rekisteröitävistä kuvailutiedoista. Näillä tiedoilla dokumentoidaan osaltaan asiankäsittelyn etenemistä sekä pyritään varmistamaan lainmukainen asiankäsittely. Kuvailutietojen avulla voidaan myös kehittää prosessiohjattuja automaattisia toimintaprosesseja, jolloin määritellyt kuvailutiedot toimivat pohjana prosessiohjaukselle. Tiedonhallintalain 26 §:ssä ei ole kuitenkaan säädetty varsinaisesti asiankäsittelyn vaiheisiin liittyvistä kuvailutiedoista, vaan kukin viranomainen määrittelee ne itse osana toimintaprosessiensa suunnittelua. Asiankäsittelyvaiheisiin ei voida luoda yhtä yhtenäistä mallia, vaan käsittelyvaiheen kuvailutietojen hallinnan yhdenmukaisuutta voidaan edistää erilaisten tiettyyn toimialaan kohdistuvien suositusten avulla.

Palvelujen tiedonhallinnasta säädetään tiedonhallintalain 27 §:ssä. Säännös luo yleiset puitteet sille, miten viranomaisten on otettava huomioon asiakirjojen yksilöintiin ja asiakirjajulkisuuden toteuttamiseen liittyvät vaatimukset huomioon tiedonhallinnassaan.

6.9 Johtopäätöksiä

Yleislainsäädännössä ei ole säädetty nimenomaisesti tietojärjestelmien ja niissä olevien automatisoitujen prosessien asianmukaisuuteen liittyvistä vaatimuksista, jotka pitäisi ottaa huomioon jo tietojärjestelmiä kehitettäessä. Tietojärjestelmiä käytetään keskeisesti viranomaisen selvittämisvelvollisuuden toteuttamisessa, joka jää hallintolaissa säädettynä varsin yleiselle tasolle. Yleislainsäädännössä ei ole säädetty hallinnon tietojärjestelmien olennaisista vaatimuksista hallintoasian asianmukaisen selvittämisvelvollisuuden toteuttamiseksi, vaan tämä jää viranomaisen laajaan ja osin sääntelemättömään harkintavaltaan. Viranomaisen on kuitenkin tehtävä tämä harkinta jo siinä vaiheessa, kun tietojärjestelmän toiminnallisuuksia suunnitellaan.

Hallinnon lainalaisuusvaatimuksen näkökulmasta tietojärjestelmien käyttöä koskevaa sääntelyä hallintoasioiden käsittelyssä voidaankin pitää puutteellisena. Työryhmän näkemyksen mukaan tällaisia vaatimuksia voitaisiin asettaa sääntelyssä, joka koskee *tietojärjestelmien olennaisia vaatimuksia*. Erityisesti työryhmä pitää tarpeellisena, että ainakin niihin tietojärjestelmien osiin, joissa asiaa käsitellään täysin automaattisessa toimintaprosessissa, kohdistettaisiin laissa säädettyjä olennaisia ja yhdenmukaisia asianmukaisen asiankäsittelyn varmistavia vaatimuksia.

Työryhmä pitää myös tarpeellisena arvioida jatkovalmistelussa sitä, että hallinnon asiakas saisi asiansa käsittelyssä tiedot siitä, mihin yksilöityihin tietoihin viranomainen perustaa päätöksentekonsa niissä tilanteissa, joissa päätös voidaan tehdä täysin automatisoidusti. Niin ikään asiakkaalle (asianosaiselle) tulisi kertoa yleisen tietosuoja-asetuksen edellyttämää informointia yksilöidymmin siitä, että hänen asiansa saatetaan käsitellä kyseisessä prosessissa täysin automaattisesti. Asianosaisaloitteisissa asioissa tällainen informointi pitäisi tehdä todennettavalla tavalla vireillepanon yhteydessä tai viimeistään ennen asian käsittelyn aloittamista. Viranomaisaloitteisissa asioissa informointi tehtäisiin siinä vaiheessa, kun asianosaista kuullaan asian käsittelyn aikana. Tilanteissa, joissa myönnettäisiin erityislainsäädännön perusteella jokin etu tai oikeus automatisoidusti ilman asianosaisen esittämää vaatimusta, tulisi informoitavat tiedot antaa osana viranomaisen tekemää päätöstä.

Jatkovalmistelussa tulisi arvioida, mitä tietoja asiakkaalle tulisi antaa täysin automatisoidusta toimintaprosessista, ja liittyisikö tähän informointiin mahdollisesti jotain oikeuksia, joita asiakas voisi käyttää tietosuoja-asetuksessa säädettyjen oikeuksiensa lisäksi. Työryhmä ei kuitenkaan pidä realistisena eikä ymmärrettävyyden tai selitettävyyden kannalta tarkoituksenmukaisena sitä, että automatisoitujen toimintaprosessien algoritmit tulisi julkistaa tai esittää asianosaiselle. Annettavien tietojen tulisi, hyvän hallinnon periaatteita noudattaen, olla asiakkaan kannalta ymmärrettäviä ja konkreettisia, jotta hän voi käyttää menettelyyn liittyviä tai tiedollisia oikeuksiaan.

Myös vastuukysymyksien läpinäkyvyyttä tulisi selkeyttää. Tietoa siitä, kuka vastaa julkisen vallan käytöstä, ei pitäisi jättää pelkästään julkisuuslaissa säädettyjen tiedonsaantioikeuksien varaan. Tietojen tulisi siis myös virkavastuuseen liittyvistä syistä olla asianosaiselle annettavissa osana asiankäsittelyn dokumentaatiota. Tällä omalta osaltaan korostettaisiin myös sitä, että viranomaisen tietojärjestelmän toiminnassa on pystyttävä osoittamaan toiminnasta vastuulliset henkilöt. Tällainen läpinäkyvyyteen liittyvä vaatimus edellyttää tarkempaa lisäarviointia, koska tietojärjestelmien kehittämistä koskevat velvollisuudet hajautuvat viranomaisessa tyypillisesti useammalle henkilölle. Kaikki nämä henkilöt eivät välttämättä ole edes palvelussuhteessa viranomaiseen, vaan toimintavelvollisuudet toteutetaan viranomaisen toimeksiannosta. Lisäksi tietojärjestelmän hankinnan, kehittämisen ja käytön kannalta merkityksellisiä päätöksiä voidaan tehdä toimielimessä, esimerkiksi jossain kunnan toimielimessä.

Vastuuseen nimetyt henkilöt voivat myös vaihtua viranomaisessa, jolloin pelkästään uuden henkilön tai tietyn roolin edustajan nimeäminen vastuulliseksi ei täytä tosiasiallisen virkavastuun vaatimuksia, koska tällaisissa tilanteissa pitäisi olla jokin toimintavelvollisuus, josta uusi nimetty henkilö tai roolin haltija olisivat vastuussa. Se, missä määrin virkamieshallinnon ulkopuolisia voivat olla vastuussa tietojärjestelmän teknisten ja toiminnallisten vaatimusten täyttämisen varmistamisesta, edellyttää jatkovalmistelussa tarkempaa arviointia, kunhan nämä vaatimukset ja toimintavelvollisuudet ovat konkretisoituneet. Esimerkiksi kunnissa tietojärjestelmiä kehittävät, kuntaan palvelussuhteessa olevat henkilöt eivät läheskään aina ole virkasuhteessa, tai tietojärjestelmistä vastuussa ovatkin IT-yritykset.

Viranomaisten toiminnassa digitaalisissa palveluissa käytetään jo varsin yleisesti palveluautomaatiota neuvontavelvollisuuden toteuttamiseksi sekä palveluihin ohjaamiseksi. Kuitenkaan tällaiselle automaation käytölle ei ole olemassa hyvän hallinnon ja oikeusturvan sekä muiden perusoikeuksien toteutumista varmistavaa lainsäädäntöä. Tällainen neuvonta ja palveluohjaus voivat vaikuttaa hallinnon asiakkaaseen merkittävästi. Työryhmä pitää tarpeellisena, että lainsäädännön valmistelussa selvitetään mahdollisuudet säätää esimerkiksi digipalvelulaissa edellytykset tällaisille automatisoiduille toiminnallisuuksille.

Tiedonhallintalaissa säädetään lähinnä tietoturvallisuuteen liittyvistä vaatimuksista, jotka kohdentuvat suoraan tietojärjestelmiin. Niin ikään asianhallinnan sääntely asettaa suoraan vaatimuksia tietojärjestelmän toiminnallisuuksille sekä kerättävien tietojen sisällölle. Tiedonhallintalaissa ei ole säädetty varautumiseen liittyvistä vaatimuksista. Tällaista sääntelyä voidaan pitää tarpeellisena, koska viranomaisen on varauduttava toiminnassaan siihen, että tietojärjestelmät vikaantuvat tai niiden toiminta muusta syystä estyy. Viranomaisen on pystyttävä suorittamaan tehtävänsä myös tilanteissa, joissa tietojärjestelmää ei voida käyttää. Työryhmän näkemyksen mukaan tiedonhallintalaissa tulisi säätää varautumiseen liittyvistä vaatimuksista.

Tiedollisten oikeuksien ja oikeusturvan toteutumisen, sekä asiankäsittelyn asianmukaisuuden, läpinäkyvyyden ja virkavastuun toteutumisen kannalta olisi syytä arvioida, missä määrin ns. black box -tekoälyjä on mahdollista käyttää toimintaprosessien automatisointiin. Tällaisille tekoälyteknologioille ominaista on se, että tarkkaa toimintalogiikkaa ei pystytä ymmärtämään joko sen perimmäisestä luonteesta johtuen, tai koska se on ihmisen ymmärryskyvyn saavuttamattomissa; kummassakin tapauksessa järjestelmään syötetään tietoa ja se tuottaa näistä lopputuloksia, mutta ihminen ei pysty käsittämään, mihin lopputulokset perustuvat. Työryhmän näkemyksen mukaan varsinainen tekoälyjärjestelmien käytön edellytysten sääntelytarpeen tarkempi arviointi tulisi tehdä siinä vaiheessa, kun Euroopan unionissa valmisteilla oleva sääntely on tarkentunut. Tästä syystä työryhmä ei näe edellytyksiä sille, että tässä vaiheessa kansallisella valmistelulla voitaisiin lähteä ratkomaan varsinaisten tekoälyjärjestelmien käyttöön liittyviä sääntelytarvekysymyksiä.

7 Virkavastuu tietojärjestelmien kehittämisessä ja käytössä

Tietojärjestelmien kehittämiselle on ominaista projektiluonteinen ja ryhmissä tehtävä työ, joka on omiaan hämärryttämään eri toimijoiden vastuuta.[70] Kehittämistä tehdään pääsääntöisesti julkisen hallinnon organisaation ja yksityisoikeudellisen yhteisön välisenä yhteistyönä projekteissa, joissa vastuukysymyksiä on joiltakin osin ratkaistu tietojärjestelmien toimitussopimuksissa.

7.1 Virkavastuu

Perustuslain 118 §:ssä on säädetty *virkamiehen vastuusta virkatoimistaan*. Pykälän 1 momentin mukaan virkamies vastaa virkatoimiensa lainmukaisuudesta. Hän on myös vastuussa sellaisesta monijäsenisen toimielimen päätöksestä, jota hän on toimielimen jäsenenä kannattanut. Pykälän 2 momentin mukaan esittelijä on vastuussa siitä, mitä hänen esittelystään on päätetty, jollei hän ole jättänyt päätökseen eriävää mielipidettään.

Perustuslain 118 §:n 3 momentissa vielä säädetään, että jokaisella, joka on kärsinyt oikeudenloukkauksen tai vahinkoa virkamiehen tai muun julkista tehtävää hoitavan henkilön lainvastaisen toimenpiteen tai laiminlyönnin vuoksi, *on oikeus vaatia tämän tuomitsemista rangaistukseen sekä vahingonkorvausta julkisyhteisöltä taikka virkamieheltä tai muulta julkista tehtävää hoitavalta sen mukaan kuin lailla säädetään*. Tässä tarkoitettua syyteoikeutta ei kuitenkaan ole, jos syyte on perustuslain mukaan käsiteltävä valtakunnanoikeudessa.

Perustuslain 118 §:n 3 momenttia on muutettu vuonna 2011 (L 1112/2011) siten, että sanamuotoon aiemmin kuulunut ”sen mukaan kuin lailla tarkemmin säädetään” on muutettu muotoon ”sen mukaan kuin lailla säädetään”. Ennen muutosta asianomistajalla katsottiin olevan suoraan perustuslain 118 §:n 3 momentin nojalla oikeus nostaa syyte virkarikoksesta virkamiestä vastaan. Muutoksella on tavoiteltu laajempaa lainsäätäjän harkintavaltaa, ja käytännössä mahdollisuutta järjestää asianomistajan syyteoikeus myös virkarikosasioissa toissijaiseksi, kuten rikosasioissa pääsääntönä on. Lain perusteluissa on lisäksi katsottu, että oikeusvaltioperiaatteen toteutumisen kannalta ei

70 Tähän kysymykseen on kiinnitetty huomiota jo 1980-luvulla tietojärjestelmien kehittämisessä, ks. Kuopus, Jorma (1988): Hallinnon lainalaisuus ja automatisoitu verohallinto, esim. s. 525–526.

ole merkityksellistä, onko asianomistajan syyteoikeus järjestetty ensisijaiseksi vai toissijaiseksi.[71] Tarkoitettu muutos on toteutettu oikeudenkäynnistä rikosasioissa annetun lain (689/1997, rikosoikeudenkäyntilaki) muutoksella (L 18/2012).[72] Nykyisin rikosoikeudenkäyntilain 1 luvun 14 §:n 1 momentissa säädetään, että asianomistaja saa itse nostaa syytteen rikoksesta vain, jos syyttäjä on päättänyt jättää syytteen nostamatta taikka esitutkintaviranomainen tai syyttäjä on päättänyt, ettei esitutkintaa toimiteta taikka että se keskeytetään tai lopetetaan. Asianomistaja saa nostaa syytteen myös, jos esitutkintatoimenpiteiden suorittamista on tutkinnanjohtajan päätöksellä siirretty. Tämä pääsääntö on voimassa myös virkarikosten kohdalla. Sen sijaan virkamiehen tai julkisyhteisön vahingonkorvausvastuun osalta oikeustilaa ei ole muutettu.

Perustuslaissa tarkoitettua oikeutta vaatia virkamiehen tuomitsemista rangaistukseen voidaan soveltaa, vaikka virkavelvollisuuden rikkomista koskevilla säännöksillä suojellaan ensisijaisesti virkatoiminnan oikeellisuuteen liittyvää yleistä etua, mikäli teot ovat myös sellaisia, että ne loukkaavat rangaistusta vaativan henkilön oikeuksia.[73] Toisaalta säännöksen ei ole nähty mahdollistavan muiden kuin rikoksen varsinaisten asianomistajien oikeutta vaatia rangaistusta, vaikka oikeus vaatia vahingonkorvausta saman teon perusteella olisikin.[74] Asianomistajan oikeus vaatia rangaistusta perustuu rikosoikeudenkäyntilakiin ja oikeus vahingonkorvaukseen ratkaistaan puolestaan pääsääntöisesti vahingonkorvauslain (412/1974) mukaisesti. Tästä tekee kuitenkin joissakin tilanteissa poikkeuksen tietosuoja-asetuksessa säädetty vahingonkorvausvastuu, joka on kohdennettu rekisterinpitäjälle ja joissakin tilanteissa henkilötietojen käsittelijälle. Säännöstä sovelletaan ensisijaisesti henkilötietojen käsittelystä johtuvien vahinkojen vahingonkorvausvelvollisuutta arvioitaessa.

71 HE 60/2010 vp, s. 46–47.

72 HE 116/2011 vp.

73 KKO 2007:46, kohdat 1–4. Tähän oikeusohjeeseen on syytä liittää pieni varauma, sillä perustuslakia on muutettu lailla 1112/2011 siten, että aiemmin säännöksen sanamuodossa käytetystä ilmaisusta ”sen mukaan kuin lailla tarkemmin säädetään” on poistettu sana ”tarkemmin”. Ehdotettua sanamuotoa on pidetty lainsäätäjän harkintavallan kannalta väljempänä, ja sen on katsottu mahdollistavan esimerkiksi syyttäjän syyteoikeuden ensisijaisuuden ja asianomistajan syyteoikeuden toissijaisuuden, ks. HE 60/2010 vp, s. 46–47. Myös oikeudenkäynnistä rikosasioissa annettua lakia on perustuslain muuttamisen myötä muutettu siten, että myös virkarikosasioissa syyttäjän syyteoikeus on pääsäännön mukainen eli ensisijainen suhteessa asianomistajaan, ks. HE 116/2011 vp.

74 KKO 2004:75, kohdat 1–5.

7.2 Virkavastuun kohdentuminen tietojärjestelmiä käytettäessä

Muodollisen virkavastuun toteuttamiseen, ilman tosiasiallisen virkavastuun toteuttamisen mahdollisuutta käytännössä, on suhtauduttu kielteisesti sekä eduskunnassa lakiehdotuksen käsittelyn yhteydessä että korkeimmassa hallinto-oikeudessa viranomaisen toteuttaman järjestelyn yhteydessä.[75] Perustuslakivaliokunta on pitänyt selvänä, ettei päätöksenteon siirtäminen automaattiseen käsittelyyn saa johtaa siihen, että virkavastuuta koskevat perustuslain säännökset menettävät merkityksensä.[76] Automaattisen päätöksenteon ja muutoinkin tietojärjestelmien käytössä virkavastuumallin rakentamisessa tulee siten mahdollistaa virkavastuun toteutuminen tosiasiallisesti. Virkavastuuseen kuuluu myös siten julkisen vallan käytöstä ja konkreettisesti hallintopäätöksestä vastuussa olevan henkilön tai henkilöiden yksilöinti siten, että tällaisille henkilöille kohdistetaan toimintavelvollisuuksia, joilla voidaan varmistaa asianosaisen oikeuksien toteutuminen sekä muun viranomaisen toiminnan asianmukaisuus. Virkavastuukysymykset ovat merkityksellisiä myös hallinnon sisällä tehtävistä taloudellisista toimista päätettäessä, vaikka niissä ei suoraan olisikaan asianosaista.

Nykyinen hallintomenettelyllinen sääntely ei edellytä muodollisesti vastuussa olevan henkilön tai henkilöiden yksilöintiä hallintopäätöksessä. Toisaalta laillisuusvalvonnassa ja oikeuskäytännössä on katsottu, että julkisen vallan käyttäjien on toimittava nimillään, ja myös hyvään hallintoon kuuluu päätöksentekijän yksilöinti esimerkiksi allekirjoituksella.[77] Laillisuusvalvonnassa on myös todettu, että asian käsittelijän nimen avoin ilmoittaminen olisi omiaan edistämään myös viranomaisen toiminnan kontrolloitavuutta. Hallinnon asiakkaalla ei esimerkiksi ole mahdollisuutta reagoida asiaansa käsittelevän henkilön esteellisyyteen, jos käsittelijä jää anonyymiksi.[78]

Hallintolakia säädettäessä ei eduskuntakäsittelyssä virkavastuun kohdentamista arvioitu hallintovaliokunnan mietinnössä, vaan asiaa arvioitiin lähinnä oikeusturvan näkökulmasta.[79] Siten voidaan todeta, että hallintolaissa olevat hallintopäätöksen sisältöön liittyvät muotovaatimukset eivät ole yleisemminkään ongelmattomia suhteessa siihen, mitä virkavastuusta ja sen kohdentamisesta on säädetty perustuslain 118 §:ssä.

75 Ks. PeVL 9/2018 vp ja KHO 2014:98.

76 PeVL 7/2019 vp, s. 11.

77 OKV/399/1/2017, EOA 686/4/09, KHO 2014:83, KHO 2019:11 ja EOA 1084/4/00, 11.3.2002

78 OKV/305/10/2020 – OKV/316/10/2020, 2.5.2021.

79 HaVM 29/2002 vp, s. 9.

Laissa ei tällä hetkellä erikseen säädetä virkamiehen roolista tietojärjestelmän kehittämisen valvonnassa ja ominaisuuksien ja toiminnallisuuksien määrittelyssä, testaamisessa tai käyttöönotossa. Tietojärjestelmien käytön valvonta perustuu tietosuoja-asetuksen 24 (1), 25 (2) ja 32 (4) artiklassa säädettyyn rekisterinpitäjän vastuuseen toteuttaa tekniset ja organisatoriset toimet henkilötietojen suojaamiseksi ja sen varmistamiseksi, että henkilötietoja käsitellään rekisterinpitäjän ohjeiden mukaisesti. Käytännössä eräs tällainen asetuksessa tarkoitettu toimi on valvonnan järjestäminen ja sen dokumentointi. Tietosuoja-asetuksen 39 (1) artiklan mukaisesti tietosuojavastaavan tehtävänä valvoa tietosuojaa koskevien vaatimustenmukaisuuden noudattamista. Tiedonhallintalain 4 §:n 2 momentin 5 kohdassa puolestaan säädetään siitä, että tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta. Edellä esitetyssä sääntelyssä ei ole kuitenkaan säädetty mitään erityisiä vaatimuksia valvonnalle tai sen toteuttamiselle, vaan se jää laajasti rekisterinpitäjän ja tiedonhallintayksikön johdon vastuulle.

Se, että riittävä asiantuntemus viranomaisen puolelta on käytettävissä tietojärjestelmän elinkaaren eri vaiheissa, riippuu tällä hetkellä viranomaisen oma-aloitteisuudesta sekä siitä, miten yleisiä lainsäädännön vaatimuksia esimerkiksi hyvän hallinnon, tehokkaan toiminnan ja asianmukaisen käsittelyn toteuttamisesta tulkitaan ja noudatetaan.

Viranomaisen ei tarvitse nykylainsäädännön mukaan tehdä päätöstä tietojärjestelmän käyttöönottamisesta tai käytössä olevan tietojärjestelmän olennaisesta muutoksesta, kuten valmistelussa käytettävän automaation käyttöönottamisesta. Tämä jää pikemminkin hallinnon sisäiseksi toiminnaksi, joka on eri viranomaisissa järjestetty eri tavoin. Varsinainen päätös esimerkiksi tietojärjestelmän tai siihen liittyvien palveluiden hankinnasta on tosin yleensä erillinen päätös, mutta se jää irralliseksi varsinaisesta tietojärjestelmän käyttöönottoa tosiasiassa koskevasta ratkaisusta.

7.3 Valvonta

Tietojärjestelmien käyttöä koskeva valvonta on hajautunut monelle eri viranomaiselle ja osin valvonta perustuu viranomaisen sisäiseen valvontaan tai nk. omavalvontaan.

Tietosuoja-asetuksen 51–59 artikloissa on säädetty tietosuojan valvontaviranomaisesta, sen tehtävistä ja toimivallasta. Tietosuojalain (1050/2018) 3 luvussa on säädetty tietosuoja-asetuksessa tarkoitetusta kansallisesta valvontaviranomaisesta, joka on tietosuojavaltuutettu. Koska tietojärjestelmissä käsitellään pääosin henkilötietoja ja automatisoidun päätöksenteon rajoitussääntely perustuu tietosuoja-asetukseen, toimii

tietosuojavaltuutettu suoraan tietosuoja-asetuksen ja tietosuojalain nojalla valvontaviranomaisena silloin, kun kysymys on tietojärjestelmien käytöstä ja niihin sovellettavasta tietosuojalainsäädännön noudattamisesta.

Tietosuoja-asetuksessa on säädetty myös rekisterinpitäjän ja henkilötietojen käsittelijän omavalvonnasta. Viranomaistoiminnassa kaikilla rekisterinpitäjällä on oltava nimettynä tietosuojavastaava, jonka nimittämisestä, asemasta ja tehtävistä on säädetty tietosuoja-asetuksen 37–39 artikloissa. Tietosuoja-asetuksen 39 (1) artiklan b alakohdan mukaan tietosuojavastaavan tehtävänä on muun muassa valvoa (monitor compliance) tietosuoja-asetuksen ja muun tietosuojasääntelyn noudattamista. Rekisterinpitäjälle on puolestaan säädetty useissa tietosuoja-asetuksen säännöksissä velvollisuuksia toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi ja käsittelyn vaatimustenmukaisuuden varmistamiseksi (5 (1) f alakohta, 24 (1) artikla, 25 (2) artikla, 32 (4) artikla). Näiden velvollisuuksien toteuttamisessa olennaisena osana on toteuttaa riittävät tekniset ja organisatoriset valvontajärjestelyt henkilötietojen käsittelyyn ja muun muassa rekisterinpitäjän antamien ohjeiden noudattamiseen.

Tiedonhallintalain 4.2 §:n mukaan tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta. Säännöstä voidaan pitää osin täydentävänä tietosuoja-asetukseen nähden, koska tiedonhallintalakia sovelletaan myös henkilötietojen käsittelyyn ja tiedonhallintalaissa on käytetty tietosuoja-asetuksen puitteissa kansallista liikkumavaraa. Valvonnan järjestämisvastuu on tiedonhallintalaissa kohdennettu suoraan tiedonhallintayksikön johdolle, jolloin johdon toimintavelvollisuutena on järjestää riittävä valvonta. Valvonnan kohteena on tiedonhallinta, joka saa sisältönsä tiedonhallintalaista, mutta josta on säädetty myös erityislainsäädännössä. Tiedonhallintaan sisältyy myös tietoturvallisuus. Tiedonhallintalain sääntelykohteena on muun muassa hallintoasioiden käsittelyssä käytettävä tietojärjestelmät, joten tiedonhallintalaissa tarkoitettu tiedonhallintayksikön omavalvonta ulottuu myös tietojärjestelmien kehittämiseen ja käyttöön.

Tiedonhallintalain 10.1 §:n 1 kohdan mukaan julkisen hallinnon tiedonhallintalautakunnan tehtävänä on arvioida valtion virastojen ja laitoksen sekä kuntien ja kuntayhtymien toimintaa, noudattavatko ne tiedonhallintalain 4 §:n 2 momentin, 5, 19, 22–24 ja 28 §:n sekä 6 luvun säännöksiä. Säännös sisältää myös toteuttamisen arvioinnin, miten tiedonhallintayksiköt ovat toteuttaneet tiedonhallintalaissa säädetyt vaatimukset. Tiedonhallintalautakunnan arviointitehtävä on valvonnallinen ja keskittyy mainittujen säännösten noudattamisen valvontaa. Toteutustavan arviointi puolestaan palvelee hyvin käytäntöjen tunnistamista ja levittämistä, joka tukee lautakunnalle tiedonhallintalain 10.1 §:n 2 kohdassa säädetty edistämistehtävää. Tiedonhallintalautakunta voi antaa tiedonhallintalain 11.3 §:n nojalla hallinnollista ohjausta arviointikohteilleen tiedonhallintalain mukaisten menettelyjen toteuttamiseen ja vaatimusten täyttämiseen.

Tietoturvallisuuden arviointilaitoksista annetun lain 6 §:n nojalla Liikenne- ja viestintävirasto valvoo tietoturvallisuuden arviointilaitoksia. Virkavastuun näkökulmasta katsottuna, arviointilaitosten toimintaan ei sovelleta virkavastuuta koskevia säännöksiä, kun ne suorittavat arviointilaitoslain perusteella arviointeja. Arviointilaitoslaissa on säädetty sinällään eräiden hallinnon yleislakien soveltamisesta arviointilaitosten toimintaan, mutta virkavastuuta tarkoittavaan sääntelyyn laissa ei ole säännöksiä. Tältä osin sääntelyä voidaan pitää puutteellisena. Sääntely jättää epäselväksi, miltä osin arviointilaitosten toiminta on julkisen hallintotehtävän hoitamista, jolloin tästä on säädettävä erikseen tietoturvallisuuden arviointilaitoksista annettuun lakiin (1405/2011, arviointilaitoslaki) nähden erityislaissa. Esimerkiksi asiakastietolaissa tai arviointilaissa ei ole säännöksiä, jolla arviointi sidottaisiin virkavastuusäännöksiin.

Ylimmät laillisuusvalvojat, eduskunnan oikeusasiamies ja valtioneuvoston oikeuskansleri, valvovat julkisten tehtävien hoitamista. Ylimmät laillisuusvalvojat ovat ottaneet laillisuusvalvonnassaan pääosin yksittäisten kanteluasioiden käsittelyn yhteydessä kantaa jo pitkällä aikavälillä julkisen hallinnon tietojärjestelmien käyttöä koskeviin ongelmiin erityisesti perusoikeuksien toteutumiseen ja muihin valtiosääntöisiin kysymyksiin liittyen, mutta myös yleis- ja erityislakien noudattamiseen tietojärjestelmien käytössä. Esimerkiksi vuonna 1996 eduskunnan oikeusasiamies totesi nykyistä Verohallintoa koskevassa ratkaisussaan, että pelkästään virkavastuu ja velvollisuus korvata verovelvolliselle virheestä mahdollisesti aiheutuvat vahingot eivät riittävästi takaa verovelvollisen oikeusturvan toteutumista. Oikeusasiamies piti tuolloin Verohallinnon tietojärjestelmien tietoturvallisuutta ja riskienhallintaa vakavasti puutteita sisältävänä.[80] Oikeusasiamies on myös tämän jälkeen kiinnittänyt toistuvasti huomiota verotuksen automatisointiin liittyviin laillisuusongelmiin.[81]

7.4 Johtopäätöksiä

Automaattisen toimintaprosessin käyttöönottamisessa olisi otettava huomioon automatisoitavan asiakokonaisuuden (tehtävän) tai -kokonaisuuksien (tehtävien) soveltuvuus automatisoituun asiankäsittelyyn ja päätöksentekoon. Viranomaisen toimintaan pitäisi kohdistaa selkeitä toimintavelvollisuuksia tietojärjestelmien kehittämisessä ja käyttöönotossa siten, että hyvän hallinnon ja oikeusturvan vaatimukset on varmistettu ennakollisesti toimintaprosesseissa. Virkavastuun asianmukainen toteuttaminen edellyttää sitä, että automatisoitujen toimintaprosessien kehittämiseen, käyttöönottoon sekä käytön seurantaan luodaan normisto, jonka perusteella virkamiesten ja muiden vastuullisten

80 EOA 73/4/96, 22.4.1996.

81 Ks. esim. EOAK/6863/2019, 28.12.2020, EOAK/3379/2018, 26.11.2019, EOAK/2216/2018, 20.11.2019 ja AOA 2826/2/13, 19.4.2016.

virkavelvollisuudet ovat selvästi määriteltävissä, ja nämä virkavelvollisuudet täyttämällä hallinnon lainalaisuusperiaatteen, oikeusturvan, hyvän hallinnon takeiden sekä muiden hallintolain menettelysäännösten, asiakirjajulkisuuden ja tietosuojan viranomaistoiminnalle asettamien vaatimusten toteutuminen turvataan asianmukaisesti. Lisäksi vahingonkorvausvastuu tulee järjestää siten, että automatisoitujen prosessien virheiden tai niiden kehittämiseen liittyvien laiminlyönnin vuoksi vahinkoa kärsinyt saa asianmukaisesti korvauksen vahingostaan. Asianmukainen muutoksenhaku- tai uudelleenkäsittelyjärjestelmä vähentää aiheutuvia vahinkoja kuitenkin merkittävästi. Osittain vahingonkorvausvastuu määräytyy tietosuoja-asetuksen perusteella, mutta se ei kata kaikkia tilanteita. Jatkoarvioinnissa on vielä selvitettävä, onko vahingonkorvauslainsäädäntöä muuten tarvetta täsmentää ottamaan huomioon automatisoidut prosessit julkista valtaa käytettäessä.

Virkavastuun tosiasiallinen toteuttaminen on mahdollista kehittämällä päätöksentekojärjestelmiä ja automatisoitujen toimintaprosesseja koskevia viranomaisen auditointimenettelyjä, sekä sisäisiä että ulkoisia menettelyjä. Algoritmien ja järjestelmien tekninen sekä juridinen arviointi voivat muodostaa sen virkatoimen, johon perustuslain 118 §:n mukainen vastuu kohdistuu. Jotta virkavastuu toteutuu asianmukaisesti, on auditoinnin suorittavien henkilöiden toimittava virkavastuulla. Perustuslain 124 §:n tulkintakäytännöstä johtuen tästä asiasta säätäminen muodostuu lainsäädännön perustuslainmukaisuuden edellytykseksi.[82]

Kaiken kaikkiaan tietojärjestelmien kehittäminen, käyttöönotto ja käyttö tulisi hahmottaa osana julkisen vallan käyttöä, kun niitä koskevaa sääntelyä kehitetään. Tällöin julkisen vallan käytölle pitäisi olla oikeudellinen perusta, joka tällä hetkellä on tietojärjestelmien kehittämiseen ja käyttöönottoon liittyvässä viranomaistoiminnassa varsin välillistä. Tähän toimintaan on myös kohdistettava riittäviä kontrolleja valvonnan mahdollistamiseksi. Säädetyt toimintavelvollisuudet puolestaan korostaisivat vallankäyttäjien vastuuta.

Lisäksi sääntelyä kehitettäessä on selvitettävä vielä erikseen, onko vallankäytön kohteena olevilla riittävän tehokkaan oikeussuojan mahdollistavat menettelyt. Tietojärjestelmien kehittäminen ja käyttöönotto ovat valmistelevia toimia siihen, että tietojärjestelmällä voidaan tehdä hallintopäätöksiä ja siten käyttää julkista valtaa. Eduskunnan hallintovaliokunta on lausunnossaan todennut, että valmistelutoimenpiteet voivat olla julkisen vallan käyttöä tehtävien kokonaisuuden osana, jolloin virkavastuu ulottuu myös tällaisiin tehtäviin päätöksenteon yhteydessä.[83] Myös eduskunnan tarkastusvaliokunta on kiinnittänyt huomiota virkavastuun hämärtymiseen erilaisissa tietojärjestelmäprojekteissa.[84]

82 Esim. PeVL 8/2014 vp, s. 5.

83 HaVL 2/2002 vp, s. 3.

84 TrVM 1/2008 vp, s. 3 ja 14.

Työryhmän näkemyksen mukaan tietojärjestelmien kehittämisen ja käytön valvontaan liittyviä vastuita tulisi eri viranomaisten välillä täsmentää tai selkeyttää. Osittain valvonta voidaan järjestää viranomaisen omana valvontana, mutta tämän rinnalle tarvitaan riittävä ulkoinen lain täytäntöönpanoon liittyvä valvontamekanismi. Tällaisen valvontamekanismin toimivuuden ja lain noudattamisen valvonta kuuluu suoraan, ilman erityistä sääntelyä, ylimmille laillisuusvalvojille. Arviointisääntelyn yhteydessä on vielä erikseen arvioitava, missä määrin valvontamekanismiin on tarvetta luoda oikeussuojakeinoja, jos valvontaan tai arviointiin liittyy viranomaispäätöksiä.

8 Tietovarantoihin kohdistuvat vaatimukset

8.1 Tietovarannot

8.1.1 Tietovarannon määritelmä ja liittyvät määritelmät

Kuten edellä luvussa 4 on kuvattu, lainsäädännössä viitataan tietojärjestelmiin ja tietovarantoihin erilaisilla, paikoin ristiriitaisillakin käsitteillä. Tiedonhallintalain (906/2019) 2 §:n mukaan *tietovarannolla* tarkoitetaan viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettäviä tietoaineistoja sisältävää kokonaisuutta, jota käsitellään tietojärjestelmien avulla tai manuaalisesti. Tietovarannoissa olevia tietoja käytetään hallinnon asiakkaiden ja muiden etujen, oikeuksien ja velvollisuuksien määrittämiseen ja toteuttamiseen sekä viranomaisten tehtävien hoitamiseen.

Säännöksen perusteluiden mukaan tietovaranto on viranomaisten tehtävien hoidon tuloksena syntyvistä tietoaineistoista muodostuva looginen kokonaisuus, joka koostuu sekä tietojärjestelmissä olevista tiedoista että muusta aineistosta, kuten paperiasiakirjoista.[85] Tietovarannon lisäksi laissa määritellään *yhteisten tietovarantojen* käsite, jolla tarkoitetaan toimijoiden käyttöön suunniteltua ja ylläpidettyä tietovarantoa, jonka tiedot ovat luovutettavissa ja hyödynnettävissä eri tarkoituksiin. Yhteisille tietovarannoille katsotaan olevan ominaista, että tietovarannon tiedot kerätään vain kerran ja päivitetään tiedon muuttuessa, jonka jälkeen ne ovat tietopalvelujen ja muiden tietoja hyödyntävien palvelujen käytettävissä.[86]

85 Ks. HE 284/2018 vp, s. 65.

86 Ks. HE 284/2018 vp. s. 65.

Tietovarantoja koskevassa erityislainsäädännössä tietovaranto-käsitettä on lähinnä tarkennettu tietovarannon käyttötarkoituksen kautta.[87] Tietovaranto käsitteenä korvautuu erityislainsäädännössä usein *tietojärjestelmällä*, vaikka sääntelykohteena olisivatkin tiedot, tietojenkäsittely sekä tietojenluovuttaminen tietovarannosta. Esimerkiksi Suomessa yhteiskunnan perusrekisterijärjestelminä pidetään *väestötietojärjestelmää* ja siihen kuuluvia rakennustietoja, *kiinteistötietojärjestelmää* sekä valtakunnallista *yritys- ja yhteisötietojärjestelmää*.[88] Nimikkeen tietojärjestelmä-käsitteestä huolimatta perustietovarantoja koskevalle sääntelylle on ominaista säännösten kohdistuminen ylläpidettäviin tietoihin sekä niiden luovuttamiseen ja saamiseen muita toimijoilta. Vastaavasti myös erityissääntelyssä tietovarantojen osalta on tyypillistä, että käytetään tietovarannon käsitteen sijaan tietojärjestelmän käsitettä, vaikka niissäkin sääntelykohteena ovat tietovaranto sekä siihen liittyvä tietojenkäsittely tai tietojenluovuttaminen.

Esimerkiksi maaseutuelinkeinohallinnon tietojärjestelmää koskevassa sääntelyssä määritellään tietojärjestelmän sisältö ja rakenne yksilöimällä rekisterit ja niiden sisällöt, rekisterinpitovastuut ja vastuut tietojen luovuttamisesta (laki maaseutuhallinnon tietojärjestelmästä (284/2008) 4–9 §). Kansallisen viisumitietojärjestelmän osalta sääntelykohteena ovat tietojärjestelmään tallennettavat tiedot, tietojen käsittely, rekisterinpitäjien vastuut sekä järjestelmään tietoihin kohdistuvat tietojensaantioikeudet ja tietojenluovuttaminen (Laki henkilötietojen käsittelystä maahanmuuttohallinnossa (615/2020) 5–14 a §). Huoneistotietojärjestelmän osalta sääntelykohteena ovat osakehuoneistoja ja hallintokohteita koskevien tietojen tallentaminen, tietojen käsittely sekä tietopalvelujen järjestäminen tietojen luovuttamiseksi (Laki huoneistotietojärjestelmästä (1328/2018) 2–4 luku).

Tietovarannon käsitteeseen liittyy tai rinnastuu usein myös *rekisterin* käsite. Viranomaisen toiminnan julkisuudesta annetussa laissa (621/1999, julkisuuslaki) käytetään käsitettä *yleiseen käyttöön tarkoitettu rekisteri* tai *viranomaisen rekisteri*, ilman käsitteen tarkempaa määrittelyä. Julkisuuslakiin sisältyy myös käsite *rekisteriviranomainen* (15.2 §).

87 Esimerkiksi oikeushallinnon valtakunnallinen tietovaranto palvelee oikeusministeriön hallinnonalan tutkimus- ja suunnittelutoimintaa (laki oikeushallinnon valtakunnallisesta tietovarannosta 955/2020), varhaiskasvatuksen valtakunnallinen tietovaranto mahdollistaa varhaiskasvatustietojen turvallisen kokoamisen sähköisesti (varhaiskasvatuslaki 540/2018) ja opetuksen ja koulutuksen valtakunnallista tietovarantoa käytetään henkilön hakeutuessa koulutukseen, koulutuksen aikana, työelämässä sekä henkilön hakiessa koulutukseen liittyviä etuisuuksia (Laki valtakunnallisista opinto- ja tutkintorekistereistä 884/2017).

88 Ks. HE 89/2008 vp, s. 64. Vuoden 2019 loppuun saakka voimassa olleen julkisen hallinnon tietohallinnon ohjauksesta annetun lain (634/2011) esitöiden mukaan perustietovarantonimikkeen alle voidaan edellä mainittujen lisäksi nostaa myös kaupparekisteri, yhdistysrekisteri sekä säätiörekisteri (ks. HE 246/2010 vp, s. 30).

Tietosuoja-asetuksen (EU) 2016/679 4 (6) artiklassa määritellään rekisteriksi mikä tahansa jäsennelty, henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Asetuksessa *rekisterinpitäjällä* tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Tietovarantoja koskevassa sääntelyssä on tyypillistä, että tietovarannon yhteydessä kuvaillaan jokin siihen kuuluva osa tai sen muodostavat osat rekisteri-käsitteen avulla. Esimerkiksi yritys- ja yhteisötietolain (244/2001, YTJ-laki) 2 §:ssä määritellään yritys- ja yhteisötunnusrekisteri, joka on yritys- ja yhteisötietojärjestelmän tietoja sisältävä yleiseen käyttöön tarkoitettu rekisteri.

8.1.2 Tietovarannon ylläpitoon liittyvät vastuut

Tiedonhallintalain 5 §:n mukaan tiedonhallintayksiköiden on ylläpidettävä toiminta-ympäristönsä tiedonhallintaa kuvaavaa *tiedonhallintamallia*, jonka on sisällettävä muun muassa tiedot tietovarannoista ja niistä vastaavista viranomaisista. Tiedonhallintalain 28.1 §:n mukaan tiedonhallintayksikön on julkisuusperiaatteen toteuttamista varten ylläpidettävä kuvausta sen hallinnoimista tietovarannoista ja asiarekisteristä, jossa sen tulee esittää tiedot tietojen antamisesta päättävästä viranomaisesta. Tiedonhallintalaissa säädetään myös viranomaisen vastuusta suunnitella tietovarantojensa tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa (13.3 §). Tiedonhallintalain 20.1 §:ssä viitataan viranomaiselle muussa laissa säädettyyn oikeuteen saada tietoja toisen viranomaisen tietovarannosta. Lain 23.1 §:n mukaan viranomainen voi avata katseluyhteyden toiselle viranomaiselle tietovarantonsa tietoihin. Tietosuoja-asetuksen 30 (1) artiklassa säädetyssä tietojen käsittelytoimija kuvaavassa selosteessa rekisterinpitäjän tulee kuvata henkilötietojen käsittelyn käyttötarkoitukset ja käsittelyyn liittyvät vastuut. Julkisuuslain 13 ja 16 §:ssä tunnistetaan viranomaisen henkilörekisteriin liittyvänä vastuuna tietojenluovutus ao. rekisteristä ja 15 §:ssä yleiseen käyttöön tarkoitettu rekisteri, johon viranomaisella on vastuu tallentaa tietoja. Sääntelykohteesta ja siinä käytetystä sanamuodosta huolimatta, edellä yleislainsäädännössä esitetyt vastuut ja velvoitteet saattavat kohdistua käytännössä samaan tietovarantoon ja samoihin tietoaineistoihin.

Tietovarantoja koskevassa erityissääntelyssä tietovarannon ylläpidon osalta on erikseen eritelty vastuu

- rekisterinpidosta (esim. väestötietolaki (507/1993) 4 §, varhaiskasvatuslaki (540/2018) 67 §),
- tietojen ylläpidosta, ilmoittamisesta tai tallentamisesta (esim. laki valtakunnallisista opinto- ja tutkintorekistereistä (884/2017) 7–9 §, väestötietolaki 25–26 §),
- tietovarannon kehittämisestä (esim. laki kiinteistötietojärjestelmästä ja siitä tuotettavasta palvelusta (453/2002, KTJ-laki) 5 §, laki huoneistotietojärjestelmästä (1328/2018) 15 §) tai
- teknisestä ylläpidosta ja muusta tietovarannon teknisen toimivuuden varmistavasta vastuusta (esim. YTJ-laki 1 §, varhaiskasvatuslaki 67 §).

Rekisterinpitoa koskevan vastuu on määritelty selkeimmin, koska sen kohdalla viitataan tietosuoja-asetuksessa säädettyihin vastuisiin. Muilta osin säännöksissä käytettyjen sanamuotojen ja epäyhtenäisten määritelmien sekä niukkojen perusteluiden vuoksi yhdenmukainen ymmärrys vastuun sisällöstä jää muodostumatta.

8.2 Tietojen laatu

8.2.1 Tietojen laatu tiedonhallinnan yleissääntelyssä

Tiedonhallintalain 15.1 §:n 3 kohdassa edellytetään viranomaisia varmistamaan tietoturvallisuustoimenpitein tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys. Säännöksen kaikkia tietoaineistoja koskevan vaatimuksen on katsottu varmistavan viranomaistoiminnan asianmukaisuuden, sekä hallinnossa työskentelevien ja hallinnon asiakkaiden oikeusturvan.[89] Tiedonhallintalaissa ei kuitenkaan säännellä tarkemmin, mitä esitetyt virheettömyys- ja ajantasaisuusvaatimukset ovat. Laillisuusvalvonnassa on todettu itsestään selvänä lähtökohtana, että viranomaisen laatimien asiakirjojen ja ylläpitämien tiedostojen on oltava oikeita, virheettömiä ja ajantasaisia. Tämän on katsottu tarkoittavan myös sitä, että viranomaisten ylläpitämien tietojärjestelmien on oltava sellaisia, että niistä on tulostettavissa oikeaa tietoa ja tietojen keräämiseen tarkoitetun ohjelman tulee käsitellä järjestelmän sisältämiä tietoja siten, että tietojen keräämisen tuloksena syntyneet tiedot ovat oikeita.[90]

89 Ks. HE 284/2018 vp, s. 95.

90 AOKS OKV/1242/1/2013, 28.4.2014 sekä EOAK/5372/2019, 22.6.2020.

Tietosuoja-asetuksen 5 (1) artiklan d kohdan mukaan henkilötietojen käsittelyn periaatteena on vaatimus henkilötietojen täsmällisyydestä ja ajantasaisuudesta tarpeen mukaan. Tietojen käsittelyssä on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

Tiedon laatuvaatimuksista on kyse myös 5 (1) artiklan f kohdassa, jonka mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (”eheys ja luottamuksellisuus”). Tietosuoja-asetuksen 24 (1) artiklassa säädetään rekisterinpitäjän vastuusta toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Tietosuoja-asetuksessa tai tietosuojalaissa (1050/2018) ei säädetä tarkemmin, mitä tietojen täsmällisyydellä ja ajantasaisuudella tarkoitetaan missäkin yhteydessä.

Tiedonhallintalain ja tietosuoja-asetuksen tietojen laatua koskevat vaatimukset kytkeytyvät viranomaisen velvollisuuteen huolehtia asioiden *asianmukaisesta selvittämisestä* päätöksenteon yhteydessä. Hallintolain 31 §:ssä säädetään viranomaisen velvollisuudesta huolehtia asian asianmukaisesta ja riittävästä selvittämisestä hankkimalla asian ratkaisemiseksi tarpeelliset tiedot sekä selvitykset. Hallintolain esitöiden mukaan asian riittävällä selvittämisellä tarkoitetaan sitä, että viranomainen hankkii sellaiset tiedot ja selvitykset, joilla se arvioi olevan merkitystä asian ratkaisemiselle. Viranomaisen on tapauskohtaisesti arvioitava selvitysten laajuus ja tarve.[91]

Laillisuusvalvonnassa riittävän selvittämisen on katsottu tarkoittavan riittävää perehtymistä asiassa esitettyihin tosiseikkoihin. Selvityksen riittävyys ja sen oikea tulkitseminen ovat olennaisia edellytyksiä asian oikealle ratkaisemiselle ja perustelemiselle.[92] Selvittämisvelvollisuuden on katsottu korostuvan silloin, kun ratkaisulla on vaikutusta asiakkaiden etuihin ja oikeuksiin.[93] Oikeuskirjallisuudessa on katsottu, että hallintopäätöksen perusteena olevat virheelliset tai puutteelliset tiedot voivat aiheuttaa päätöksen pätemättömyyden. Kun hallintopäätös perustuu lain soveltamiseen yksittäisen tapauksen tosiasioihin, korostuu päätöksenteossa tosiasioita kuvaavien tietojen oikeellisuus.[94]

---

91 Ks. HE 72/2002 vp, s. 92–93.

92 AOKS OKV/2059/1/2013, 18.7.2014.

93 EOA EOAK/5974/2017, 10.10.2018.

94 Ks. esim. Mäenpää, Olli (2017): Yleinen hallinto-oikeus, s. 324 ja Kulla, Heikki (2018): Hallintomenettelyn perusteet, s. 227 ja 232.

Automatisoidun päätöksenteon näkökulmasta tietoaineistojen virheettömyyttä ja ajantasaisuutta voidaan lähestyä tietoja päätöksenteossa hyödyntävän viranomaisen sekä tietoja ylläpitävän ja niitä päätöstä tekevälle viranomaiselle luovuttavan viranomaisen näkökulmasta. Ensin mainitun tulee varmistaa, että sen päätöksenteossa käyttämät tiedot ovat riittävän oikein ja jälkimmäisen, että se luovuttaa tietojensaajalla oikeat ja ajantasaiset tiedot. Molemmissa tietojen virheettömyyttä ja ajantasaisuutta koskevat vaatimukset määräytyvät tietojen käyttötarkoituksen sekä käyttötilanteen kautta, eikä voimassa oleva tiedonhallintaa ja hallintomenettelyä koskeva yleislainsäädäntö esitä vastausta siihen, milloin päätöksenteossa käytettävien tietojen voidaan katsoa olevan riittävän oikein ja milloin viranomaisten päätöksenteossa käyttämään tietoon liittyvä selvittämisvelvollisuus voidaan katsoa toteutuneeksi.

8.2.2 Tiedon laatu perustietovarantoja koskevassa erityissääntelyssä

Tietojen laatua koskevaa sääntelyä voidaan analysoida myös tietovarantoja tai määriteltyjä tietoaineistoja koskevan sääntelyn kautta. Suomessa tietyt keskeiset yhteiseen käyttöön tarkoitetut tietovarannot lasketaan niin kutsuttujen perustietovarantojen tai perusrekisterien kategoriaan, joille tyypillisiksi ominaisuuksiksi on katsottu muun muassa tietojen kattavuus, luotettavuus, monikäyttöisyys, tietojen suojaus sekä tunnuseheys.[95] Rekistereihin talletetuille perusyksiköille on katsottu olevan yhteistä, että niillä on perusrekistereissä yhteiskäyttöinen yksilöivä tunnus (henkilötunnus, kiinteistötunnus, yritystunnus ym.), ajallinen ulottuvuus (syntymäajankohta, valmistumisvuosi ym.), ominaisuuspiirteitä (ikä, pinta-ala, liikevaihto ym.) ja paikantava tieto (osoite, koordinaattipiste ym.). Perusrekistereille ominaista on myös, että kukin niistä muodostaa yhtenäisen ja loogisen tietojärjestelmäkokonaisuuden, jonka tietosisältö koostuu useista eri tietolähteistä kerätyistä tiedoista. Perusrekistereiden sisältämiin tietoihin liitetään yleensä myös jonkin tasoinen *julkinen luotettavuus* tai muu vastaava laissa säädetty tietojen luotettavuutta korostava tai sen takaava seikka tai ominaisuus.[96] Juuri julkisesta luotettavuudesta johtuen perusrekisteritietojen perusteella tai niihin tukeutuen on katsottu voitavan tehdä muun muassa henkilön oikeuksia ja velvollisuuksia koskevia viranomaisratkaisuja. Tästä johtuen perusrekisterinpitäjää koskee muuta rekisterinpitoa ankarampi tosiasiallinen vastuu tiedoissa mahdollisesti olevien virheiden tai puutteiden vahingollisista tai haitallisista seurauksista.[97]

95 Ks. HE 89/2008 vp, s. 29.

96 Ks. HE 89/2008 vp, s. 4, 64–65.

97 Ks. HE 89/2008 vp, s. 30.

Perusrekistereitä koskevassa lainsäädännössä vain väestötietojärjestelmään tallennetut tietyt henkilötiedot on säädetty erikseen julkisesti luotettaviksi, eli tietoja voidaan pitää lähtökohteisesti luotettavina, jollei asiasta esitetä vastanäyttöä. Muiden väestötietojärjestelmään tallennettujen tietoja saa sääntelyn mukaan käyttää henkilöä koskevassa päätöksenteossa vain, jos hänelle annetaan päätöksenteon yhteydessä nimenomainen selvitys tietojen sisällöstä ja käytöstä (väestötietolaki 18 §). Kiinteistötietojärjestelmän lainhuuto- ja kiinnitysrekisteritiedot on katsottu myös julkisesti luotettaviksi, vaikka siitä ei erikseen maakaaressa (540/1995) säädetä.[98]

Muiden perustietovarantojen tietojen osalta tietojen laadun varmistava sääntely on yleensä muodostettu virheellisen tiedon käytöstä aiheutuvien vahinkojen korvausvelvollisuuksien (ks. KTJ-laki 8 §, YTJ-laki 17.1 §), rekisterimerkinnän oikeusvaikutuksen (ks. yhdistyslaki 6.1 § ja 52.2 §, osakeyhtiölaki 2:9 §)[99] tai merkinnän julkisuuden kautta (ks. kaupparekisterilaki 26.1 §).

8.2.3 Muu tietojen laatua varmistava sääntely

Tiedonhallintaa koskevan yleissääntelyn lisäksi tietovarantoja ja muuta tiedonhallintaa koskevasta erityissääntelystä on mahdollista tunnistaa myös muita sääntelytapoja, joilla tietojen laatua pyritään varmistamaan. Perusrekistereitä koskevaa sääntelyä vastaavasti tarkoitettuina varmistuskeinoina voidaan tunnistaa rekisterimerkinnän oikeusvaikutus sekä myös rekisterimerkintään liittyvät rikosoikeudelliset vaikutukset.

Tietovarantojen tietojen laatua varmistaa osaltaan rekisterimerkinnän muodostama oikeusvaikutus. Kun oikeudet muodostuvat vasta rekisterimerkinnän kautta, on myös oikeudensaajalla intressi huolehtia merkinnän olemassa olosta. Esimerkiksi yhdistys voi hankkia oikeuksia ja tehdä sitoumuksia sekä olla asianosaisena tuomioistuimessa ja muun viranomaisen luona vasta, kun se on rekisteröity (yhdistyslaki 6.1 §) ja yhdistyksen sääntöjen muutokset tulevat voimaan vasta, kun muutos merkitään rekisteriin (yhdistyslaki 52.2 §), ovat rekisteritiedot lähtökohtaisesti oikeellisia ja vastaavasti voidaan tietojen ilmoittajalla arvioida olevan intressi myös ylläpitää tietoja ajantasaisena.

98 Maakaaren esitöiden mukaan luotettavuutta osoittaa se, että rekisteriin merkitty lainhuuto riittää selvitykseksi omistusoikeudesta sekä uusia kirjaamishakemuksia tehtäessä että kiinteistöä myytäessä tai pantattaessa (Ks. HE 30/2009 vp, s. 5).

99 Esimerkiksi osakeyhtiö syntyy vasta, kun se rekisteröidään kaupparekisteriin (osakeyhtiölaki 624/2006 2:9 §). Yhdistys voi puolestaan hankkia oikeuksia ja tehdä sitoumuksia sekä olla asianosaisena tuomioistuimessa ja muun viranomaisen luona vasta, kun se on rekisteröity yhdistysrekisteriin (yhdistyslaki 6.1 §).

Toinen tapa varmistaa tietojen laatua koskee virheellisten tietojen käytöstä aiheutuvia oikeusvaikutuksia.[100] Kiinteistötietojärjestelmän tietojen osalta on säädetty kiinteistörekisterinpitäjän korvausvelvollisuudesta, jos rekisterimerkinnässä oleva virhe tai puute aiheuttaa vahinkoa tiedon käyttäjälle (KTJ-laki 8 §). Lain mukaan tietojen luovuttaja vastaa vahinkoa kärsineelle myös muun lain tai asetuksen mukaisessa tiedossa olevasta virheestä tai puutteesta aiheutuneesta vahingosta sen mukaan kuin vahingonkorvauslaissa (412/1974) säädetään. Kiinteistötietojärjestelmästä tietojen luovuttaja vastaa vahinkoa kärsineelle myös lainhuuto- ja kiinnitysrekisterin mukaisessa tiedossa olevasta virheestä tai puutteesta aiheutuneesta vahingosta (KTJ-laki 8.2 §). Jos kiinteistötietojärjestelmästä luovutetussa tiedossa oleva virhe tai puute on aiheutunut kiinteistötietojärjestelmään siirretyssä tiedossa olevasta virheestä tai puutteesta tai kiinteistötietojärjestelmään tietojen tallennusvelvollisuuden laiminlyömisestä, asianomainen julkisyhteisö on velvollinen korvaamaan tiedon luovuttajalle tämän suorittaman vahingonkorvauksen (KTJ-laki 8.4 §). Jos taas kiinteistötietojärjestelmään sisältyvän tiedon virheellisyys aiheutuu kiinteistötietojärjestelmän hallinnosta huolehtivan Maanmittauslaitoksen järjestelmän hallintoa, ylläpitoa, tietopalvelua ja järjestelmän kehittämistä koskevasta toiminnasta, Maanmittauslaitos vastaa tiedon luovuttajalle virheestä aiheutuneesta vahingosta (KTJ-laki 8.5 §).

Yritys- ja yhteisöjärjestelmään tallennettavien tietojen virheistä aiheutuvat oikeusvaikutukset määräytyvät järjestelmän kantarekistereitä koskevien säännösten mukaan (YTJ-laki 17.1 §). Koska yritys- ja yhteisötunnusrekisterin tiedoilla ei sellaisenaan ole välittömiä oikeusvaikutuksia, ei myöskään ole katsottu tarpeelliseksi järjestää erityistä muutoksenhakumenettelyä siinä mahdollisesti esiintyvien virheellisyyksien korjaamiseksi, vaan yleiset hallinnollisten oikaisu- ja muutoksenhakumenettelyjen on nähty olevan riittäviä tietojen poikkeamien oikaisemiseen.[101]

Rekisterimerkintärikos

Rikoslain 16 luvun 7 §:ssä säädetään rekisterimerkintärikoksesta. Rekisterimerkintärikoksessa on kyse siitä, että viranomaiselle annetaan väärä tieto, joka aiheuttaa oikeudellisesti merkityksellisen virheen kyseisen viranomaisen pitämään yleiseen rekisteriin. Lisäksi rekisterimerkintärikokseksi katsotaan se, että edellä kuvatulla tavalla aiheutettua virhettä käytetään hyväksi hankkimaan hyötyä tai aiheuttamaan vahinkoa. Virheellisen tiedon

100 Perusrekistereistä ainoastaan väestötietojärjestelmän osalta ei säädetä tietojen ilmoittamisen laiminlyönnistä tai virheellisistä tiedoista aiheutuvista sanktioista. Väestötietojärjestelmän tietojen osalta mahdollisen vahingonkorvauksen on katsottu voivan tulla kysymykseen vain vahingonkorvauslain (412/1974) mukaisena vastuuna eli tilanteissa, joissa ilmoittaja on tahallisesti tai tuottamuksellisesti laiminlyönyt hänelle kuuluvia velvollisuuksia ja aiheuttanut näin vahinkoa (ks. HE 89/2008 vp, s. 92).

101 Ks. HE 188/2000 vp, s. 21.

antamisen viranomaiselle säätämisellä rikoksi pyritään turvaamaan viranomaisten ylläpitämien tietoaineistojen ja rekistereiden laatua. Säännöksessä mainitun *yleisen rekisterin* yleisyyden arvioinnin kannalta keskeistä on se, millainen oikeudellinen merkitys rekisteritiedoilla on, ja onko rekisteri usean viranomaisen keskinäisessä käytössä, vai vain yhden viranomaisen sisäinen rekisteri. Myös väärän todistuksen antaminen viranomaiselle on säädetty rikokseksi (rikoslain 16 luvun 8 §). Väärän todistuksen antamisessa on kyse viranomaiselle annettavasta oikeudellisesti merkityksellisestä totuudenvastaisesta kirjallisesta todistuksesta tai siihen rinnastettavasta tallenteesta.

Sekä rikoslain 16 luvun 7 §:n että 8 §:n tunnusmerkistössä on olennaista *oikeudellinen merkityksellisyys*. Annetun väärän tiedon on oltava sellaista, että sillä on vaikutusta esimerkiksi viranomaisen tehtävän suorittamiseen tai viranomaisen päätöksentekoon. Merkittävää on myös se, että rekisterimerkintärikosta tai väärän todistuksen antamista viranomaiselle ei voi tehdä tuottamuksellisesti, vaan ainoastaan tahallisesti. Tiedon antajan on rekisterimerkintärikoksen tehdäkseen tiedettävä tai hänen pitää tietää, että väärä tieto on tarkoitettu kirjattavaksi yleiseen rekisteriin.

Tiettyjen tietovarantojen kohdalla väärien tietojen antaminen vahingon aiheuttamiseksi tai oikeudettoman hyödyn saamiseksi voi olla rangaistavaa myös muuna rikoksena kuin rekisterimerkintärikoksena ja väärän todistuksen antamisena, esimerkiksi veropetoksen (rikoslain 29 luvun 1 §) tai avustuspetoksen (rikoslain 29 luvun 5 §) kohdalla.

Rikosoikeudellisen seuraamuksen uhalla ei voida varmistua viranomaisten tietovarantojen tiedon laadusta ja luotettavuudesta, eikä tämä olisi tarkoituksenmukaistakaan. Rikosoikeudellinen seuraamus toimii lähinnä viimeisenä vaihtoehtona, jolla voidaan reagoida ilmeisiin väärinkäytöksiin.

8.3 Tietojen käyttö

8.3.1 Käsittelyn lainmukaisuus ja käyttötarkoitussidonnaisuus

Tietosuoja-asetus edellyttää, että henkilötietoja käsitellään asianmukaisesti ja lainmukaisesti tiettyä ja laillista tarkoitusta varten, ja että vain tätä tarkoitusta varten tarvittavia tietoja käsitellään. Henkilötietojen käsittely on asetuksessa määritelty laajasti tarkoittavan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Käsittely on tietosuoja-asetuksen 6 artiklan mukaisesti lainmukaista, jos se perustuu suostumukseen[102], sopimuksen täytäntöön panemiseen, rekisterinpitäjän lakisääteisen velvoitteen noudattamiseen, henkilön elintärkeiden etujen suojaamiseen, yleistä etua koskevan tehtävän suorittamiseen, rekisterinpitäjän julkisen vallan käyttämiseen, tai rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Tietosuojalain 4.1 §:n 2 kohdassa yleistä etua koskevan tehtävän suorittamista tai julkisen vallan käyttämistä tarkennetaan oikeudella käsitellä tietoja, jos käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi. Kansallisen säännöksen tarkoituksena on mahdollistaa viranomaisten toimesta tapahtuva henkilötietojen käsittely silloin, kun oikeutta käsittelyyn ei voida suoraan johtaa viranomaista koskevasta tehtävä- ja toimivaltasäännöksestä eikä mahdollisesta yksityiskohtaisemmasta erityissääntelystä.[103] Tietosuoja-asetus tai tietosuojalaki eivät tarkenna viranomaisten tehtävien kautta hyödynnettäviä tietoja tai hyödyntämiselle asetettavia vaatimuksia, muuten kuin käsittelyä koskevien yleisten periaatteiden kautta.[104]

Yhteisesti käytettäviä tietovarantoja koskevassa sääntelyssä tietovarannon käyttötarkoitukset perustuvat yleensä viranomaisten lakisääteisiin tehtäviin. Esimerkiksi yhteiskunnan toimintojen ja tietohuollon tukena toimiva väestötietojärjestelmä on tarkoitettu tuomioistuin- ja hallintomenettelyyn, viranomaisen suunnittelu- ja selvitystehtävään sekä muuhun näitä vastaavaan viranomaistehtävään (väestötietolaki 1 ja 29 §). Tulorekisterin käyttötarkoituksena on vastaanottaa ja tallettaa suorituksen maksajien ilmoittamia tulotietoja ja muita niihin liittyviä tietoja sekä välittää tiedot muun muassa verotusta varten sekä työntekijän eläkelaissa (395/2006) ja julkisen alojen eläkelaissa (81/2016), työtapaturma- ja ammattitautilaissa (873/2015) sekä liikennevakuutuslaissa (460/2016) säädettyjen tehtävien toimeenpanoa varten. Toinen tyypillinen sääntelytapa on määrittää tietovarannon tiedot yleiseen käyttöön (ks. KTJ-laki 6 §, YTJ-laki 16 §).

8.3.2 Päätöksenteossa käytettävien tietojen lähteet

Toisen viranomaisen tietoaineistojen hyödyntäminen

Tiedonhallintalain 20.1 §:n mukaan viranomaisen on pyrittävä hyödyntämään toisen viranomaisen tietoaineistoja, jos viranomaisella on oikeus saada tarvittavat tiedot toiselta viranomaiselta teknisen rajapinnan tai katseluyhteyden avulla. Säännöksen tarkoituksena on

102 Rekisterinpitäjänä toimivan viranomaisen osalta tietojen käsittelyn tulisi kuitenkin ensisijaisesti perustua muuhun kuin rekisteröidyn antamaa suostumukseen, esimerkiksi yleistä etua koskevan tehtävän suorittamiseen, julkisen vallan käyttämiseen tai lakisääteisen velvoitteen noudattamiseen (Tietosuoja-asetus 7 artikla ja resitaali 43).

103 Ks. HE 9/2018 vp, s. 79.

104 Ks. (EU) 2016/679 5 artikla.

vähentää viranomaisten rinnakkaista ja päällekkäistä tietojen keräämistä hallinnon asiakkailta sekä varmistaa, että viranomaiset käyttävät ajantasaisia tietoja niiden alkuperäisistä tietolähteistä. Viranomaisen on arvioitava toimintaprosessien suunnittelussaan, mistä jo olemassa olevista tietovarannoista sen tarvitsemat tiedot olisi mahdollista saada ajantasaisina tiedonsaantioikeuksien ja tietojen käsittelyoikeuksien puitteissa ilman, että tietoja tarvitsisi erikseen pyytää asianosaiselta tai muulta hallinnon asiakkaalta.[105] Tiedonhallintalaissa ei kuitenkaan säädetä viranomaisten tiedonsaantioikeuksista tai määritellä, mitä tietojen hyödyntämisellä eri tehtävissä tarkoitetaan.

Tiedonhallintalain 20.1 §:n jälkimmäisessä virkkeessä säädetään viranomaisen velvoitteesta huolehtia asianosaisen tai muun hallinnon asiakkaan oikeusturvasta, kun se hyödyntää toisen viranomaisen tietoaineistoa. Säännöksellä on tarkoitus varmistaa, ettei viranomainen voi tehdä hallinnon asiakasta koskevia välittömän oikeusvaikutuksen aiheuttavia päätöksiä pelkästään kerättyjen tietojen perusteella, vaan hallinnon asiakasta pitäisi muun muassa kuulla ennen päätöksentekoa tai järjestää asiankäsittely tai palvelujen tuottaminen siten, että asianosainen tai asiakas voi jo asiankäsittelyn tai palvelun tuottamisen aikana varmistaa viranomaisella olevien tietojen oikeellisuuden.[106] Tiedonhallintalain velvoite edellyttää automaattisen päätöksenteon yhteydessä viranomaista muodostamaan menettelyn, jonka avulla asianosaisen on mahdollista tarkistaa päätöksenteon perusteena käytettävien tietojen oikeellisuus ennen päätöksentekoa. Tämän kaltaisesta menettelystä käytännön esimerkkinä voidaan käyttää verotuksen suorittamiseen liittyvää, verovelvollisen tarkistettavaksi tulevaa esitäytettyä veroilmoitusta. Voimassa olevassa lainsäädännössä tämänkaltaisesta menettelystä ei kuitenkaan ole säädetty.

Tiedon hyödyntäminen muuhun kuin sen alkuperäiseen käyttötarkoitukseen

Oman erityispiirteensä muodostavat ne päätöksenteossa käytettävät tiedot, jotka on alun perin kerätty muuhun käyttötarkoitukseen. Tietosuoja-asetuksen 6 (4) artiklan mukaan, jos tietoja käsitellään muuhun kuin alkuperäiseen käyttötarkoitukseen, on rekisteripitäjän otettava huomioon tietojen käsittelyn lainmukaisuuden varmistamiseksi alkuperäisen tietojen keruun ja tarkoitusten ja aiotun myöhemmän käsittelyn tarkoitusten väliset yhteydet, henkilötietojen keruun asiayhteys erityisesti rekisteröityjen ja rekisterinpitäjän välisen suhteen osalta, henkilötietojen luonne (erityisesti erityisten henkilötietoryhmien ja rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot), aiotun myöhemmän käsittelyn mahdolliset seuraukset rekisteröidyille sekä asianmukaisten suojatoimien, kuten salaamisen tai pseudonymisoinnin, olemassaolo.

105 Ks. HE 284/2019 vp, s. 100–101.

106 Ks. HE 284/2019 vp, s. 101.

Tietosuoja-asetuksessa ei säännellä tarkemmin, mitä nämä varmistustoimenpiteet tarkoittaisivat viranomaisten päätöksenteon tai päätöksenteossa käytettävien tietojen osalta. Asetuksen johdanto-osan kappale 42 tarkentaa säännöksen tavoitetta vain niiltä osin, että tilanteissa, joissa muuhun käyttötarkoitukseen kerätty tieto perustuu rekisteröidyn suostumukseen ja jos suostumus annetaan muuta seikkaa koskevan kirjallisen ilmoituksen yhteydessä, olisi varmistettava suojatoimin, että rekisteröity on tietoinen antamastaan suostumuksesta ja siitä, kuinka pitkälle menevästä suostumuksesta on kyse.[107]

Tietojen toissijaista käyttöä koskevassa kansallisessa lainsäädännössäkään ei ole säännöksiä, jotka koskisivat tietojen käyttöä päätöksenteon yhteydessä.[108]

Viranomaisten käyttöön tarkoitettujen ulkoisten tietovarantojen hyödyntäminen

Päätöksenteossa käytettävien tietojen arvioinnin osalta on syytä ottaa huomioon myös käytännön menettelyt, joilla tietoja ylläpidetään. Erityisesti tilanteissa, joissa käytettävät tiedot perustuvat muilta viranomaisilta saataviin tietoihin, eikä niitä tarkisteta asiakkaalta asiointitilanteissa, korostuvat tietojen ylläpidossa noudatettavien käytäntöjen vaikutukset muun muassa tietojen ajantasaisuuteen. Kun suuri osa viranomaisten päätöksenteossa käyttämästä tiedosta tukeutuu viranomaisen asian käsittelyssä käyttämien tietojärjestelmien tietokantoihin, joiden sisältöä ylläpidetään myös ulkoisista tietolähteistä, vaikuttavat käsiteltävien tietojen laatuun ja ajantasaisuuteen tavat, joilla tiedot viranomaisen omaan tietovarantoon päivitetään.

Suomessa on perinteisesti koottu yhteiskunnan toiminnassa tarvittavat tiedot kansalaisilta, eri viranomaisilta sekä yrityksiltä ja yhteisöiltä kansallisiin tietovarantoihin, joista tiedot ovat niitä tarvitsevien käytettävissä laadukkaasti ja kustannustehokkaasti. Vaihtoehtona olisi, että viranomaiset keräisivät toiminnassaan ja päätöksenteossaan tarvitsemansa tiedot alusta alkaen itse ja joka kerralla erikseen.

Esimerkkejä tällaisista tietovarannoista ovat jo edellä mainitut perustietovarannot, joiden sisältämiin tietotoihin on liitetty jonkin tasoinen julkinen luotettavuus tai muu vastaava laissa säädetty tietojen luotettavuutta korostava tai sen takaava seikka tai ominaisuus, jonka vuoksi tietoja hyödynnetään laajalti eritasoisessa päätöksenteossa.[109] Esimerkiksi kun henkilön perustietoja, kotipaikka- ja osoitetietoja sekä henkilösuhdetietoja hyödynnetään niiden kansallisesta primäärilähteestä, välitetään väestötietojärjestelmästä tiedot niitä käyttäville viranomaisille joko määräajoin päivitysaineistoina odottamaan tietojen

107 Ks. tietosuoja-asetuksen resitaali 42.

108 Ks. esim. laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019).

109 Ks. HE 89/2008 vp, s. 4, 64–65.

myöhempää käyttöä tai suoralla teknisellä rajapinnalla tai katseluyhteydellä. Kun väestötietojärjestelmästä saatetaan toimittaa tiedot vaikkapa vain joka toinen viikko ja rekisterimerkintä on tehty tietojen toimitusajankohtaa aikaisemmin, ja koska viranomaiselta kuluu vielä oma aikansa tietojensa päivittämiseen, päätöksenteossa käytettävät tiedot voivat olla jo lähtökohtaisesti vanhentuneita. Tietojen jatkuva ylläpito riippumatta niiden käyttötarpeesta taas olisi ongelmallista yleisen tietosuoja-asetuksen tietojen käsittelyn tarkoitussidonnaisuuden periaatteen kannalta.

8.3.3 Tietojen luovuttaminen

Tietojen saantioikeudet ja -luovutusvelvoitteet

Automatisoidun päätöksenteon yhteydessä käytettävien tietojen osalta nousee yhdeksi näkökulmaksi päätöksen tekevän viranomaisen tietojensaannin osalta tietojensaajalle säädetyt velvoitteet varmistaa vastaanottamansa tietojen laatu sekä tiedot luovuttavalle viranomaiselle säädetyt velvoitteet luovuttaa virheetöntä ja ajantasaista tietoa.

Julkisuuslaissa säädetään yleisellä tasolla tietojensaamisesta viranomaisten asiakirjoista. Julkisuuslain 9 §:ssä vahvistetaan julkisuusperiaatteen mukainen säännös myös viranomaisten osalta saada tieto toiselta viranomaiselta julkisesta asiakirjasta. Julkisen asiakirjan osalta viranomaisella ei ole harkintavaltaa sen suhteen, antaako se tiedon julkisen asiakirjan sisällöstä, vaan tieto on pyydettäessä aina annettava.[110] Julkisuuslain 10 §:n mukaan salassa pidettävästä viranomaisen asiakirjasta tai sen sisällöstä saa antaa tiedon vain, jos niin on erikseen julkisuuslaissa säädetty. Viranomaisen tietojensaantioikeus määräytyy pääasiassa erityislainsäädännön mukaisesti.[111] Julkisuuslain 28 §:ssä säännöksen perusteella viranomainen voi antaa myös luvan toiselle viranomaiselle saada salassa pidettäviä tietoja tieteellistä tutkimusta, tilastointia taikka viranomaisen suunnittelu- tai selvitystyötä varten, jos on ilmeistä, ettei tiedon antaminen loukkaa niitä etuja, joiden suojaksi salassapitovelvollisuus on säädetty.[112]

Julkisuuslain 29 §:ssä säädetään viranomaisten oikeudesta antaa salassa pidettäviä tietoja toiselle viranomaiselle, jos tiedon antamisesta tai oikeudesta tiedon saamiseen on laissa erikseen nimenomaisesti säädetty tai se, jonka etujen suojaamiseksi salassapitovelvollisuus on säädetty, antaa siihen suostumuksensa. Lisäksi tiedot voidaan antaa, jos asiakirja on tarpeen muun muassa muutoksenhaun tai kantelun käsittelemiseksi, tai tieto on tarpeen viranomaiseen kohdistuvan yksittäisen valvonta- tai tarkastustehtävän

110 Ks. HE 30/1998 vp, s. 64.
111 Ks. HE 30/1998 vp, s. 101.
112 Ks. HE 30/1998 vp, s. 105.

suorittamiseksi. Julkisuuslain 26.2 §:n mukaan viranomainen voi salassapitosäännösten estämättä antaa tiedon muun muassa toisen taloudellisesta asemasta taikka liikesalaisuudesta, terveydenhuollon tai sosiaalihuollon asiakassuhteesta tai myönnetystä etuudesta, jos tieto on tarpeen yksityisen tai toisen viranomaisen laissa säädetyn tiedonantovelvollisuuden toteuttamiseksi tai tiedot antavan viranomaisen hoidettavaksi kuuluvan korvauksen tai muun vaatimuksen toteuttamiseksi. Edelleen julkisuuslain 27.1 §:ssä säädetään viranomaisen mahdollisuudesta antaa tietoja arkistoon siirretystä, salassa pidettäväksi säädetystä viranomaisen asiakirjasta tutkimusta tai muuta hyväksyttävää tarkoitusta varten, jollei asiakirjan siirtänyt viranomainen ole toisin määrännyt.

Yleisellä tietosuoja-asetuksella vahvistetaan säännöt luonnollisten henkilöiden suojelulle henkilötietojen käsittelyssä sekä säännöt, jotka koskevat henkilötietojen vapaata liikkuvuutta. Tietosuoja-asetuksen 6 artiklassa säädetään henkilötietojen käsittelyn, ml. tietojen luovuttaminen[113], lainmukaisuusvaatimuksista, joita ovat muun muassa rekisteröidyn suostumukseen perustuva tai rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi tarpeellinen tietojen käsittely. Tietosuojalain 28 §:n mukaan oikeuteen saada tieto ja muuhun henkilötietojen luovuttamiseen viranomaisen henkilörekisteristä sovelletaan, mitä viranomaisten toiminnan julkisuudesta säädetään.

Tiedonhallintalain 15.1 §:ssä säädetään viranomaisen velvoitteesta varmistaa tarpeellisin tietoturvallisuustoimenpitein, että sen tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu. Tiedonhallintalain säännös edellyttää, että molempien, tietoja luovuttavan ja tietojen saajan tulisi pystyä varmistamaan osaltaan, että tiedot ovat saatavilla käyttökelpoisessa muodossa. Laissa ei kuitenkaan tarkemmin määritellä, mitä tällä tarkoitetaan eri yhteyksissä tai millä kriteereillä vaatimuksen toteutumista olisi mahdollista arvioida.

Tietojen luovuttamista koskevassa yleissääntelyssä ei ole erillisiä säännöksiä, joissa luovutettaville tiedoille asetetaan selkeitä laatu- tai ajantasaisuusvaatimuksia. Vaatimukset luovutettaville tiedoille onkin johdettava joko tietoja ylläpitävän viranomaisen omaa tietoaineistojen hallintaa ja käsittelyä koskevista vaatimuksista (ks. edellä tietojen laatu ja tietojen hyödyntäminen) tai asiaa koskevasta erityissääntelystä.

113 Yleisessä tietosuoja-asetuksessa henkilötietojen käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista (Ks. Euroopan unionin virallinen lehti EUVL 4.5.2016, L 119/33).

Perustietovarantoja koskevassa sääntelyssä väestötietojärjestelmän tietojen osalta on säädetty erikseen tietojen ilmoittajan velvollisuudesta vastata rekisterinpitäjälle ilmoittamiensa tietojen luotettavuudesta ja niiden pysymisestä ajan tasalla (väestötietolaki 27 §). Kiinteistötietojärjestelmälain 4 §:n mukaan viranomaisella, jonka vastuulla on kiinteistötietojärjestelmän tietosisältöön kuuluvan tiedon tuottaminen, on myös velvollisuus huolehtia tällaisen tiedon tallentamisesta kiinteistötietojärjestelmään ja sen pitämisestä ajan tasalla. Yritys- ja yhteisötunnusrekisteriin tehtävien merkintöjen oikeellisuudesta vastaa se viranomainen, jonka kantarekisteriin kyseinen tieto on tallennettu tai joka tekee merkinnän yritys- ja yhteisötietojärjestelmään (YTJ-laki 17.1 §). Perustietovarannon ylläpidosta ja rekisterinpidosta vastaava viranomainen huolehtii pääosin vain tietovarannon teknisestä ylläpidosta sekä tietovarantoon toimitettavien tietojen eheydestä. Perustietovarantoja koskevaa sääntelyä vastaavaa sääntelytapaa, jossa vastuu tietojen laadusta on eriytetty yhteisen tietovarannon ylläpitoa koskevista vastuista, sisältyy myös esimerkiksi varhaiskasvatuksen valtakunnallista tietovarantoa[114], opetuksen ja koulutuksen valtakunnallista tietovarantoa[115] sekä tulotietojärjestelmää[116] koskevaan sääntelyyn.

Tietojen luovutustapa

Automaattisen päätöksenteon näkökulmasta yhdeksi tarkastelukohteeksi nousee tietojen sähköistä luovuttamistapaa koskeva sääntely. Julkisuuslain 16.2 §:ssä säädetään viranomaisen velvoitteesta antaa sen ratkaisurekisterin julkisista tiedoista kopio teknisenä tallenteena tai muutoin sähköisessä muodossa. Tietojen antaminen vastaavassa muodossa

114 Varhaiskasvatuksen valtakunnallisen tietovarannon osalta kunta, kuntayhtymä tai yksityinen palvelujentuottaja vastaa tietovarantoon tallentamiensa tietojen osalta niiden sisällöstä ja virheettömyydestä. Lisäksi niiden on huolehdittava myös tietojen ajantasaisuudesta. Opetushallitus vastaa tietovarannon yleisestä toiminnasta sekä ohjelmointirajapinnoista tietojen tallentamista, käsittelyä ja luovutusta varten sekä tietovarannon käytettävyydestä, eheydestä ja muuttumattomuudesta sekä suojaamisesta ja säilyttämisestä (varhaiskasvatuslaki 540/2018 67.1 §).

115 Opetuksen ja koulutuksen valtakunnallisen tietovarannon osalta opetuksen ja koulutuksen järjestäjät sekä oppilaitosten ylläpitäjät vastaavat tallentamiensa tietojen täsmällisyydestä yleisen tietosuoja-asetuksen vaatimusten mukaisesti ja Opetushallitus muista yleisessä tietosuoja-asetuksessa rekisterinpitäjälle säädetyistä velvollisuuksista sekä tietovarannon yleisestä toiminnasta sekä teknisestä käyttöyhteydestä tietojen tallentamista, käsittelyä ja luovutusta varten (Laki valtakunnallisista opinto- ja tutkintorekistereistä 884/2017 5 §).

116 Tulotietojärjestelmän osalta suorituksen maksajat vastaavat tulorekisteriin talletettavaksi antamiensa tietojen oikeellisuudesta sekä tietojen oikaisemisesta ilman aiheetonta viivytystä (Laki tulotietojärjestelmästä 53/2018 4.3 §) ja tietojärjestelmän rekisterinpitäjän toimiva Verohallinnon tulorekisteriyksikkö vain välittää ja luovuttaa tiedot tiedon käyttäjälle sellaisina kuin ne suorituksen maksajan antaman tietojen perusteella tulorekisteriin talletettu (Laki tulotieto-järjestelmästä 53/2018 14.1 §).

muusta julkisesta asiakirjasta on viranomaisen harkinnassa[117]. Pykälän 3 momentin mukaan viranomaisen henkilörekisteristä saa antaa henkilötietoja sisältävän kopion tai tulosteen tai sen tiedot sähköisessä muodossa, jollei laissa ole toisin erikseen säädetty, jos luovutuksensaajalla on henkilötietojen suojaa koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia henkilötietoja.

Tiedonhallintalain 22.1 §:n mukaan viranomaisten on toteutettava säännöllisesti toistuva ja vakiosisältöinen sähköinen tietojen luovuttaminen tietojärjestelmien välillä teknisten rajapintojen avulla, jos vastaanottavalla viranomaisella on tietoihin laissa säädetty tiedonsaantioikeus. Säännös koskee tilanteita, jolloin viranomainen luovuttaa toiselle viranomaiselle säännöllisesti tietovarannostaan tietoja toisen viranomaisen tietotarpeita varten. Säännös muodostaa sekä tiedot luovuttavalle että tiedot saavalle viranomaiselle velvollisuuden huolehtia siitä, että niiden tietojärjestelmien välinen tietoliikenne hoidetaan yhteentoimivien teknisten rajapintojen avulla.[118]

Rajapintojen avulla tapahtuvaan tietojenluovuttamiseen liittyy myös viranomaisille säädetty velvoite toteuttaa tietojen luovuttaminen teknisten rajapintojen avulla siten, että myös teknisesti varmistetaan luovutettavien tietojen tapauskohtainen tarpeellisuus tai välttämättömyys tietoja saavan viranomaisen tehtävien hoitamiseksi, jos luovutettavat tiedot ovat henkilötietoja tai salassa pidettäviä tietoja (tiedonhallintalain 22.2 §). Automatisoidun tietojenvaihdon osalta vaatimus tarkoittaa menettelyn luomista sille, miten tietoja pyytävän rajapinnan ja tietoja luovuttavan rajapinnan käyttöönoton yhteydessä myös luovutuksen oikeudelliset edellytykset tulevat varmistetuiksi, jottei tietojenluovutuksen yhteydessä ole tarvetta käyttää tapauskohtaista harkintaa.

Tietojenluovutustapaa koskevassa yleissääntelyssä ei aseteta erikseen tai tarkemmin vaatimuksia päätöksenteossa käyttävien tietojen luovutukselle. Julkisen hallinnon yhteisiä tietovarantoja koskien on muodostunut tietovarantokohtaista erityissääntelyä, joka tarkentaa tietojenluovutustapavaihtoehtoja suhteessa viranomaisten tehtävissä tarvitsemaan

117 Tähän on avoimen datan direktiivin (EU) 2019/1024 täytäntöönpanon johdosta tulossa muutos ns. tiheästi tai reaaliaikaisesti päivittyvien tietojen sekä eräiden ns. arvokkaiden tietoaineistojen osalta, ks. HE 74/2021 vp ja EV 107/2021 vp.

118 Ks. HE 284/2018 vp, s. 106.

tietoon. Tietovarantokohtainen sääntely ei muodosta luovutustapaa koskevien vaatimusten osalta mitään yhdenmukaista kokonaisuutta, vaan sääntelyn tavat ja tarkkuustasot vaihtelevat tietovarannon ja toimialan mukaan.[119]

Muut tietojen luovuttamiseen liittyvät menettelyt

Tietojenluovutustavan lisäksi automatisoidussa päätöksenteossa tarvittavien tietojen hyödyntämiseen vaikuttavat omalta osaltaan myös muut tietojen luovuttamiseen liittyvät menettelyt. Näitä ovat muun muassa tietoa luovuttaville viranomaisille säädetyt menettelyt, joilla tietojen luovuttamiseen liittyvien edellytysten olemassaolo pyritään selvittämään, sekä osaltaan myös luovutettavista tiedoista perittävät maksut. Tilanteissa, joissa automatisoidun päätöksenteon edellytyksenä on muilta viranomaisilta saatavat tiedot ja tietojenluovutus toteutetaan tietojärjestelmien välillä pitkälti automatisoituna, korostuvat luovutusmenettelyä koskevat säännökset erityisesti, jos tietoja tarvitaan useilta viranomaisilta ja useista tietovarannoista.

Julkisuuslain 14.1 §;n mukaan viranomaisen asiakirjan antamisesta päättää se viranomainen, jonka hallussa asiakirja on. Salassa pidettävien asiakirjojen osalta julkisuuslain 28 §:ssä säädetään viranomaisen mahdollisuudesta antaa yksittäistapauksessa lupa tietojen saamiseen salassa pidettävästä asiakirjastaan tieteellistä tutkimusta, tilastointia taikka viranomaisen suunnittelu- tai selvitystyötä varten, jos on ilmeistä, ettei tiedon antaminen loukkaa niitä etuja, joiden suojaksi salassapitovelvollisuus on säädetty.

Yleislainsäädännön lisäksi tietojenluovutuksen luvanvaraisuutta koskevia säännöksiä sisältyy perustietovarantojen sääntelyyn sekä muita yhteiseen käyttöön tarkoitettuja tietovarantoja koskevaan sääntelyyn. Väestötietojärjestelmästä luovutettavien tietojen osalta Digi- ja väestötietovirasto tekee tietojen tarvitsijan kirjallisesta hakemuksesta päätöksen tiedonluovuttamisesta (väestötietolaki 50 §). Kiinteistötietojärjestelmän tietojen luovuttamiseen teknisellä käyttöyhteydellä myöntää luvan Maanmittauslaitos (KTJ-laki 6.3 §), joka myöntää myös määräaikaisen luvan huoneistotietojärjestelmän tietojen luovuttamiseen (laki huoneistotietojärjestelmästä 20 §).

119 Esimerkiksi Maanmittauslaitokselle on säädetty mahdollisuus luovuttaa kiinteistötietojärjestelmän tietoja teknisellä käyttöyhteydellä muun muassa oikeushallinnon viranomaiselle, aluehallintovirastolle, elinkeino-, liikenne- ja ympäristökeskukselle, kunnalle, Verohallinnolle, puolustusministeriölle, Puolustusvoimille, Rajavartiolaitokselle, poliisille ja muulle esitutkintaviranomaiselle, pelastusviranomaiselle, kiinteistönmuodostamistehtäviä hoitavalle viranomaiselle, väestökirjahallinnon viranomaiselle (KTJ-laki 6.3 §). Maanmittauslaitoksella on oikeus luovuttaa myös huoneistotietojärjestelmän tietoja sähköisessä muodossa, jos luovutuksen saajalle ja välittäjänä toimivalle myönnetään käyttölupa (laki huoneistotietojärjestelmästä 20.1 §).

Oman erityispiirteensä viranomaisten tietojenluovutuksiin muodostavat luovuttavalle viranomaiselle erikseen säädetyt oikeudet tarkistaa tietojensaajan tiedonhallinnassa ja tietojen käsittelyssä käyttämät käytännöt. Väestötietolain 44 §:ssä säädetään Digi- ja väestötietoviraston oikeudesta saada tarvittaessa tiedon käyttäjältä selvitys siitä, kuinka luovutettujen tietojen käyttö ja suojaus on tarkoitus järjestää. Selvitys on annettava kirjallisesti ja siinä on ilmoitettava, kuinka luovutettavien tietojen hallinnollinen ja fyysinen turvallisuus sekä henkilöstö-, tietoliikenne-, ohjelmisto-, tietoaineisto-, käyttö- ja laitteistoturvallisuus on tarkoitus varmistaa. Pykälän 2 momentin mukaan selvitys on vaadittava, jos tiedot luovutetaan teknisen rajapinnan avulla.

Erityisesti ulkoisten tietovarantojen hyödyntämisessä tietojen käyttöön vaikuttavat tietojen käytöstä perittävät maksut. Maksujen vaikutukset tietojen hyödyntämiseen ovat viime vuosina vähentyneet, kun viranomaistehtäviä varten tarkoitettujen tietovarantojen käytöstä perittäviä maksuja on vähennetty. Päätöksenteossa käytettävien tietojen maksullisuus ja useat erilaiset maksun muodostumis- ja laskutuskäytännöt saattavat estää tietojen tehokasta hyödyntämistä ja heikentää käytetyn tiedon laatua.

Viranomaisten asiakirjojen antamisen maksuttomuudesta tai maksun määräytymisen perusteista säädetään yleisesti julkisuuslain 34 §:ssä. Säännöksen mukaan julkisesta asiakirjasta ei peritä maksua muun muassa, kun sähköisesti talletettu asiakirja toimitetaan pyytäjälle tai asianosaiselle sähköpostilla.[120] Jos sähköisesti tallennetut tiedot annetaan teknisen käyttöyhteyden avulla, luovutukseen sovelletaan valtion viranomaisten osalta valtion maksuperustelakia (150/1992) ja kunnallisten viranomaisten osalta kuntalakia (410/2015). Viranomaisten välillä luovutettaviin salassa pidettäviin tietoihin julkisuuslain 34 §:ää ei kuitenkaan sovelleta.

Valtion maksuperustelakia (150/1992, maksuperustelaki) sovelletaan silloin, kun alakohtaisesti ei ole olemassa tarkempaa maksuja koskevaa sääntelyä (2.1 §). Maksuperustelain lähtökohta on suoritteiden maksullisuus. Jos suorite katsotaan sellaiseksi, jonka kysyntä perustuu lakiin tai asetukseen ja jonka tuottamiseen viranomaisella on tosiasiallinen yksinoikeus (*julkisoikeudellinen suorite*), tulee suoritteesta perittävän maksun vastata suoritteen tuottamisesta aiheutuvia kustannuksia (3 ja 6 §). Muista kuin julkisoikeudellisista suoritteista voidaan 7 §:n mukaan periä maksu liiketaloudellisin perustein. Useiden tietovarantojen osalta tulee kuitenkin sovellettavaksi tietovarannon erityissääntely. Esimerkiksi väestötietojärjestelmän tietojenluovutuksien hinnoittelun perusteita

120 Avoimen datan direktiivin (EU) 2019/1024 täytäntöönpanoa koskevassa hallituksen esityksessä (HE 74/2021 vp) on ehdotettu muutettavan julkisuuslain 34 §:ää siltä osin, että komission täytäntöönpanosäädöksillä määrittelemät arvokkaat tietoaineistot olisivat saatavilla maksutta.

täsmennetään väestötietolain 72 §:ssä. Yritys- ja yhteisötietojärjestelmän hinnoittelun perusteita täsmennetään Patentti- ja rekisterihallituksen suoritteista annetun lain (1032/1992) 5.2 §:ssä.

Maksuperustelain 8 §:n mukaan asianomainen ministeriö päättää, mitkä ministeriön ja hallinnonalan muiden viranomaisten suoritteet tai suoriteryhmät ovat maksullisia ja mistä suoritteesta tai suoriteryhmästä maksu määrätään omakustannusarvon perusteella sekä mitkä suoritteet hinnoitellaan liiketaloudellisin perustein. Ministeriön päätöksen mukaisesti tietovarantojen suoritteista perittävistä maksuista on annettu ministeriön asetus.[121]

Kunnallisten viranomaisten osalta kuntalain (410/2015) 14 §:n mukaan kunnanvaltuusto päättää palveluista ja muista suoritteista perittävien maksujen yleisistä perusteista. Kuntien ylläpitämien tietovarantojen osalta mahdollisesta maksullisuudesta tai maksuttomuudesta on säädetty tarkemmin erityislainsäädännössä, jonka nojalla tietovarantoja ylläpidetään.

8.3.4 Tietojen saatavuus ja käytettävyys

Automatisoidussa päätöksenteossa käytettävään tietoon liittyy olennaisesti myös tietojen saatavuus ja käytettävyys päätöksenteon yhteydessä. Onkin arvioitava, miten voimassa olevassa sääntelyssä on säädetty tietovarantojen saatavuuden tai käytettävyyden vaatimuksista. Vaatimuksia korostavat laillisuusvalvonnassa esitetyt huomiot perusoikeuksien mukaisesta palvelujen turvaamisesta myös tietojärjestelmien ongelmatilanteissa. Viranomaisen ei ole katsottu voivan perustella poikkeamista hyvän hallinnon vaatimuksista tietojärjestelmien toimimattomuuteen liittyvillä syillä. Jos toimimattomuuden syynä ovat olleet tietojärjestelmän käsittelemät tiedot, korostuu viranomaisen vastuu varmistaa myös päätöksenteossa tarvittavien tietojen käytettävyys.[122]

Valmiuslain (1552/2011) 12 §:n mukaan viranomaisten tulee varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa. Varautumisvelvoitteen on katsottu koskevan myös muita, poikkeusoloja lievempiä häiriötilanteita.[123]

121 Esim. valtiovarainministeriön asetus Digi- ja väestötietoviraston suoritteiden maksuista vuonna 2021 (969/2020).

122 Ks. esim. EOA 206/4/11 (31.5.2012), AOA 1301/2017 (18.4.2017), AOA 649/2017 (20.3.2017), AOA 3591/4/09 (21.6.2010), AOA 33/2/06 ja 34/2/06 (31.5.2006)

123 Ks. HE 3/2008 vp, s. 37.

Tiedonhallintalain 13.2 §:ssä säädetään viranomaisen velvoitteesta varmistaa tehtäviensä hoitamisen kannalta olennaisten tietojärjestelmien *vikasietoisuus* ja *toiminnallinen käytettävyys* riittävällä säännöllisellä testauksella. Yleisen tietosuoja-asetuksen henkilötietojen käsittelyn turvallisuutta koskevissa säännöksissä rekisterinpitäjän vastuulle on säädetty velvoite toteuttaa tarvittavat toimenpiteet, joilla taataan tietojen käytettävyys sekä kyetä palauttamaan nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa (32 (1) artikla b ja c kohdat).

Mikäli viranomaisen päätöksenteossa tarvitsemien tietojen saaminen on kiinni asiakkaiden toimittamista tai ilmoittamista tiedoista, tulee viranomaisen tarjota jokaiselle mahdollisuus toimittaa asiointitarpeeseensa liittyvät sähköiset viestit ja asiakirjat käyttäen digitaalisia palveluita tai muita sähköisiä tiedonsiirtomenetelmiä (Laki digitaalisten palvelujen tarjoamisesta 306/2019 5.1 §, digipalvelulaki). Lisäksi viranomaisen on huolehdittava sen vastuulla olevien digitaalisten palvelujen ja muiden viranomaisen käytössä olevien sähköisten tiedonsiirtomenetelmien saatavuudesta muulloinkin kuin viranomaisen asiointipisteiden aukioloaikoina sekä ajoitettava palvelujen käyttökatkot ajankohtaan, jolloin niiden käyttö on vähäistä. Käyttökatkoista on tiedotettava sopivalla tavalla ennalta (digipalvelulaki 4.2 §). Säännöksen tarkoituksena on korostaa viranomaisten varautumisvelvollisuutta digitaalisten palvelujen ja muiden sähköisten tiedonsiirtomenetelmien ennalta suunniteltuihin käyttökatkoihin.[124]

Perusrekisterejä koskevassa sääntelyssä tietovarantojen tietojen saatavuudesta tai käytettävyydestä on vain vähän sääntelyä ja sekin kohdentuu pääosin vain vastuullisen viranomaisen määrittämiseen. Samantapaisesti on säädetty myös muista toimialojen yhteisiä tietovarantoja koskevista ylläpito- ja käytettävyysvaatimuksista. Esimerkiksi varhaiskasvatuksen valtakunnallisen tietovarannon osalta Opetushallituksen tehtäväksi on säädetty vastuu tietovarannon yleisestä toiminnasta sekä tietovarannon käytettävyydestä (varhaiskasvatuslaki (540/2018) 67.2 §). Tulotietojärjestelmän osalta Verohallinnon Tulorekisteriyksikön ja Verohallinnon vastuulle on säädetty tulotietojärjestelmän ylläpito sekä vastuu tulotietojärjestelmän toimivuudesta ja tietoturvallisuudesta (Laki tulotietojärjestelmästä (53/2018) 4.2 §). Kuitenkaan mainituissa laeissa tai niiden esitöissä ei tarkenneta, mitä tietovarannon ylläpidolla, yleisellä toiminnalla, käytettävyydellä tai toimivuudella tarkoitetaan.[125]

124 Ks. HE 60/2018 vp, s. 65.

125 Ks. HE 40/2018 vp., HE 134/2017 vp, s. 77., Ks. HE 127/2018 vp, s. 59.

8.4 Johtopäätöksiä

8.4.1 Tietovarantojen ja niiden sisältämien tietojen sääntelystä

Tietovarantoja koskeva yleissääntely painottuu tietojen käsittelyä ja tietojen käsittelyn vastuita, sekä tietojen saantia ja luovuttamista koskevaan sääntelyyn. Varsinainen tietovarantoja ja niissä olevien tietojen hyödyntämistä koskeva sääntely on tyypillisesti toteutettu erillissäätelyllä kohteittain. Tällöin sääntelyn kohde, sääntelytapa ja -taso määräytyvät toimialakohtaisesti ja riippuvat ajankohdasta, jolloin sääntely on valmisteltu.

Tietovarannon käsite on määritelty yleisesti tiedonhallintalaissa. Koska tiedonhallintalain erityislainsäädäntöä ohjaava vaikutus ei ole vielä ehtinyt muodostua, on voimassa runsaasti *rekistereitä* ja *tietojärjestelmiä* koskevaa sääntelyä, joissa sääntelyn kohteena ovat kuitenkin itse asiassa *tietovarannot* ja niiden sisältämien tietojen käsittely. Epäselvyyttä aiheuttaa myös se, että tietovarannon nimike on usein johdettu tietovarantoa toteuttavasta tai hyödyntävästä tietojärjestelmästä.

Tietovarantojen ja niiden sisältämien tietojen ylläpitoon liittyvät vastuut on yleisellä tasolla säädetty henkilötietojen käsittelyn tai tietovarannon vastuuviranomaisen sekä tietojen luovuttamista tai tietoturvallisuustoimenpiteistä vastaavan viranomaisen kautta. Tietojen luovuttamisen osalta sääntely jää pääosin yleiselle tasolle, ja vasta erityissäätelyn kautta on tunnistettavissa paremmin viranomaisten tehtäviä, joihin tiedot luovutetaan. Yleissäätelyyn sisältyvät määritelmät, kuten ”tietovaranto on tietoaineistoja sisältävä kokonaisuus” ja ”tietojärjestelmä on tietojen käsittelystä koostuva kokonaisjärjestely”, eivät tarkenna sääntelykohdetta suhteessa niihin liittyviin vastuisiin, vaan tarkentaminen on tehtävä tehtäväkohtaisen sääntelyn ja siinä esitettyjen viranomaisvastuiden kautta.

Työryhmä katsoo, että kun valmistellaan tietovarantoja koskevaa sääntelyä, tulisi kiinnittää erityistä huomiota käytettyihin määritelmiin. Tiedonhallintalailla on jo pyritty muodostamaan ohjaavaa yleistason sääntelyä olennaisista määritelmistä. Koska se on vielä suhteellisen uutta sääntelyä, on vielä odotettava, millaiseksi sen ohjausvaikutus vakiintuu. Tietovarantojen vastuiden ja tietojen käytön vastuiden osalta automaattinen päätöksenteko edellyttäisi nykyistä tarkempaa sääntelyä.

8.4.2 Tietojen laatua koskeva sääntely

Tietojen tai tiettyyn käyttötarkoitukseen muodostetun tietovarantojen tietojen laadusta on vain vähän yleissääntelyä. Yleisen tietosuoja-asetuksen 5 (1) d kohta edellyttää henkilötietojen käsittelyn olevan täsmällistä, tiedonhallintalain 15 §:ssä säädetään viranomaiselle velvoite varmistaa tietoaineistojen ajantasaisuus ja virheettömyys, ja hallintolain 31 §:ssä

säädettyyn viranomaisen selvitysvelvollisuuteen sisältyy asian ratkaisemisessa tarvittavien tietojen ja selvitysten hankinta. Mainitut lait eivät kuitenkaan tarkenna, mitä virheettömyydellä tai ajantasaisuudella missäkin yhteydessä tarkoitetaan.

Tietojen laatua koskevasta sääntelystä saatava kuva tarkentuu vain osittain, kun tarkastellaan tietovarantoja tai tiettyyn toimintaan tai toimialaan liittyviä tietoja. Perustietovarantoja koskevassa sääntelyssä vain väestötietojärjestelmän sisältämät tietyt henkilötiedot ovat erikseen säädetty *julkisesti luotettaviksi* (väestötietolaki 18 §). Muiden tietovarantojen laatua varmentava sääntely muodostuu lähinnä tietojen avoimuuden tai tietojen ilmoittajalle asetetun vastuun kautta. Taloustietojen ja tilastotietojen osalta sääntelyssä määritellään käsitteet oikeellisista ja riittävistä tiedoista (talousarviolaki, kirjanpitolaki) sekä tilastojen luotettavuudesta (tilastolaki), mutta ei esitetä millä kriteereillä vaatimusten täyttymistä olisi mahdollista arvioida.

Osana valtiovarainministeriön asettamaa Tiedon hyödyntäminen ja avaaminen -hanketta on laadittu alustavat tiedon laatukriteerit, jotka perustuvat kansainväliseen ISO 25012 -standardiin. Laatukriteerien on tarkoitus valmistua vuoden 2021 loppuun mennessä. Alustavia laatukriteereitä ovat:

- *Oikeellisuus, tarkkuus, ajantasaisuus ja johdonmukaisuus*. Käytettyjen tietojen virheettömyys on olennaista asianmukaisen käsittelyn ja lainmukaisen lopputuloksen saavuttamiseksi. Tiedonhallintalain 15.1 §:n 3 kohdassa säädetään viranomaisten velvollisuudesta varmistaa tietoaineistojen ajantasaisuus ja virheettömyys. Myös yleisessä tietosuoja-asetuksessa edellytetään tietojen täsmällisyyttä ja ajantasaisuutta sekä velvoitetaan korjaamaan tai poistamaan virheelliset tiedot.
- *Kattavuus*. Kattavuus kuvaa sitä, että tietoaineisto sisältää kaikki määritellyt kohdeyksiköt. Kattavuus toteutuu lainsäädännössä asettamalla toimijoille velvollisuus ilmoittaa tai merkitä erilaisia tietoja tietovarantoihin, kuten esimerkiksi väestötietolain 25 §:ssä tai oikeushallinnon valtakunnallisesta tietovarannosta annetun lain (955/2020) 5–6 §:ssä. Jos rekisteriin tehty merkintä on välttämätön tietyn oikeusvaikutuksen aikaansaamiseksi, kuten esimerkiksi yhdistyslain 6.1 §:ssä säädetään, tietovarannon kattavuuden voidaan olettaa varmistuvan varsin tehokkaasti. Tällöin tietovarannon ei tarvitse vastata todellisuutta, jota se kuvaa, koska tietovaranto itsessään on tällainen todellisuus.
- *Täydellisyys*. Täydellisyys kuvaa sitä, että tietoaineisto sisältää kaikki siihen sisältyvän kohdeyksikön määritellyt ominaisuustiedot. Tietoaineistojen täydellisyyttä turvaavaa sääntelyä on varsin runsaasti, sillä laissa yleensä säädetään yksityiskohtaisesti, mitä erilaisia tietoja tietystä kohteesta on merkittävä. Esimerkiksi väestötietolaissa tällaista sääntelyä on 13–16 §:ssä.

Olennaista on kuitenkin se, onko eri ominaisuustiedot kirjattava, vai voidaanko ne kirjata. Laissa saatetaan siis säätää luettelo tiedoista, joita voidaan käsitellä, mutta joita ei ole velvoitetta kirjata. Lainsäädännössä ei kuitenkaan aina ole tarkoituksenmukaista velvoittaa kirjaamaan erilaisia ominaisuustietoja kovin yksityiskohtaisesti. Tietystä kohteesta ei tapauksesta riippuen ole saatavilla kaikkia laissa mainittuja ominaisuustietoja, eikä niiden kaikkien kirjaaminen ole aina viranomaisen tehtävän hoitamiseksi tarpeellistakaan.

- *Ymmärrettävyys*. Ymmärrettävyydellä tarkoitetaan sitä, että tietoaineistolla on kuvailutietoja (metatietoja), jotka auttavat tietoaineiston ymmärtämisessä. Ilman riittäviä koneluettavassa muodossa olevia kuvailutietoja, ei tietoja voida käyttää automaattiseen käsittelyyn. Tiedonhallintalain 19.2 §:n mukaan viranomaisen on huolehdittava, että tietoaineisto on saatavilla ja hyödynnettävissä yleisesti käytettävässä koneluettavassa muodossa kuvailutietoineen, jos tietoaineisto voidaan saattaa alkuperäisestä muodosta suoraan koneluettavaan muotoon. Tiedonhallintalain 25 § velvoittaa tiedonhallintayksiköitä muodostamaan viranomaisten käyttöön asiarekistereitä, joihin kirjataan 26 §:n mukaisesti viranomaisessa käsiteltävistä asioista erilaisia kuvailutietoja, kuten tiedonhallintayksikön y-tunnus, asiakirjan laatimis- tai saapumisajankohta, asiakirjan laatija tai lähettäjä, ja niin edelleen. Tiedonhallintalain 27 §:n mukaan tiedonhallintayksikön on järjestettävä myös muun kuin asiankäsittelyn yhteydessä muodostuvan tietoaineiston hallinta siten, että tietoaineistosta muodostettavat asiakirjat ovat haettavissa jollakin tietokokonaisuudet yksilöivällä tunnuksella.
- *Suositustenmukaisuus*. Lainsäädännössä ei pääsääntöisesti erikseen säädetä tietoaineistojen suositustenmukaisuudesta. Suositusten noudattamiseen sellaisenaan velvoittaminen lailla olisi ongelmallista, koska suosituksia ei ylläpidetä lainsäädäntöprosessin kautta. Lisäksi suosituksen rooli muuttuu olennaisesti, jos siitä tuleekin suosituksen sijaan osa velvoittavaa lainsäädäntöä.
- *Jäljitettävyys*. Jäljitettävyys kertoo siitä, että tietoaineistoon ja sen tietoihin tehdyt muutokset voidaan jäljittää, ja että tiedon alkuperä on tiedossa. Tiedonhallintalain 13 §:n mukaan tiedonhallintayksikön on varmistettava tietoaineistojen tietoturvallisuus koko niiden elinkaaren ajan. Tietoturvallisuuteen kuuluu myös tietoaineistojen eheys. Tiedonhallintalain 15.1 §:n mukaan viranomaisen on varmistettava tietoaineistojen muuttumattomuus ja alkuperäisyys. Lisäksi tiedonhallintalain 20 §:n vaatimus teknisten rajapintojen käytössä viranomaisten välisessä säännöllisessä tiedonvaihdossa sekä 17 §:n vaatimus lokitietojen keräämisestä ovat omiaan varmistamaan tietojen alkuperää ja jäljitettävyyttä.

- *Koneluettavuus*. Koneluettavuus kuvaa sitä, onko tietoaineisto rakenteellisessa muodossa siten, että sitä voidaan käsitellä koneellisesti, ja käsittely on mahdollista eri tietojärjestelmissä. Tiedonhallintalain 19.2 §:n mukaan viranomaisen on huolehdittava, että tietoaineisto on saatavilla ja hyödynnettävissä yleisesti käytettävässä koneluettavassa muodossa kuvailutietoineen, jos tietoaineisto voidaan saattaa alkuperäisestä muodosta suoraan koneluettavaan muotoon.
- *Täsmällisyys* (tai oikea-aikaisuus). Täsmällisyys tarkoittaa sitä, että tietoaineisto julkaistaan tai päivitetään ilmoitettuna ajankohtana ja riittävän tiheästi siinä tapahtuviin muutoksiin nähden. Tiedonhallintalaissa on edellä kuvatun mukaisesti tiedon ajantasaisuutta varmistavia säännöksiä, ja sähköinen luovutustapa tai teknisen rajapinnan kautta tapahtuva luovuttaminen tukee yleensä myös käytettävissä olevan tietoaineiston oikea-aikaisuutta.

Työryhmä katsoo, että tietojen laatu ei ole vain automaattisesta päätöksenteosta johtuva vaatimus tietojen hyödyntämiselle, vaan päätöksenteossa käytettävän tiedon oikeellisuuden ja virheettömyyden selvittämisvelvollisuus sisältyy yleisesti hallintoasioiden valmisteluun. Koska voimassa olevassa sääntelyssä tiedon laatuvaatimukset vaihtelevat tapauskohtaisesti, olisi tietojen laatua koskevaa sääntelyä yhdenmukaistettava ja jäsennettävä. Yhdenmukaisten kriteerien avulla viranomaisen olisi helpompi arvioida selvitysvelvollisuutensa toteutumista eri asioiden käsittelyn yhteydessä. Tämä selkeyttäisi myös virkavastuun kohdistumista automaattisessa päätöksenteossa. Lisäksi tulisi selvittää, miten viranomaiset käyttävät tai voivat käyttää automaattista tietojenkäsittelyä tietojen laadun varmistamiseen, ja onko näiltä osin tarve myös uudelle sääntelylle.

Tietojärjestelmillä toteutettavaan tietojen käsittelyyn liittyviä tiedon laadunvarmistustoimenpiteitä voidaan yleisellä tasolla jäsentää menettelyihin, joilla varmistetaan tietojen laatu tietojen kirjaamisen yhteydessä, tarkastetaan tietojen oikeellisuus toisista tietolähteistä (viranomaisen hallussa olevat tai toisten viranomaisten tietoaineistot), tarkistetaan eri tietoaineistojen välinen eheys (esim. tietoaineistojen ristiin tarkastaminen), tai tarkistetaan tietoaineiston sisäinen eheys (esim. erilaiset tietoaineistojen loogiset tarkistustekniikat). Tiedon laadunvarmistamiseen liittyviksi toimiksi voidaan katsoa myös tietosuoja-asetuksessa säädettyjen rekisteröidyn oikeuksien toteuttaminen.

Kuten laatukriteerien osalla, myös tietojen laadunvarmistamisessa käytetyt menetelmät ovat pitkälti riippuvaisia käsiteltävässä asiassa tarvittavista tiedoista, tarvittavien tietojen muodostumisesta sekä niiden ylläpitomenettelyistä. Koska tiedon laadulle ei voida asettaa täydellistä oikeellisuuden ja virheettömyyden vaatimusta, liittyy viranomaisten käyttämien tietojen laadun varmistamiseen myös menettelyt, joiden avulla viranomainen korjaa tiedon käytön yhteydessä havaitsemansa puutteet. Työryhmän näkemyksen mukaan

yleissääntelyn avulla on haasteellista tarkentaa muun muassa, miten tiedot tulisi tarkistaa missäkin tilanteessa ja milloin viranomaisten voisi arvioida suorittaneen tarkistustoimenpiteensä riittävällä tasolla. Tietojen laadun ja ajantasaisuuden varmistamisen ollessa jatkuva tehtävä, on vaatimusten kiinnittäminen vain tiettyyn tietojärjestelmän elinkaaren vaiheeseen ongelmallista. Tietojärjestelmien kehittämisen yhteydessä vaatimukset kohdistuvat järjestelmien suunnitteluun ja testaamiseen kohdistuviin vaatimuksiin, järjestelmän käyttöönoton yhteydessä tietokantaan ladattavien tietojen eheyden varmistamiseen ja käytön yhteydessä erilaisiin kontrolleihin, joilla tietojen kirjaamista, tarkistusta ja korjaamista voidaan ohjata tiedon laadun näkökulmasta.

8.4.3 Tiedon käytön ja tiedon laadun välinen suhde

Tietovarantojen tietojen hyödyntämistä koskeva yleissääntely perustuu käsittelyn lainmukaisuuteen ja käyttötarkoitussidonnaisuuteen. Tietosuoja-asetuksen mukaan tietojen käsittely on lainmukaista, kun se perustuu lakisääteisen velvoitteen noudattamiseen ja tehdään käyttötarkoituksen edellyttämässä laajuudessa.

Tiedolle asetettaviin laatuvaatimuksiin vaikuttaa olennaisesti se, onko kyse suoraan päätöksenteossa käytettävästä tiedosta vai siitä, että käsittely on käynnistynyt viranomaisen tai asianosaisen aloitteesta. Viranomaisen aloitteesta asian vireille tuleminen liittyy tyypillisesti tilanteisiin, joissa viranomaiselle on säädetty velvoite omatoimisesti selvittää ovatko päätöksenteon perusteet ja edellytykset olemassa, jotka muodostavat sille velvollisuuden käynnistää asiankäsittely.

Tiedon laatua koskeva sääntely ei tällä hetkellä ota huomioon sitä, mihin tietoa eri tilanteissa käytetään. Sen sijaan tiedon laatua säännellään yhtämittaisuuden lähtökohdasta, jossa kaiken tiedon on täytettävä tiedolle asetetut yleiset vaatimukset. Työryhmä katsoo, että jos hallintotoiminnassa käytettävän tiedon laadusta säännellään jatkossa tarkemmin, ei yhtämittaisuus olisi tarkoituksenmukaista, vaan tiedon laatuvaatimusten tulisi olla suhteellisia tiedon käyttötarkoituksen kanssa.

Tiedon laadun osalta voidaan erottaa edellä kuvatun perusteella kolme tiedon käyttötarkoitusta:

1. tietoa käytetään sellaisenaan automaattisen päätöksen tai muun automaattisen hallintotoimen tekemiseen,

2. tietoa käytetään valvonta- tai seurantatarkoituksessa, jonka perusteella viranomainen saattaa panna asian vireille, tai

3. tietoa käytetään arvioimaan asianosaisen antaman tiedon paikkansapitävyyttä.

Kun tietoa käytetään sellaisenaan automaattisen päätöksen hallintotoimen tekemiseen ilman, että käsittelyyn osallistuu ihminen, on käytettävän tiedon laadulle asetettava myös verrattain korkeat vaatimukset. Käytetyillä tiedoilla on tällöin oikeusvaikutuksia, vaikkei niiden alkuperäisellä kirjaamisella välttämättä olisi ollutkaan. Tietojen laatu onkin yksi asianmukaisen käsittelyn edellytys. Jos käytetyt tiedot eivät ole riittävän laadukkaita, ei viranomaisen selvitysvelvollisuus voi toteutua. Ei kuitenkaan ole kohtuullista edellyttää tiedoilta täydellistä laatua, tai muutoin minkäänlainen päätöksenteko ei olisi enää mahdollista.

Kun tietoa käytetään valvonnassa tai seurannassa tai asianosaisen antamien tietojen tarkistamiseksi, tietoa koskevien laatuvaatimusten ei tarvitse olla yhtä korkeita kuin silloin, kun tietoja käytetään suoraan automaattiseen päätöksentekoon tai muuhun toimeen. Valvonnan tai tarkistamisen tilanteessa syntyvän herätteen johdosta viranomainen ryhtyy tarpeellisiksi katsomiin toimenpiteisiin, kuten kuulemaan asianosaista tai hankkimaan muuta selvitystä. Jos valvonnassa tai tarkistamisessa syntynyttä lopputulosta käytetään sellaisenaan automaattiseen käsittelyyn, olisi tiedon laadusta noudatettava samaa, mitä edellytetään muutenkin automaattisen käsittelyn pohjana olevalta tiedolta.

Tietojen arviointi ja tarkistaminen voi olla hyvin toimiala- tai tapauskohtaista.[126] Työryhmän arvion mukaan olisi selvitettävä tarkemmin, miltä osin tietojen arviointia tehdään tai voisi tehdä automaattisesti. Useissa viranomaisaloitteisissa asioissa viranomaista

126 Esimerkiksi ympäristönsuojelulaissa (527/2014) tarkoitetun ympäristöluvan myöntämisessä, jossa lupaa koskevassa hakemukseen luvan hakija on liittänyt hakemukseen lupaharkinnan kannalta tarpeelliset selvitykset toiminnastaan, sen vaikutuksista, asianosaisista ja muista merkityksellisistä seikoista, tietojen tarkistaminen on luonteeltaan eri tyyppistä kuin esimerkiksi toimeentulotuesta annetussa laissa (1412/1997) tarkoitettua perustoimeentulotuen myöntämisessä arvioitavien menojen osalta.

velvoitetaankin lainsäädännössä kuulemaan asianosaista ennen asian ratkaisemista[127]. Hallintoasian yhteydessä velvoite informoida asiakasta käsittelystä ja käytettävistä tiedoista sekä velvoite selvittää tietojen oikeellisuus voisivat olla toteutettavissa automaattisin keinoin, esimerkiksi kuulemalla asiakasta asian vireillepanon jälkeen tai, asianosaisaloitteisen asian kohdalla, jo sen yhteydessä.

8.4.4 Päätöksenteossa käytettävän tiedon tietolähteet

Tiedonhallintalain 20 §:ssä säädetään viranomaisen velvoitteesta pyrkiä hyödyntämään toisen viranomaisen hallussa olevaa tietoa ja huolehdittava tietoja hyödyntäessään asianosaisen ja asiakkaan oikeusturvasta. Koska tiedonhallintalain esitöiden mukaan viranomainen ei voisi tehdä hallinnon asiakasta koskevia välittömän oikeusvaikutuksen aiheuttavia päätöksiä pelkästään kerättyjen tietojen perusteella, työryhmä katsoo, että viranomaisen tulisi muodostaa menettelyt, joiden avulla se pystyy varmistamaan vastaanottamiensa tietojen riittävän oikeellisuuden selvitysvelvoitteensa mukaisesti. Mikäli viranomainen hyödyntää päätöksenteossaan alun perin muuhun käyttötarkoitukseen keräämäänsä tietoa, edellyttää tietosuoja-asetus henkilötietojen käsittelyn osalta tietojen käsittelijää arvioimaan päätöksenteossa suoritettavan tietojen käsittelyn seuraukset rekisteröidylle sekä alkuperäisen käyttötarkoituksen väliset yhteydet. Kun muuhun tarkoitukseen kerätyn tiedon hyödyntämistä voidaan tietojen laadun osalta verrata toisilta viranomaisilta saatuun tietoon, tulisi vastaavien tietojen oikeellisuutta ja laatua koskevien menettely- ja informointitarpeiden koskea myös tietojen toissijaista käyttöä.

Viranomaiset saavat pääosin päätöksenteossa käyttämänsä tiedot asianosaiselta, toisilta viranomaisilta tai muilta tietoja tehtävän tarpeisiin luovuttavilta toimijoilta sekä keräämällä tiedot itse asian selvittämisen yhteydessä. Viranomaiset käyttävät päätöksenteossaan myös sellaisia ulkoisia tietolähteitä, jotka on perustettu tukemaan nimenomaisesti viranomaisen tehtävissä tarvittavien tietojen saamista. Työryhmän näkemyksen mukaan erityisesti niissä tilanteissa, joissa vastuu yhteiseen käyttöön tarkoitettujen tietovarantojen tietojen laadusta on säädetty pääosin tietojen ilmoittajalle, tulisi tietoja hyödyntävän viranomaisen pystyä tarvittaessa esittämään, *miten* tiedot ovat sen päätöksenteossa hyödyntämään tietovarantoon muodostuneet, erityisesti tietojen oikeellisuuden osalta. Tietojen muodostumista esittävää selvitystä ei olisi tarpeen tehdä

127 Esimerkiksi ulkomaalaislain (301/2004) 145 §.

tapauskohtaisesti päätöksenteon yhteydessä[128], vaan osana kuvauskokonaisuutta, jonka avulla viranomainen muutenkin toteaa tietojärjestelmiensä tietojenkäsittelyn toimivuuden vaatimusten mukaisesti. Tätä edesauttaisi osaltaan se, että tiedonhallintalain 5 §:ssä säädetyn tiedonhallintamallin sisältöä tarkennettaisiin kattamaan selkeämmin myös muita viranomaisilta saatavat tiedot.

Erityisesti kun viranomainen käyttää päätöksenteossaan muilta viranomaisilta saatuja tietoja, vaikuttavat tietojen ajantasaisuuteen myös oikeudet tietojensaantiin sekä tietojen luovuttavan velvoitteet ja menettelyt, joilla se tietoja tarvitsijalle luovuttaa. Päätöksenteossa käytettävän tiedon edellytyksenä on viranomaisten oikeudet saada tietoja lainmukaiseen käyttötarkoitukseen. Koska tietoa tarvitsevan ja sitä luovuttavan viranomaisen on tiedonhallintalain 15 §:n mukaan varmistettava tietoaineistojen saatavuus ja käyttökelpoisuus suhteessa käyttötarkoitukseen, tulisi työryhmän näkemyksen mukaan molempien tietojenvaihtoon osallistuvien tahojen pystyä osaltaan varmistamaan tietojen luovuttamisessa ja vastaanottamisessa tarvittavien oikeudellisten ja teknisten edellytysten olemassaolo.

Tietojensaantioikeuksia ja erityisesti tietojenluovuttamiseen liittyviä menettelyjä koskeva sääntely muodostaa monimuotoisen kokonaisuuden, jota esimerkiksi tiedonhallintalain sääntely ei muuta, koska tiedonhallintalaissa ei säädetä tietojensaantioikeuksista. Automaattisessa päätöksenteossa hyödynnettävien ulkoisten tietovarantojen osalta voimassa oleviin säännöksiin sisältyy monin paikoin tarpeetonta, kaksinkertaista sääntelyä, jossa on säädetty sekä tietojen luovuttamisesta, että tietojen saannista. Kaksinkertaisen sääntelyn purkamista voisi edesauttaa tietojensaantioikeuden edellytyksiä koskevan yleissääntelyn kehittäminen. Jos tietoja tarvitsevan toimijan tiedonsaantioikeudesta on jo säädetty, eikä tietojenluovuttamiseen liity tehtäväkohtaisia erityispiirteitä (esimerkiksi tietojenluovutusmuotoa tai -ajankohtaa koskevat vaatimukset), ei tarvetta erilliselle tietojenluovutuksen mahdollistavalle sääntelyllä ole. Työryhmä katsoo kuitenkin, että tietojensaantioikeuksia ja tietojenluovutusvelvoitteita koskevan sääntelyn kehittämisessä on kyse automaattista päätöksentekoa laajemmasta viranomaisten tehtävien suorittamisen ja tietovarantojen yhteentoimivuutta koskevan sääntelyn kehittämisestä, jota käsillä olevan lainvalmisteluhankkeen yhteydessä ei ole mahdollista tehdä.

128 Automaattisen päätöksenteon yhteydessä ulkoisista tietolähteistä saatujen tietojen esittäminen päätöksen perusteina ei ole kaikilta osin tarkoituksenmukaista tai edes mahdollista. Kun kaikissa käytössä olevissa tietojärjestelmissä ole toiminnallisuutta, jolla tietokannassa oleva tieto olisi eriteltävissä sen saantitavan mukaan, vaatimuksen toteuttaminen tulisi edellyttämään merkittäviä muutoksia viranomaisten tietojärjestelmiin.

Voimassa olevassa lainsäädännössä on ylipäätään vain vähän tietovarantojen tietoaineistojen saatavuutta ja tietovarannon käytettävyyttä koskevaa sääntelyä. Vähäinenkin sääntely perustuu lähinnä joko viranomaisten yleisiin velvoitteisiin varmistaa toiminnan jatkuvuus tai tietovarantoa ja järjestelmää koskevaan vastuujakoon (esimerkiksi vastuu tietovarannon ylläpidosta ja toimivuuden varmistamisesta). Tällä hetkellä tiedonhallintalaissa säädetään muiden viranomaisten tietojen hyödyntämisestä, sähköisistä tietojenluovutustavoista (tekninen rajapinta ja katseluyhteys) sekä vaatimuksista, joita niiden toteutuksessa tulee varmistaa, mutta ei vaatimuksista, mitä ulkoisten tietojärjestelmien hyödyntäminen automaattisessa päätöksenteossa edellyttäisi tietojen saatavuuden ja käytettävyyden varmistamisen osalta. Kun viranomaisen vastuulla olevan tietovarannon tietoja käyttävät muut toimijat omien tehtäviensä toteuttamisessa, korostuvat tietovarannon ja sen tarjoamien ohjelmistorajapintojen palvelutasovaatimukset, kuten miten ja milloin tiedot ovat niitä tarvitsevan käytettävissä.

Työryhmä katsoo, että automaattisen päätöksenteon tukeutuminen ulkoisiin tietovarantoihin edellyttäisi varmuutta tietojen saantiin, sekä sovittuja menettelyjä, joilla mahdollisissa häiriötilanteissa tietojärjestelmät pystyvät toimimaan tarkoituksenmukaisella tavalla ja vähintäänkin ilmoittamaan häiriön olemassaolosta päätöstä suorittavalle osapuolelle tai prosessille. Viranomaisten tullessa yhä riippuvaisemmiksi toistensa tietovarannoista, tulisi sääntelyn kehittämisen rinnalla miettiä myös muita toimenpiteitä, joilla huolehditaan viranomaisten sujuvasta yhteistyöstä ja suositusten sekä standardien noudattamisesta.

Tietojen saatavuuden ja käytettävyyden osalta on myös syytä huomioida, ettei niiden varmistaminen ole vain automaattista päätöksentekoa koskeva vaatimus, vaan vastaava varmuus tukisi myös muita hallinnollisten asioiden valmistelua, kun ne tukeutuvat ulkoisiin tietolähteisiin ja muilta viranomaisilta saatavaan tietoon. Sääntelyn näkökulmasta tällöin olisi kuitenkin kyse enemmän viranomaisten tietojenluovutusta koskevan menettelyn yhdenmukaistamiseen tähtäävästä sääntelystä, kuin tietojärjestelmien tai tietovarantojen ominaisuuksia koskevasta sääntelystä.

Edellä mainitun lisäksi, tällä hetkellä viranomaisten hallinnoimista tiedoista osaa ylläpidetään jatkuvasti kaikkien potentiaalisten asianosaisen osalta, esimerkiksi väestötietojen ylläpito valtion viranomaisissa jokaisen Suomessa vakinaisesti asuvien osalta tai kunnallisissa viranomaisissa jokaisen kunnan asukkaiden osalta. Työryhmä toteaa, että tietovarantojen välistä tiedon luovuttamista ei voida muodostaa säännölliseksi ja jatkuvaksi päivittämiseksi vain sen vuoksi, että tiedot olisivat käytettävissä ”varmuuden vuoksi” häiriötilanteen tapahtuessa, vaan tiedon käsittelyn on oltava kytköksissä tiettyyn käyttötarkoitukseen.

Työryhmän näkemyksen mukaan automaattisen päätöksenteon yhteydessä käytettävän tiedon osalta korostuvat myös asianosaisen oikaisukeinot korjata päätöksenteon perusteena käytettäviä tietoja tilanteissa, joissa päätöksessä oleva virhe on johtunut siinä käytettävistä tiedoista. Tällöin kyse on kuitenkin enemmän päätöksentekomenettelyyn liittyvän sääntelyn kehittämisestä kuin tietojärjestelmiä tai tietovarantoja koskevasta sääntelystä. Tietojärjestelmien tietojenkäsittelyn tulee toteuttaa hallinnolta vaadittua menettelyä. Vastaavasti tietojärjestelmiin kohdistuvalla sääntelyllä olisi mahdollista kohdentaa erillisiä vaatimuksia niihin tietojärjestelmien toiminnallisuuksiin, joilla varmistetaan riittävän informaation saaminen tietojärjestelmän suorittamasta tietojenkäsittelystä ja käsiteltävien tietojen tekninen eheys. Tietojärjestelmiä koskevalla sääntelyllä ei aseteta vaatimuksia sille, miten viranomainen hankkii tai saa tietoja tehtäviensä tarpeisiin, tai näihin liittyvästä selvittämisvelvoitteista ja harkinnasta.

9 Tietojärjestelmien vaatimustenmukaisuuden arviointi

9.1 Nykytila

9.1.1 NLF-asetus ja akkreditointilaki

NLF-asetuksessa[129] vahvistetaan vaatimustenmukaisuuden arviointilaitosten akkreditointia koskevat säännöt sekä akkreditointielimiä koskevat vaatimukset. FINAS on NLF-asetuksessa tarkoitettu Suomen ainoa kansallinen akkreditointielin. NLF-pakettiin liittyvä sääntely (NLF-asetus ja -päätös sekä pakettiin kuuluvat tuotedirektiivisäännökset) lähtee siitä, etteivät kansalliset akkreditointielimet tai ilmoittamisesta vastaavat toimivaltaiset viranomaiset (jollainen myös Liikenne- ja viestintävirasto on esim. radiolaitteiden ja ilmailulaitteiden osalta) saa olla mukana arviointilaitostoiminnassa. Kansalliset akkreditointielimet eivät saa kilpailla vaatimustenmukaisuuden arviointilaitosten kanssa eikä ilmoittamisesta vastaava toimivaltainen viranomainen saa tarjota tai suorittaa mitään toimintoja, joita vaatimustenmukaisuuden arviointilaitokset tekevät. Kansallisen turvallisuuden piiriin kuuluvat asiat eivät ole NLF-asetuksen piirissä, joten se ei koske kansallisen turvallisuuden piiriin liittyvää arviointitoimintaa eli turvallisuusluokiteltua tietoa käsittelevien kohteiden arviointia.

Vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annettua lakia (920/2005) eli akkreditointilakia sovelletaan vaatimustenmukaisuuden arviointipalvelujen akkreditointiin ja siihen rinnastettavaan pätevyyden arviointiin. Lain mukaan akkreditoinnilla tarkoitetaan ”pätevyyden toteamista yhdenmukaisten kansainvälisten tai eurooppalaisten arviointiperusteiden mukaisesti;”. Lain 6 §:n mukaan ”akkreditointiin sovelletaan yhdenmukaisia kansainvälisiä ja eurooppalaisia arviointiperusteita”.

129 Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta.

9.1.2 Arviointilain ja arviointilaitoslain mukainen arviointi ja todistus

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011, arviointilaki) tarkoituksena on kehittää tietoturvallisuutta viranomaisissa. Laissa säädetään menettelystä, jolla voidaan arvioida viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen vaatimustenmukaisuutta. Arviointitehtävä on laissa annettu Viestintävirastolle (nykyisin Liikenne- ja viestintävirasto). Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta arvioiva viranomainen kuuluu myös osana eri maissa noudatettuihin ja useissa kansainvälisissä sopimuksissa ja säädöksissä edellytettyihin järjestelyihin.

Arviointilain mukaan valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain kyseisessä laissa tarkoitettua menettelyä (Liikenne- ja viestintäviraston suorittama arviointi) taikka sellaista arviointilaitosta, joka on saanut Liikenne- ja viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, arviointilaitoslaki) mukaan.

Arviointilaissa säädetään Liikenne- ja viestintäviraston tehtäväksi arvioida viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimuksenmukaisuutta. Arviointi voidaan tehdä viranomaisen pyynnöstä ja pyynnön voi viranomaisen toimeksiannosta tehdä myös se, joka tekee viranomaisen lukuun hankintoja taikka tuottaa tietojenkäsittely- tai tietoliikennepalveluja taikka hoitaa niiden järjestämiseen liittyviä palvelutehtäviä.

Liikenne- ja viestintävirasto voi lain mukaan myös valtiovarainministeriön pyynnöstä tehdä selvityksiä valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta ja valtiovarainministeriö voi myös pyytää valtionhallinnon tietoturvallisuudesta annettujen säännösten täytäntöönpanon seuraamiseksi sekä niiden kehittämiseksi Liikenne- ja viestintävirastoa laatimaan selvityksen valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta.

Lisäksi arviointilaissa luetellaan käytettävät tietoturvallisuuden arviointiperusteet yleisellä tasolla sekä säädetään salassa pidettävien tietojen saamisesta ja oikeudesta päästä tiloihin ja tietojärjestelmiin. Liikenne- ja viestintävirasto voi pyydettäessä antaa arvioinnista todistuksen ja laissa säädetään edellytyksistä todistuksen voimassaololle sekä sen peruuttamisesta.

Arviointilaitoslain yhtenä tarkoituksena on edistää yritysturvallisuutta luomalla valvonta yritysten tietoturvallisuutta arvioiville laitoksille. Vaikka yrityksiä koskevan turvallisuusselvityksen laatiminen kuuluukin turvallisuusselvityslain (726/2014) mukaan viranomaiselle, yritykset voivat arviointilaitoslain myötä varautua osallistumaan esimerkiksi sellaisiin

kansainvälisiin hankintakilpailuihin, joissa edellytetään viranomaisen laatimaa turvallisuusselvitystä ja sen perusteella annettavaa todistusta. Tämän järjestelyn on ollut tarkoitus parantaa suomalaisten yritysten kilpailukykyä kansainvälisissä hankinnoissa. Myös viranomaiset voivat käyttää arviointilaitosten palveluja – ja valtionhallinnon viranomaisten tulee arviointilain mukaan käyttää joko Liikenne- ja viestintäviraston taikka hyväksytyn arviointilaitoksen arviointipalveluja.

Arviointilaitoslaissa säädetään arviointilaitosten hyväksymismenettelystä, hyväksymisen edellytyksistä sekä hyväksymisen peruuttamisesta. Lisäksi säädetään Liikenne- ja viestintäviraston tarkastusoikeudesta sekä tiedonsaantioikeudesta sekä hyväksytyn arviointilaitoksen tiedonanto- ja ilmoitusvelvollisuudesta Liikenne- ja viestintävirastolle. Laissa säädetään myös arviointilaitoksen tehtävistä sekä käytettävistä tietoturvallisuuden arviointiperusteista. Hyväksytyn arviointilaitoksen on arviointilaitoslaissa tarkoitettuja tehtäviä hoitaessaan noudatettava hallintolakia, julkisuuslakia sekä kielilakia.

Hyväksytyn arviointilaitoksen aseman saavuttamiseksi yhteisön täytyy hakea ensin kansallisen akkreditointiyksikön (FINAS)[130] akkreditointi vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annettua lakia (920/2005, akkreditointilaki) noudattaen. FINASin tehtävänä on arviointilaitoslain 5 §:n mukaan arvioida 5 §:n 1 momentin 1–3 kohdissa[131] säädettyjen vaatimusten toteutuminen. Tämän jälkeen yhteisön on haettava Liikenne- ja viestintäviraston hyväksyntä 5 §:n 1 momentin 4 ja 5 kohdissa tarkoitettujen vaatimusten toteutumisesta, eli siitä, että 4) laitoksen vastuuhenkilöiden luotettavuus on varmistettu ja laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan; ja että 5) laitoksella on asianmukaiset ohjeet toimintaansa ja sen seurantaa varten.

130 Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (NLF-asetus) vahvistetaan vaatimustenmukaisuuden arviointilaitosten akkreditointia koskevat säännöt sekä akkreditointielimiä koskevat vaatimukset. FINAS on NLF-asetuksessa tarkoitettu Suomen ainoa kansallinen akkreditointielin.

131 Arviointilaitoslain 5 §:n 1 momentin 1–3 kohtien mukaan tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että:1) laitos on toiminnallisesti ja taloudellisesti riippumaton arvioinnin kohteesta; 2) laitoksen henkilökunnalla on hyvä tekninen ja ammatillinen koulutus sekä riittävän laaja-alainen kokemus toimintaan kuuluvissa tehtävissä; 3) laitoksella on toiminnan edellyttämät laitteet, välineet ja järjestelmät.

Liikenne- ja viestintäviraston on arviointilain 4 §:n mukaan ennen tietoturvallisuuden arviointilaitoksen hyväksymistä varattava suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Suojelupoliisi noudattaa lausuntoaan laatiessaan, mitä turvallisuusselvityslaissa säädetään.

Arviointilaitoksille ei ole myönnetty pätevyyttä arvioida korkeimpien turvallisuusluokkien tietoturvallisuusvaatimusten täyttymistä. Tällä hetkellä hyväksyttyjä arviointilaitoksia on kolme, joista kahdella on pätevyysalueena turvallisuusluokan IV ja III tietoja käsittelevien järjestelmien arviointi (ns. Katakri-pätevyys). Arviointilaitos voi VAHTI- tai Katakri-pätevyyden saatuaan tehdä tietoturvallisuuden arviointeja sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007, asiakastietolaki) kuvatuille A-luokan järjestelmille sekä sosiaali- ja terveystietojen toissijaisesta käytöstä annetussa laissa (552/2009) kuvatuille käyttöympäristöille. Arviointilaitoslaissa säädetyt edellytykset arviointilaitoksen hyväksymiselle ovat hyvin yleisluontoiset. Tämä on johtanut siihen, että hyväksyntä perustuu suurelta osin Liikenne- ja viestintäviraston antamaan ohjeeseen tietoturvallisuuden arviointilaitoksille (Ohje 210/2016 O) – eli ei sitovaan normistoon. Lisäksi nykytilanteen eräänä haasteena on, että arviointilaitosten osaamisalueet eivät täysin vastaa viranomaisarvioinnilta (eli Liikenne- ja viestintäviraston tekemältä arvioinnilta) vaadittavaa sisältöä, ja arviointilaitosten pätevyysalueita on jouduttu hyväksymään osittaisina. Arviointilaitosten pätevyysalueet eivät kata esimerkiksi salausratkaisujen, yhdyskäytäväratkaisujen tai hajasäteilysuojausten riittävyyden arviointia kuin osittaisina ja rajauksin.

Turvallisuusluokkien TL IV ja TL III tietojärjestelmien ja tietoliikennejärjestelyjen arviointien alueella Liikenne- ja viestintävirasto toimii viranomaisten tietojärjestelmien arvioinnissa samoilla markkinoilla kaupallisten toimijoiden kanssa, mutta hinnoittelee palvelunsa maksuperustelain mukaisesti. Liikenne- ja viestintävirasto on vuoden 2019 jälkeen tehnyt vain yksittäisiä arviointilakiin perustuvia TL IV tason arviointeja ja on keskittynyt korkeampien turvallisuusluokkien käsittely-ympäristöjen arviointeihin. Arviointilaitokset tekevät vuosittain useita kymmeniä TL IV tai TL III tason arviointeja. Liikenne- ja viestintävirasto ei arviointilain perusteella arvioi muiden kuin viranomaisten tietojärjestelmiä ja tietoliikennejärjestelyjä – eikä siten arviointilain perusteella kilpaile yksityisten yhteisöjen kanssa yksityisen sektorin tietoturvallisuuden arviointitoiminnassa. Sen sijaan yritysturvallisuusselvitysten tekeminen on turvallisuusselvityslaissa säädetty yksinomaan viranomaisten (suojelupoliisi, pääesikunta ja Liikenne- ja viestintävirasto) tehtäväksi.

Tietojärjestelmän tietoturvallisuuden arviointi on yksi keino tunnistaa ja arvioida järjestelmään kohdistuvia turvallisuusriskejä. Arviointilain mukaista arviointia ei ole kansallisella tasolla säädetty pakolliseksi, eikä valtion hallinnon viranomaisella ole velvollisuutta hankkia arviointilaissa tarkoitettua todistusta siitä, että tietojärjestelmä täyttää vaatimukset.

Tyypillisesti kansallisten tietojen käsittelyyn käytettyjen tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja teetetään hyväksytyillä arviointilaitoksilla siten, että arviointilaitos antaa arvioinnin tilaajalle arviointiraportin, ja tietojärjestelmästä vastaava viranomainen arvioi jäännösriskit ja tekee erillishyväksynnän riskienhallintakäytäntöjensä sekä tiedonhallintalain 13 § mukaisesti.

Kansallisille arvioinneille on vain harvoin haettu lisäksi arviointilaitoksen todistusta tai Liikenne- ja viestintäviraston todistusta. Arviointilain 8 a §:n mukaan asetuksella voidaan säätää, että valtionhallinnon viranomaisten on hankittava todistus tietojärjestelmistä tai tietoliikennejärjestelyistä, joissa käsitellään tietoja, joiden turvallisuusluokka on TL I tai TL II.

9.1.3 Laki kansainvälisistä tietoturvallisuusvelvoitteista – yritysturvallisuusselvitys (ja -todistus)

Kansainvälisiin tietoturvavelvoitteisiin liittyvistä vastuista on säädetty kansainvälisistä tietoturvavelvoitteista annetussa laissa (588/2004). Ulkoministeriö toimii kansainvälisten tietoturvavelvoitteiden toteuttamisessa kansallisena turvallisuusviranomaisena ja Liikenne- ja viestintävirasto tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa laissa tarkoitettuna määrättynä turvallisuusviranomaisena. Muita määrättyjä turvallisuusviranomaisia ovat puolustusministeriö, pääesikunta ja suojelupoliisi, jotka toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa.

Kansainvälisen tietoturvallisuusvelvoitteen edellyttäessä, esimerkiksi käsiteltäessä EU:n tai Naton turvallisuusluokiteltuja tietoja sähköisessä muodossa, tulee kyseisten tietojen käsittelyyn käytettävien tietojärjestelmien läpikäydä hyväksyntäprosessi, jonka päätteeksi kansallinen hyväksyntäviranomainen (SAA, Security Accreditation Authority, Suomessa Liikenne- ja viestintäviraston NCSA-toiminto) myöntää tietojärjestelmälle hyväksynnän (accreditation). Viranomaisten tietojärjestelmien suojausten arviointi toteutetaan kansainvälisistä tietoturvavelvoitteista annetun lain mukaisesti siten, että suojelupoliisi tai Pääesikunta toimivat fyysisen turvallisuuden ja Liikenne- ja viestintävirasto teknisen tietoturvallisuuden arvioivana ja hyväksyvänä viranomaisena.

Kansainvälisessä tietoturvallisuusvelvoitteessa edellytetty yritysturvallisuusselvitys laaditaan siten kuin turvallisuusselvityslaissa säädetään. Yritysturvallisuusselvitystodistuksen antaa kuitenkin kansallinen turvallisuusviranomainen (ulkoministeriö), jollei erityisistä syistä muuta johdu. Selvityksen laatineen viranomaisen on salassapitosäännösten

estämättä toimitettava todistuksen antamista ja siihen liittyvää harkintaa varten kansalliselle turvallisuusviranomaiselle tieto kaikista selvityksen laadinnassa ilmi tulleista selvityksen kohdetta koskevista seikoista.

9.1.4 Turvallisuusselvityslaki – yritysturvallisuusselvitys (ja -todistus)

Tietojärjestelmien tietoturvallisuuden arviointi yritysturvallisuusselvityksissä perustuu turvallisuusselvityslakiin. Vuonna 2013 voimaan tulleeseen turvallisuusselvityslakiin sisällytettiin säännökset yritysturvallisuusselvityksistä, joiden avulla selvitetään yrityksen vastuuhenkilöiden taustoja, tietoturvallisuuden tasoa yrityksessä ja yrityksen sitoumusten hoitokykyä.

Lain 9 §:n mukaan yritysturvallisuusselvityksen tekemisestä päättää suojelupoliisi. Pääesikunta päättää kuitenkin yritysturvallisuusselvityksen tekemisestä yrityksestä, joka hoitaa tai jonka on tarkoitus hoitaa puolustusvoimien antamaa tehtävää, taikka yrityksestä, joka liittyy puolustusvoimien hankintoihin. Liikenne- ja viestintävirasto laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen

Yritysturvallisuusselvitystä voi lain 33 §:n mukaan hakea:

1. *se, joka tarvitsee selvitystä laissa tai sen nojalla säädetyn taikka kansainvälisestä tietoturvallisuusvelvoitteesta johtuvan velvoitteen toteuttamiseksi;*

2. *viranomainen, jonka on tarkoitus tehdä sopimus selvityksen kohteen kanssa, jos sopimuksen yhteydessä yritykselle annetaan tai sopimuksen johdosta syntyy turvallisuusluokkaan I–III kuuluvaksi luokiteltuja asiakirjoja tai muita salassa pidettäviä asiakirjoja, jos näihin asiakirjoihin sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle;*

3. *2 kohdassa tarkoitetuissa tilanteissa viranomaisen toimeksiannosta valtionhallinnon hankinnoista vastaava yksikkö taikka valtionhallinnolle yhteisiä tai laajaan käyttöön tarkoitettuja tieto- ja viestintekniikkapalveluja tuottava yksikkö;*

4. *21 §:n 1 momentin 5 ja 6 kohdassa tarkoitettua toimintaa [ydinlaitosturvallisuus ja räjähdeaineturvallisuus] valvova viranomainen.*

Yritysturvallisuusselvitys voidaan tehdä selvityksen kohteen pyynnöstä, jos turvallisuusselvitystä edellytetään kansainvälisen järjestön tai toimielimen säännöissä tai toisen valtion laissa ja jos se on tarpeen sen vuoksi, että selvityksen kohde voi tulla valituksi kansainvälisen järjestön tai toimielimen järjestämään tai näiden muutoin organisoimaan hankkeeseen taikka toisessa valtiossa järjestettävään hankintakilpailuun taikka jos yritys aloittaa yritystoiminnan toisessa valtiossa.

Lisäksi turvallisuusselvityslaissa säädetään muun muassa yritysturvallisuusselvityksen hakemisesta, sen laatimisen edellytyksistä, siinä käytettävistä tietolähteistä, siihen liittyvistä tarkastuksista ja viranomaisen tiedonsaantioikeudesta sekä elinkeinonharjoittajan sitoutumisesta huolehtimaan tietoturvallisuustason säilyttämisestä sekä ilmoittamaan muutoksista.

Lain 46 §:n mukaan yritysturvallisuusselvityksen laatinut toimivaltainen viranomainen antaa yritysturvallisuusselvityksen perusteella hakijalle yritysturvallisuusselvitystodistuksen, jos yritys täyttää selvityksen perusteena olevat tietoturvallisuutta koskevat vaatimukset. Todistus annetaan myös selvityksen kohteelle. Kansallinen turvallisuusviranomainen antaa kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi tarpeellisen yritysturvallisuusselvitystodistuksen siten kuin kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa säädetään. Jos yritysturvallisuusselvitys on koskenut yksinomaan tietojärjestelmien tai tietoliikennejärjestelyjen turvallisuutta, selvityksen laatinut Liikenne- ja viestintävirasto voi antaa selvityksen perusteella todistuksen. Laissa säädetään todistuksen voimassaolosta, uusimisesta ja peruuttamisesta.

Lisäksi säädetään turvallisuusselvitysrekisteristä, tietojen antamisesta mainitusta rekisteristä sekä nuhteettomuuden seurannasta ja toimenpiteistä seurannan perusteella.

9.1.5 Yleisen tietosuoja-asetuksen mukainen sertifiointi

Yleisen tietosuoja-asetuksen 42 artiklan mukaan jäsenvaltiot, valvontaviranomaiset, tietosuojaneuvosto ja komissio kannustavat ottamaan käyttöön tietosuojaa koskevia sertifiointimekanismeja sekä tietosuojasinettejä ja -merkkejä erityisesti unionin tasolla, minkä tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat käsittelytoimia suorittaessaan yleistä tietosuoja-asetusta. Asetuksen artiklan 43 mukaan sertifioinnin myöntää ja uusii sertifiointielin, jolla on tietosuojaan liittyvä asianmukaisen tason asiantuntemus. Jäsenvaltioiden on säädettävä siitä, akkreditoiko nämä sertifiointielimet kansallinen valvontaviranomainen (tietosuojavaltuutettu) vai kansallinen akkreditointielin (FINAS) vaiko molemmat. Tietosuojalain (1050/2018) 14 §:n 4 momentin mukaan Suomessa tietosuojan sertifiointielinten akkreditointitehtävä on annettu

tietosuojavaltuutetulle.[132] Jos jäsenvaltio määrää, että valvontaviranomaisen on akkreditoitava sertifiointielimet, valvontaviranomaisen olisi vahvistettava akkreditointivaatimukset, muun muassa 43 artiklan 2 kohdassa täsmennetyt vaatimukset. Akkreditoinnissa vaatimukset tulevat standardista ISO/IEC 17065/2012, jota täydennetään valvontaviranomaisen vahvistamilla lisävaatimuksilla

Euroopan tietosuojaneuvoston sivuilla ei ole vielä tietoa sertifiointimekanismeista eikä tietosuojan sertifiointielimiä ole vielä hyväksytty Suomessakaan. Esimerkiksi rekisterinpitäjät voivat sertifioida tietoturvallisuuden hallintajärjestelmänsä tietosuojan hallintaa koskevan standardin ISO 27701 mukaisesti. (Standardi luotiin laajennukseksi ISO 27001:lle, joka koskee tietoturvan hallintaa.) Mutta sertifiointi ei ole (ainakaan vielä) yleisen tietosuoja-asetuksen mukainen sertifiointimekanismi. Toisaalta myöskään tietosuoja-asetuksen mukainen sertifiointi ei vähennä rekisterinpitäjän tai henkilötietojen käsittelijän vastuuta asetuksen noudattamisesta eikä se rajoita toimivaltaisten valvontaviranomaisten tehtäviä ja valtuuksia.

Tietosuoja-asetuksen 24 (1) artiklan nojalla rekisterinpitäjän on toteutettava riskiperusteisesti tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tietosuoja-asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa, joten rekisterinpitäjälle muodostuu tietosuoja-asetuksen nojalla velvollisuus arvioida teknisten ja organisatoristen suojatoimien (tietoturvallisuustoimenpiteiden) riittävyyttä. Rekisterinpitäjän on myös tietosuoja-asetuksen 5 (2) artiklan nojalla pystyttävä osoittamaan, että se on varmistanut henkilötietojen asianmukaisen turvallisuuden. Puolestaan tietosuoja-asetuksen 32 (1) artiklan nojalla rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Tietosuoja-asetus siten kohdentaa tietoturvallisuusvaatimusten toteuttamisen suunnittelu- ja toteuttamisvastuun rekisterinpitäjälle, jolloin tietoturvallisuuden arviointi on lähinnä rekisterinpitäjän toiminnalle tuotettavaa tietoa tietoturvallisuustoimenpiteiden riittävyydestä.

FINASin näkemyksen mukaan tietosuojan arviointitoimijoiden akkreditoinnissa tulisi Suomessa edetä akkreditointilaissa säädetyllä tavalla.

---

132 FINASin näkemyksen mukaan tietosuojan arviointitoimijoiden akkreditoinnissa tulisi Suomessa edetä akkreditointilaissa säädetyllä tavalla. Tähän liittyen Liikenne- ja viestintävirasto on tähdentänyt, että NLF-asetus ei koske kansallisen turvallisuuden piiriin liittyvää arviointitoimintaa, ja siten yllä olevat havainnot eivät päde tällaiseen arviointitoimintaan. Toisaalta on syytä huomata, että henkilötietojen käsittely, joka liittyy poliisiin, rajavartiolaitoksen ja puolustusvoimien tehtäviin kansallisen turvallisuuden alalla kuuluu henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018, rikosasioiden tietosuojalaki) piiriin eikä yleistä tietosuoja-asetusta siten sovelleta tähän.

9.1.6 EU:n kyberturvallisuusasetus

EU:n kyberturvallisuusasetus (EU) 2019/881[133] sisältää säännökset, joilla on luotu puitteet tieto- ja viestintäteknologiatuotteiden ja -palveluiden tietoturvasertifiointijärjestelmälle. Sertifioinnissa jokin tieto- ja viestintäteknologiatuote tai -palvelu saa sertifikaatin osoitukseksi kyseisen tuotteen tai palvelun tietoturvallisuudesta. Kyberturvallisuusasetus ei itsessään johda sertifikaatin olemassaoloon. Komissio julkaisee eurooppalaista kyberturvallisuussertifiointia koskevan unionin jatkuvan työohjelman, johon on sisällytettävä luettelo sellaisista tuotteista, palveluista ja prosesseista, joille voi olla hyötyä eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan kuulumisesta. Ensimmäinen unionin jatkuva työohjelma julkaistaan viimeistään 28 päivänä kesäkuuta 2020.

Sellaisia tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja varten voimassa olevat kansalliset kyberturvallisuuden sertifiointijärjestelmät ja niihin liittyvät menettelyt, jotka eivät kuulu jonkin eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän soveltamisalaan, pysyvät edelleen voimassa. Kyberturvallisuusasetus ei rajoita jäsenvaltioiden toimivaltaa sellaisten toimien osalta, jotka koskevat yleistä turvallisuutta, puolustusta, kansallista turvallisuutta tai yksittäisen valtion toimia rikosoikeuden alalla.

Kyberturvallisuusasetuksen 53 artiklan nojalla voidaan sallia, että vaatimustenmukaisuuden itsearviointi on yksinomaan tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien valmistajan tai tarjoajan vastuulla. Vaatimuksenmukaisuusilmoituksen lisäksi eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä kolmen varmuustason sertifikaatteja: perustason, korotetun tason ja korkean tason sertifikaatit. Perustason ja korotetun tason sertifikaatit myöntäisi pääsääntöisesti akkreditoidut ja viranomaisen valtuuttamat vaatimustenmukaisuuden arviointilaitokset. Hyödykkeiden valmistajat ja palveluntarjoajat hakisivat sertifiointia vaatimustenmukaisuuden arviointilaitoksilta. Arviointilaitoksen tulee täyttää asetuksessa ja sen liitteessä määritellyt vaatimukset.

Kyberturvallisuusasetuksen 58 artikla velvoittaa jäsenvaltiot kansallisen sertifiointiviranomaisen nimeämiseen. Kansallisten kyberturvallisuussertifioinnin myöntävien viranomaisten on tarkoitus vastata eurooppalaisen kyberturvallisuuden sertifiointijärjestelmien täytäntöönpanosta ja valvonnasta, ja siitä, että näiden järjestelmien mukaisesti myönnetyt sertifikaatit ovat voimassa ja tunnustettuja kaikkialla unionissa. 58 artiklassa säädetään kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen tehtävistä. Tiivistetysti

133 Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus).

kansallisen viranomaisen tehtäviin kuuluvat vaatimustenmukaisuusilmoitusten valvonta ja seuranta, vaatimustenmukaisuuden arviointilaitosten valtuuttaminen, valvonta ja seuranta sekä korkean tietoturvatason kyberturvallisuussertifikaattien myöntäminen.

Asetuksen 58 artiklan nojalla kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen on organisaatioltaan, rahoituspäätökseltään, oikeudelliselta rakenteeltaan ja päätöksenteoltaan oltava riippumaton yksiköistä, joita se valvoo. Kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen toiminnan, mikä liittyy korkean tason kyberturvallisuussertifikaattien myöntämiseen, tulee olla tiukasti erotettu saman viranomaisen valvontatoiminnasta.

Sähköisen viestinnän palveluista annetun lain 304 §:n mukaan Liikenne- ja viestintävirasto toimii asetuksen mukaisena kansallisena kyberturvallisuussertifioinnin viranomaisena.

Kyberturvallisuusasetuksen perusteella ei ole vielä hyväksytty yhtäkään sertifiointijärjestelmää, mutta valmisteilla on pilvipalveluihin ja asioiden internetiin (IoT, Internet of Things) liittyviä sertifiointijärjestelmiä. On odotettavissa, että kyberturvallisuusasetuksen merkitys tulee kasvamaan nykyisestään. Sekä ehdotus NIS2-direktiiviksi[134] että ehdotus asetukseksi harmonisoiduista säännöistä tekoälylle[135] sisältävät viittaukset kyberturvallisuusasetuksen mukaiseen vaatimustenmukaisuuden osoittamiseen. Näitä valmisteilla olevia säädösehdotuksia on kuvattu luvussa 10.

9.1.7 Erityislainsäädännön arviointivaatimuksista

Yleislainsäädännössä ei ole säädetty viranomaisille velvollisuutta hankkia todistusta tietojärjestelmän vaatimuksenmukaisuudesta taikka pyytää Liikenne- ja viestintävirastolta tai arviointilaitokselta tietojärjestelmänsä vaatimuksenmukaisuuden arviointia.

Erityislainsäädännössä on säädetty vaatimustenmukaisuuden arvioinnista. Asiakastietolain 19 d §:n mukaan laissa määriteltyyn luokkaan A kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava tietojärjestelmän valmistajan antamalla selvityksellä siitä, että järjestelmä täyttää kaikki toiminnallisuutta koskevat vaatimukset, hyväksytyllä yhteistestauksella ja tietoturvallisuuden arviointilaitoksen antamalla vaatimustenmukaisuustodistuksella. Terveyden ja hyvinvoinnin laitos voi antaa tarkempia määräyksiä

134 Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi COM (2020) 823 kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin (EU) 2016/1148 kumoamisesta

135 Ehdotus Euroopan parlamentin ja neuvoston asetukseksi tekoälyn eurooppalaisesta lähestymistavasta COM (2021) 206.

vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä. Luokkaan A kuuluvan tietojärjestelmän saa lain 19 f :n mukaan ottaa tuotantokäyttöön ja liittää Kanta-palveluihin, kun tietoturvallisuuden arviointilaitos on antanut sitä koskevan vaatimustenmukaisuustodistuksen. Sääntelyssä on syytä huomata, että asiakastietolaissa vaatimuksenmukaisuus tarkoittaa myös muuta kuin tietoturvallisuuden arviointia. Tästä syystä arviointilaitoslakia ei voida erityislainsäädännöstäkin johtuvista syistä kiinnittää pelkästään tietoturvallisuuden arviointiin.

Asiakastietolain uudistaminen on vastikään hyväksytty eduskunnassa (EV 71/2021 vp – HE 212/2020). Eduskunnan hyväksymän lain 35 §:n mukaan luokkaan A kuuluvan tietojärjestelmän ja hyvinvointisovelluksen vaatimustenmukaisuus on osoitettava sertifioinnilla eli tietojärjestelmäpalvelun tuottajan tai hyvinvointisovelluksen valmistajan antamalla selvityksellä siitä, että tietojärjestelmä tai hyvinvointisovellus täyttää käyttötarkoituksensa mukaiset toiminnallisuutta koskevat vaatimukset, hyväksytyllä yhteentoimivuuden testauksella ja 37 §:n mukaisella tietoturvallisuuden arviointilaitoksen antamalla tietoturvallisuuden arviointia koskevalla todistuksella.

Toisiolain 25 ja 26 §:n mukaan laissa tarkoitetun tietoturvallisen käyttöympäristön tietoturvallisuus on osoitettava arviointilain mukaisen tietoturvallisuuden arviointilaitoksen antamalla todistuksella. Tietoturvallisuuden arviointilaitos arvioi toisiolain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti palveluntarjoajan hakemuksesta, täyttääkö käyttöympäristö tietoturvallisuutta koskevat vaatimukset. Arviointiperusteina on käytettävä Tietolupaviranomaisen eli Terveyden ja hyvinvointilaitoksen yhteydessä toimivan Sosiaali- ja terveysalan tietolupaviranomaisen määräyksiä turvalliselle käyttöympäristölle asetettavista vaatimuksista. Arviointilaitoksen myöntämä todistus on voimassa enintään viisi vuotta.

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annettu laki (617/2009) sisältää vastaavasti sähköisten tunnistuspalvelujen tarjoamista koskevat tietojärjestelmän yhteen toimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset sekä säännökset vaatimuksenmukaisuuden arvioinnista.

9.2 Johtopäätökset ja kehittämistarpeet

9.2.1 Tietojärjestelmien vaatimuksenmukaisuuden arviointia koskevan sääntelyn soveltamisala

Arviointilain mukainen arviointi koskee viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta, mutta sääntelyä ei sovelleta sitovasti kuin valtionhallintoon. Arviointilaitoslain perusteella arviointilaitokset voivat arvioida arvioinnin kohteen

tietoturvallisuuden tasoa myös yleisemmin. Asiakastietolain mukainen arviointilain mukaan suoritettava arviointi ulottuu osittain myös muihin tietojärjestelmien olennaisten vaatimusten toteutumisen arviointiin. Vaatimustenmukaisuuden arviointia koskevat lait eivät koske automaattiseen päätöksentekoon käytettävien tietojärjestelmien olennaisten (muiden kuin tietoturvallisuusvaatimusten) arviointia. Toiminnan jatkuvuuden ja varautumisen vaatimukset ovat lainsäädännössä hyvin yleisellä tasolla eikä arviointilaeissa erikseen mainita toiminnan jatkuvuuden ja varautumisen vaatimusten arviointia.

Tietojärjestelmien vaatimuksenmukaisuuden arviointia koskevan sääntelyn soveltamisala – kehittämiskohteet

Tietoturvallisuus tavoitteena kattaa sekä tietojen että tietojärjestelmien saatavuuden, eheyden ja luottamuksellisuuden turvaamisen – kyseessä on siis varsin laajastikin tulkittavissa oleva käsite. Laajasti ottaen tietoturvallisuuden voidaan katsoa pitävän sisällään myös tietojärjestelmän käyttöön liittyvän jatkuvuuden ja varautumisen – eli saatavuuden.

On kuitenkin nähtävissä tarpeita myös tietojärjestelmien sellaistenkin ominaisuuksien/vaatimusten mukaisuuden arvioinnille, jotka eivät sisälly suoraan tietoturvallisuuteen – esimerkiksi automaattiseen päätöksentekoon liittyvien toiminnallisten vaatimusten mukaisuuden arviointi.

Tästä syystä kehittämiskohteena voidaan nähdä vaatimustenmukaisuuden arviointia koskevien lakien (arviointilaki ja arviointilaitoslaki) ulottaminen koskemaan nykyistä laajemmin tietojärjestelmiin kohdistuvien vaatimusten mukaisuuden arviointia.

Lain nimikkeiden lisäksi olisi tarkasteltava lakien soveltamisalaa, luetteloita, joissa viitataan käytettyihin arviointiperusteisiin sekä arviointilaitoksen hyväksyjää, hyväksymisperusteita (vs. arviointiperusteet), viranomaisarvioinnin suorittajaa sekä arviointilaitosten valvontaa koskevaa sääntelyä.

Vaihtoehtoisesti arviointilaitoslaki voitaisiin jättää ennalleen ja säätää arviointilaissa laajemmin viranomaisten tietojärjestelmien vaatimustenmukaisuuden (viranomaisen suorittamasta/viranomaisen johdolla suoritettavasta) arvioinnista.

Lakien soveltamisalan laajentaminen edellyttää, että arvioivalla viranomaisella sekä arviointilaitoksilla on pätevyys ja kyvykkyys arvioida uusiin arviointiperusteisiin sisältyvien vaatimusten mukaisuutta. Lisäksi pitää pystyä osoittamaan mahdollisten viranomaisen apunaan käyttämien henkilöiden pätevyys. Tältä osin myös asiakastietolain laajennuksen sisältöä ja käytäntöjä (tietojärjestelmien muiden olennaisten vaatimustenmukaisuuden arvioinnissa) tulisi tarkastella tarkemmin.

Jos arviointilakien soveltamisalaa laajennetaan tietoturvallisuuden (ml. jatkuvuuden ja varautumisen) ulkopuolelle, niin on myös ratkaistava, miltä osin ulkopuolinen taho voi arvioida esimerkiksi automaattiseen päätöksentekoon käytetyn tietojärjestelmän toiminnallisuuksia – etenkin siitä näkökulmasta, että arvioinnilla voitaisiin varmistaa tietojärjestelmän tuottamien lopputulemien eli päätösten virheettömyyttä. Tässä yhteydessä – erityisesti, jos arviointi säädetään joissain tilanteissa pakolliseksi – on myös arvioitava sitä, mikä lisäarvo järjestelmän päätöksentekosääntöjen ja lain mukaisen toimintalogiikan vaatimusten täyttymistä koskevalla ulkopuolisen tahon hyväksynnällä on. Viranomaisella on vastuu lain noudattamisesta ja siten siitä, että järjestelmän toimintalogiikka on lain mukainen. Viranomaisella on myös todennäköisesti paras asiantuntemus toimintalogiikan perusteena olevasta lainsäädännöstä sekä päätöksentekosääntöjen muodostamisesta lain perusteella. Virheet/epätarkkuudet päätöksentekosäännöissä johtavat myös virheisiin tietojärjestelmän tuottamassa lopputuloksessa, vaikka tekninen ohjelmointi olisikin tehty virheettömästi suhteessa päätöksentekosääntöihin. Päätöksentekosäännöistä johtuvia virheitä ei välttämättä ulkopuolinen arvioija pysty havaitsemaan – eikä viranomainen voi ulkoistaa sen virkavastuulle kuuluvien päätöksentekosääntöjen laatimista.

Mikäli sen sijaan tietojärjestelmälle asetetaan muita automaattisen päätöksentekoon liittyviä yleisempiä teknistoiminnallisia vaatimuksia, kuten esimerkiksi ohjelmiston suorituskykyyn tai koodin laatuun liittyviä vaatimuksia, voi näiden vaatimusten mukaisuutta todennäköisesti arvioida myös ulkopuolinen arvioija.

9.2.2 Vaatimustenmukaisuutta arvioivat viranomaiset

Arviointilain mukaan Liikenne- ja viestintävirasto on ainoa toimivaltainen viranomainen suorittamaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointia.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan ulkoministeriö toimii kansainvälisten tietoturvallisuusvelvoitteiden toteuttamisessa Suomen kansallisena turvallisuusviranomaisena. Määrätyt turvallisuusviranomaiset: puolustusministeriö, pääesikunta ja suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa sekä Viestintävirasto tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. Lain 5 §:n 2 momentin mukaan kansallinen turvallisuusviranomainen ja tehtävään määrätyt turvallisuusviranomaiset voivat sopia tietyn tehtävän tai tehtäväkokonaisuuden hoitamisesta toisen turvallisuusviranomaisen lukuun, jos järjestely on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti.

Turvallisuusselvityslain mukaan yritysturvallisuusselvityksen tekemisestä päättää suojelupoliisi, jollei asiasta päätä pääesikunta. Pääesikunta päättää yritysturvallisuusselvityksen tekemisestä yrityksestä, joka hoitaa tai jonka on tarkoitus hoitaa puolustusvoimien antamaa tehtävää, taikka yrityksestä, joka liittyy puolustusvoimien hankintoihin. Liikenne- ja viestintävirasto laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen. Turvallisuusselvityslain mukaan toimivaltaiset viranomaiset voivat yksittäistapauksessa sopia, että toinen viranomainen laatii turvallisuusselvityksen tai sen osan toisen viranomaisen sijasta taikka antaa niiden perusteella todistuksen.

Vaatimuksenmukaisuutta arvioivat viranomaiset – kehittämiskohteet

Liikenne- ja viestintäviraston tehtäväksi tietoturvallisuuden arviointiviranomaisena voitaisiin nykykäytäntöä vastaavasti säätää turvallisuusluokiteltujen (TL IV-TL I) tietojen käsittelyyn käytettyjen tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnin lisäksi (tai siihen sisältyvänä) myös toiminnan jatkuvuuden ja varautumisen vaatimustenmukaisuuden arviointi. Liikenne- ja viestintävirasto on ehdottanut, että sen arvioinnit sisältäisivät lisäksi arvioitavaan tietojärjestelmään liittyvän turvallisuusjohtamisen (hallinnollinen turvallisuus ja henkilöstöturvallisuus) arvioinnin.[136]

Mikäli viranomaisten tietojärjestelmiä arvioitaisiin yksinomaan arviointilain mukaisesti, aiheuttaisi tämä virastolle todennäköisesti lisäresurssitarpeita, jolloin voitaisiin säätää Liikenne- ja viestintävirastolle mahdollisuus käyttää apunaan yksityisiä henkilöitä (arvioija tms.), jotka täyttävät arvioijalle asetetut pätevyysvaatimukset.

Viranomaisen tietojärjestelmien tietoturvallisuuteen liittyvä fyysisen turvallisuuden arvioinnista voisi olla tarpeen säätää kansallisella tasolla. Tehtävä voitaisiin antaa esimerkiksi suojelupoliisille.

Puolustusvoimat on ehdottanut, että Puolustusvoimat olisi toimivaltainen arviointiviranomainen vastuualueenaan maanpuolustukseen liittyvien kansallista turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden (ml. jatkuvuus ja varautuminen) arviointi – sekä mahdollisesti fyysisen turvallisuuden arviointi. Tämä saattaisi edellyttää muutoksia myös turvallisuusselvityslakiin. Tältä osin mahdollisessa lainvalmistelussa on myös otettava huomioon objektiivisuus- ja

136 Lisäksi tulee arvioida, onko Liikenne- ja viestintäviraston arviointitoiminnan ohjauksesta syytä säätää tarkemmin. Arviointilain perusteluissa (HE 45/2011, s. 4) todetaan mm., että Liikenne- ja viestintäviraston ”tulosohjausta lakiehdotuksen mukaisissa uusissa tehtävissä [arviointilaitosten hyväksyntä ja arviointitoiminta] on tarkoitus toteuttaa valtiovarainministeriön ja liikenne- ja viestintäministeriön tiiviinä yhteistyönä”.

riippumattomuusnäkökulmat (esim. toimintojen organisatorinen erottaminen), sillä suurin hyöty arviosta on, että se tuottaa jäännösriskin hyväksyjälle ulkopuolisen arvion järjestelmän tilasta.

Lisäksi on harkittava, mikä viranomainen olisi toimivaltainen arvioimaan mahdollisia automaattisen päätöksentekoon liittyviä tietojärjestelmien olennaisia vaatimuksia. Tällekin viranomaiselle voitaisiin säätää mahdollisuus käyttää apunaan yksityisiä henkilöitä (arvioija tms.), jotka täyttävät arvioijalle asetetut pätevyysvaatimukset.

Tietosuojavaltuutetun ja mahdollisten sertifiointielinten rooli on myös otettava huomioon. Automaattisen päätöksenteon edellytyksistä säädetään myös yleisessä tietosuoja-asetuksessa, jonka noudattamista valvoo tietosuojavaltuutettu. Tietosuoja-asetuksessa ei kuitenkaan ole kytketty sertifiointia mitenkään erityisesti asetuksen automaattista päätöksentekoa koskeviin säännöksiin – ja toisaalta sertifiointi ei poista vastuuta asetuksessa säädetyn noudattamisesta. Jos vaatimustenmukaisuuden osoittaminen säädetään pakolliseksi, ei kuitenkaan ole kyse tietosuoja-asetuksen mukaisesta sertifioinnista.

9.2.3 Arviointilaitosten hyväksyminen, hyväksyjä ja valvonta

Arviointilaitoslain mukaan toimivaltaiset viranomaiset tietoturvallisuuden arviointilaitosten hyväksynnässä ovat FINAS (akkreditointi) ja Liikenne- ja viestintävirasto (hyväksyntä ja valvonta arviointilain mukaan). Lisäksi Liikenne- ja viestintäviraston on ennen tietoturvallisuuden arviointilaitoksen hyväksymistä varattava suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta.

Arviointilaitoslaissa säädetyt edellytykset arviointilaitoksen hyväksymiselle ovat hyvin yleisluontoiset. Tämä on johtanut siihen, että hyväksyntä perustuu suurelta osin Liikenne- ja viestintäviraston antamaan ohjeeseen tietoturvallisuuden arviointilaitoksille (Ohje 210/2016 O) – eli ei sitovaan normistoon. Hyväksymisen edellytykset on koettu jossain määrin tulkinnanvaraisiksi. Lisäksi turvallisuusluokitellun tiedon käsittelyn tietoturvallisuuden arviointilaitoksen pätevyyttä hakeneilla ei välttämättä ole prosessin alkuvaiheessa ollut riittävää ymmärrystä edellytettävästä osaamisesta ja tällaisen osaamisen hankkiminen (henkilöstö, laitteistot, ohjelmistot) on osoittautunut aikaa vieväksi. Nämä syyt ovat osaltaan johtaneet myös siihen, että arviointilaitoksen hyväksyntäprosessit ovat olleet pitkiä eikä uusia arviointilaitoksia ole tullut markkinoille. Nykytilanteen haasteena on myös, että nykyisten arviointilaitosten osaamisalueet eivät täysin vastaa viranomaisarvioinnilta (eli Liikenne- ja viestintäviraston tekemältä arvioinnilta) vaadittavaa sisältöä, ja arviointilaitosten pätevyysalueita on jouduttu hyväksymään osittaisina. Arviointilaitosten pätevyysalueet eivät kata esimerkiksi salausratkaisujen, yhdyskäytäväratkaisujen tai hajasäteilysuojausten riittävyyden arviointia kuin osittaisina ja rajauksin.

Arviointilaitosten hyväksymistä koskevat vaatimukset on arviointilaitoslaissa säädetty yleisellä tasolla siten, ettei niiden perusteella voida muodostaa selkeää kokonaiskäsitystä siitä, mitkä ovat konkreettisia vaatimuksia arviointilaitoksille.[137] Tältä osin sääntelyä voidaan pitää epätäsmällisenä, tulkinnanvaraisena ja puutteellisena. Sääntely jättää harkintavaltaa arviointilaitoksen hyväksyvälle viranomaiselle, jolloin tällaisten vaatimusten täyttämistä koskevat soveltamisohjeet voivat sisältää konkreettisia vaatimuksia, joiden tulisi olla lakitasoisia. Toisaalta tietojärjestelmien arvioinnissa vaatimuksenmukaisuuden todentaminen kohdentuu arvioinnin tekevän tarkastajan tai muun asiantuntijan ammatilliseen pätevyyteen, jolloin arvioinnin tekijän kelpoisuutta ei voida kohdentaa pelkästään yleisesti organisaatioon, vaan myös tosiasiassa arviointeja tekeviin henkilöihin.

Tietoturvallisuuden tai muiden tietojärjestelmää koskevien vaatimusten mukaisuuden arviointien kysynnän ennakoidaan kasvavan, joten yksityisiä hyväksyttyjä arviointilaitoksia tarvitaan jatkossa todennäköisesti enenevässä määrin.

Arviointilaitosten hyväksyminen (hyväksymiskriteerit ja -prosessi), hyväksyjä ja valvonta – kehittämiskohteet

Edellä esitetyistä syistä arviointilaitoslakia tulisi muuttaa siten, että siinä asetetaan sekä arviointilaitokselle että sen palveluksessa olevalle arvioitsijalle yksilöidyt vaatimukset, joita voidaan lakitasoiseen sääntelyyn perustuen valvoa. Lisäksi arviointilaitoslakia tulisi muuttaa siten, että eri viranomaistoimijoilla on selkeä ja perusteltu toimivalta päättää arviointilaitoksen hyväksynnästä ja suorittaa kelpoisuusvaatimusten noudattamista koskevaa valvontaa.

Mikäli arviointilaitoksia käytettäisiin viranomaisten tietojärjestelmien arviointiin, arviointilaitoslain sääntelykohde tulisi olla tietojärjestelmien arviointi tietoturvallisuuden arvioinnin sijaan tai lain soveltamista pitäisi ainakin selkeämmin laajentaa tietojärjestelmien arviointilaitostoimintaan. Jälkimmäistä puoltaa se seikka, että tietoturvallisuuden arviointi voi kohdistua laajemmin kuin tietojärjestelmään.

---

137 On syytä huomata, että myös akkreditointilaissa on jätetty akkreditoinnin vaatimukset yleiselle tasolle. Lain 6 §:ssä säädetään akkreditoinnin edellytyksistä seuraavasti: *Arviointielimen akkreditointiin sovelletaan yhdenmukaisia kansainvälisiä ja eurooppalaisia arviointiperusteita. Arviointiperusteiden käyttöönotosta päättää akkreditointiyksikkö kuultuaan akkreditointijärjestelmän ja vaatimustenmukaisuuden arviointipalvelujen kannalta keskeisiä tahoja. Akkreditoinnin edellytyksenä on, että arviointielimen organisaatio, henkilöstö, johtamis- ja laatujärjestelmä, sisäinen valvonta sekä vaatimustenmukaisuuden arviointipalvelu ovat asianmukaisia ottaen huomioon 1 momentin nojalla käyttöön otetut arviointiperusteet. Akkreditointiin rinnastettavassa pätevyyden arvioinnissa voidaan poiketa 1 ja 2 momentissa tarkoitetuista edellytyksistä, jos se on vaatimustenmukaisuuden arviointipalvelun laatu ja laajuus huomioon ottaen perusteltua.*

Arviointilaitoksen hyväksymismenettelyn lisäksi myös arvioinnin suorittamista koskevaa menettelysääntelyä tulisi tarkentaa. Jos sääntelyä laajennetaan uusille vaatimuksenmukaisuuden osa-alueille, tulisi harkita, että arviointilaitos voisi toimia pelkästään esimerkiksi tietoturvallisuuden arviointilaitoksena tai tietojärjestelmien arviointilaitoksena. Arviointilaitosten toimintaa erityisesti tietojärjestelmien olennaisten vaatimusten arvioinnissa on myös kehitettävä siten, että siinä huomioidaan perustuslain 124 §:ssä johdettavat sääntelyvaatimukset. Niin ikään arviointikohde on täsmennettävä siten, että viranomainen ei voisi ulkoistaa tietojärjestelmiensä kelpoisuuden arviointia kokonaisuudessaan yksityiselle, koska sillä on merkittävä vaikutus julkisen vallan käyttöön tietojärjestelmän toiminnallisuuksia käytettäessä esimerkiksi hallintoasiaan liittyvässä päätöksenteossa.

Tietojärjestelmien tietoturvallisuuteen keskittyville arviointilaitoksille voitaisiin (nykyisen käytännön mukaan) antaa pätevyysalueeksi arvioida turvallisuusluokan IV ja III sekä salassa pidettäviä ja julkisia tietoja käsittelevien tietojärjestelmien tietoturvallisuutta. Arviointilaitoksia hyväksyvälle taholle voitaisiin säätää velvollisuus pitää yllä lain soveltamisalaa vastaavaa kuvausta mahdollisista arviointilaitosten pätevyysalueista sekä pätevyysalueelle hyväksymisen vaatimuksista/kriteereistä.

Nykyiselle sääntelylle vaihtoehto voisi olla, että arviointilaitosten hyväksymistehtävä siirrettäisiin FINAS:ille. Arviointilaitoksen akkreditointi- ja hyväksyntäprosessin osana tietoturvallisuuden arviointilaitoksesta voitaisiin tehdä turvallisuusselvityslain mukainen yritysturvallisuusselvitys, jolla mm. varmistettaisiin arviointilaitoksen kyvykkyys asiakkaiden tietojen käsittelyssä, kuten salassa pidettävien tietojen suojaamisessa. Yritysturvallisuusselvitys korvaisi nykyisen Liikenne- ja viestintäviraston suorittaman arviointilaitoksen tietojenkäsittelyn turvallisuuden arvioinnin.

Kokonaisvastuun siirtämiseen FINAS:ille liittyy kuitenkin kysymys arviointilaitosten valvonnasta ja siihen käytettävistä resursseista. Arviointilaitosten hyväksyntäprosessia, hyväksyntävastuuta ja valvontaa sekä niihin käytettäviä resursseja koskevat kysymykset edellyttävä poliittista linjausta. Asiassa on otettava huomioon myös tietosuojavaltuutetun rooli. Edellä todetun lisäksi on otettava huomioon myös se että vaatimustenmukaisuuden arviointiin liittyvät asiat eivät saa sotkeutua arviointilaitosten hyväksyntään ja valvontaan. Merkittävät arviointilaitoksia hyväksyvien viranomaisten toimivaltuuksia koskevat muutokset eivät todennäköisesti ole mahdollisia hallituskaudella, mutta jatkovalmistelussa voidaan vielä arvioida mahdollisuutta muuttaa viranomaistoimivaltuuksia arviointilaitosten hyväksynnässä ja valvonnassa.

Viranomaisiin kohdistuvasta arviointilaitosjärjestelmästä luopuminen voi olla vaihtoehtoinen tapa lähestyä arviointilainsäädännön uudistamista. Tällöin viranomaisten tietojärjestelmien arvioinnit tehtäisiin (arviointilain mukaisena) viranomaistoimintana, jossa arviointiviranomainen voisi käyttää arvioinnissa apunaan yksityisiä määritetyn

ammattipätevyyden täyttäviä arvioijia. Tällöin arvioijat toimisivat arviointiviranomaisen lukuun ja valvonnassa. Asiasta pitäisi säätää perustuslain 124 §:ssä johtuvista syistä laissa, jolloin lainvalmistelussa on erikseen perusteltava, miksi julkinen hallintotehtävä on näissä yksittäisissä tarkastustilanteissa tarkoituksenmukaista antaa yksityisille. Tällaiseen arvioijajärjestelmään siirtyminen saattaa olla perusteltua, jos arviointikohteet edellyttävät hyvin laajasti erilaista osaamista esimerkiksi yleisesti tietoturvallisuudesta, tietosuojasta, eri toimialojen erityisvaatimuksista, tietojärjestelmien yleisistä olennaisista vaatimuksista ja toimialakohtaisista erityisistä olennaisista vaatimuksista. Koska arvioijat toimisivat arviointiviranomaisen lukuun, olisivat arvioinnissa käytettävät ja arvioinnissa tuotetut asiakirjat arviointiviranomaisen asiakirjoja. Tällaisessa mallissa kuitenkin rajautuisi arviointisääntelyn ulkopuolelle puhtaasti yksityisten yritysten tarpeet tietoturvallisuuden arvioinnille. Näitä arviointeja voitaisiin tehdä arviointilaitoslain perusteella. Liikenne- ja viestintävirasto tai muu viranomainen arvioinnista vastaavana viranomaisena olisi vastuussa myös yksityisten arvioijien riittävästä osaamisesta varmistumisesta sekä turvallisten työvälineiden ja toimitilojen tarjoamisesta yksityisille arvioijille. Näiden tehtävien aiheuttamat resurssitarpeet olisi otettava huomioon, vaikka varsinainen viranomaisen henkilökunnan toimesta suoritettava arviointitoiminta voitaisiin hoitaa nykyisin resurssein.

Tarvittaneen myös lisäedellytyksiä/pätevyysvaatimuksia arviointilaitoksille (ja arvioijille), mikäli arviointitoiminta laajennetaan koskemaan myös muita olennaisia vaatimuksia, kuten automaattiseen päätöksentekoon käytetyn tietojärjestelmän toiminnallisia vaatimuksia.

Arviointilaitoslaissa ei ole varauduttu tilanteeseen, jossa arviointilaitoksena toimivan yrityksen toiminta muuttuu esimerkiksi yritysoston tai toiminnan lakkaamisen kautta, jolloin arviointitoiminnassa kertyneet tiedot saattavat päätyä ennalta suunnittelemattomille tahoille. Vertailun vuoksi todettakoon, että eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annetussa laissa (278/2016) vastaavaan asiaan on varauduttu lain 6 §:n 4 momentin säännöksellä. Sen mukaan: ”Jos ilmoitettu laitos on lopettanut toimintansa tai sen hyväksyminen on peruutettu, on toimivaltaisen viranomaisen ryhdyttävä asianmukaisiin toimenpiteisiin sen varmistamiseksi, että laitoksen asiakirjat käsittelee toinen ilmoitettu laitos tai ne pidetään ilmoittamisesta ja markkinavalvonnasta vastaavien viranomaisten pyynnöstä näiden nähtävillä.” Turvallisuusselvityslain mukaisessa yritysturvallisuusselvitysprosessissa ja myönnettyyn selvitykseen liittyvässä valvontatoimessa on jo sisäänrakennettuna menettelyt laajemminkin ulkomaan sidonnaisuuksiin (FOCI, Foreign Ownership, Control or Influence) liittyvien riskien huomiointiin. Mikäli yritysturvallisuusselvitystä hyödynnettäisiin arviointilaitosten hyväksynnässä, tulisi kuitenkin täsmentää hallinnon yleislakien soveltamista ja soveltuvuutta arviointilaitostoimintaan esimerkiksi arkistointia koskevien vaatimusten osalta. Nykyisen sääntelyn perusteella voitaisiin päätyä päätelmään, jossa kaikkia hallinnon yleislakeja ei sovellettaisi arviointilaitosten toimintaan.

9.2.4 Vaatimustenmukaisuuden osoittaminen

Tietojärjestelmien tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimustenmukaisuuden arviointia ei ole säädetty yleislain tasolla pakolliseksi. Tiedonhallintalain 13 §:n 1 momentin mukaan tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan, mutta velvoitetta vaatimustenmukaisuuden arviointiin ei ole.

Vaatimustenmukaisuuden osoittaminen – kehittämiskohteet

On arvioitava, tulisiko tietoturvallisuusvaatimusten täyttymisen arviointi ja mahdollisesti tietojärjestelmien hyväksyntä säätää joissakin tilanteissa pakolliseksi (kuten asiakastietolaissa). Vaatimus ulkopuolisen arvioinnin tai todistuksen hankkimisesta voisi olla tarkoituksenmukaista säätää velvoittavaksi riskiarvioinnin perusteella niin, että se koskisi tietoturvallisuuden (korkeimmat turvallisuusluokat) tai esimerkiksi oikeusturvan (automaattinen päätöksenteko) taikka (jonkin tietyn toiminnan) jatkuvuuden kannalta kriittisimpiä järjestelmiä ja toimintoja. Nämä tulisi määritellä yksiselitteisesti laissa. Lisäksi olisi arvioitava velvoitetta säännöllisiin seuranta-arviointeihin. Tässä yhteydessä tulee arvioida myös velvoittavan sääntelyn kustannusvaikutuksia. Mahdollisesti laissa voitaisiin tuoda esille myös itsearviointi sekä kevyempi, konsultoiva tietojärjestelmien tarkastus, jonka voisi suorittaa muukin kuin arviointiviranomainen tai hyväksytty arviointilaitos.

Erityisesti yhteisiä tieto- ja viestintäteknisiä palveluja koskevia hyväksyntöjä palvelun tietoturvallisuuden tilasta olisi mahdollista laajemminkin hyödyntää siihen, että palveluja käyttävät tiedonhallintayksiköt voisivat helpommin arvioida palvelujen tietoturvallisuuden tasoa. Kun pääsääntöisesti hyväksyntää ja siihen liittyvää todistusta tietoturvallisuuden tilasta ei ole yhteisestä palvelusta saatavilla, on jokaisen tiedonhallintayksikön itse tehtävä päätös yhteisen palvelun käyttämiseen liittyvistä tietoturvallisuuden rajauksista. Tämä päätös joudutaan usein tekemään vajavaisin tiedoin tai puutteellisella osaamisella. Yhteisten palvelujen tuottajien tilaamia arviointeja koskevat arviointiraportit ovat käytännössä aina salassa pidettäviä ulkopuolisille eikä tiedonhallintayksiköillä siten ole välttämättä tiedonsaantimahdollisuutta raportteihin. Lisäksi voisi olla hyödyllistä muutoinkin edistää useiden tiedonhallintayksiköiden toimintaa palvelevien tietojärjestelmien/alihankkijoiden vaatimustenmukaisuuden arviointien tekemistä/teettämistä.

Vaatimustenmukaisuuden osoittaminen kuuluisi lähtökohtaisesti kussakin yleis- tai erityislaissa säädettäviin tietojärjestelmän käyttöä/käyttöönoton edellytyksiä koskeviin vaatimuksiin (kuten asiakastietolaissa). Lisäksi, mikäli säädetään tietojärjestelmän automaattiseen päätöksentekoon liittyvien vaatimusten arvioinnista, on harkittava:

- säädettäisiinkö ja missä määrin velvoitteeksi ulkopuolisen arvioijan (viranomainen tai arviointilaitos) suorittama arviointi ja hyväksyntä
- milloin taas riittäisi viranomaisen lakiin perustuva itsearviointi, testaus ja valvonta, mahdollinen konsultatiivinen arviointi, mahdollinen valmistajanvakuutus tms.

9.2.5 Tietoturvallisuutta ja tietojärjestelmiä (ja tietoliikennejärjestelyjä) koskevat vaatimukset (ja ns. arviointikriteeristöt)

Lainsäädännössä ei ole säädetty (olennaisista) vaatimuksista, jotka koskisivat hallinnon tietojärjestelmiä erityisesti, kun niillä tehdään etuja, oikeuksia ja velvollisuuksia koskevia päätöksiä tai ne muuten vaikuttavat suoraan hallinnon asiakkaan oikeudelliseen asemaan, kuten palveluihin pääsyyn. Erityisiä kriteereitä oikeusturvan ja hyvän hallinnon sekä virkavastuun vaatimukset toteuttaville tietojärjestelmille ei ole säädetty. Tällainen sääntely on tarpeellinen erityisesti tilanteissa, joissa asiankäsittely on pitkälle tai kokonaan automatisoitu.

Myöskään toiminnan jatkuvuudelle ja varautumiselle ei ole lakiin perustuvia yksityiskohtaisempia vaatimuksia. Tiedonhallintalaista näitä vaatimuksia olisi tosin johdettavissa. Toiminnan jatkuvuuden varmistaminen tunnistetaan vallitsevana kehityssuuntana. Se on keskeinen osa digitaalisen turvallisuuden kokonaisuutta ja tukee osaltaan tietoturvallisuuden toteutumista. Tietoturvallisuuden arviointeja on teetetty kumoutuneen tietoturvallisuusasetuksen (681/2010) perusteella tietoturvallisuuden korotetulle tai korkealle tasolle, jotta jatkuvuuden varmistamiseen liittyviä kontrolleja saataisiin mukaan arviointiin. On kuitenkin huomattava, etteivät turvallisuusluokittelu ja toiminnan jatkuvuuden varmistamisen vaatimukset riipu välttämättä toisistaan. Tietojärjestelmän eheys- tai käytettävyysvaatimukset voivat olla erittäin korkeita, vaikka siinä käsiteltävät tiedot olisivat julkisia (esimerkiksi valtioneuvoston kanslian hätätiedotusjärjestelmä, perustietovarantoja operoivat tietojärjestelmät ja viranomaisten voimassa oleviin koronarajoituksiin ja -ohjeistuksiin liittyvät sivustot).

Tietojärjestelmien tietoturvallisuuden vaatimustenmukaisuuden arvioinnissa hyödynnetään ”epävirallisia” kriteeristöjä, kuten kansallisen turvallisuusviranomaisen Katakri-kriteeristö, jonka Liikenne- ja viestintävirasto on arvioinut soveltuvan myös kansallisten

tietoturvallisuusvaatimusten arviointiin. Katakri on kansainvälisistä tietoturvavelvoitteista annettua lakia täsmentävä. Sitä käytetään nykyisin myös turvallisuusselvityslain mukaisissa kansallisissa ja kansainvälisissä arvioinneissa sekä turvallisuusluokiteltavia tietoja käsittelevien kansallisten tietojärjestelmien ja tietoliikenneratkaisujen arviointilain mukaisissa arvioinneissa. Kuitenkaan Katakri-kriteeristöä ei ole laadittu kansallisen tietoturvallisuusvaatimusten näkökulmasta eikä sen laadinnasta ole vastannut toimivaltainen viranomainen. Siten sitä ei voida pitää lähtökohtana tietoturvallisuusarvioinnille muissa kuin alkuperäisessä käyttökontekstissaan. Se ei sisällä salassa pidettävien tietojen eikä toiminnan jatkuvuuden hallinnan ja varautumisen arviointikriteerejä.

Arviointikriteereinä on käytetty myös VAHTI-ohjeita, joita ei ole enää päivitetty ja jotka eivät ole ajantasaisia. VAHTI-ohjeet eivät myöskään muodosta yhtenäistä kokonaisuutta, jonka varaan luotettava ja asianmukainen tietoturvallisuuden arviointi voitaisiin perustaa. VAHTI-ohjeet olivat pääosin valtionhallinnon käyttöön tarkoitettuja. Vanhentuneita VAHTI-ohjeita ja aiempia Katakri-versioita käytetään kuitenkin edelleen arvioinnissa. Asiaintilaa ei voida pitää tällä hetkellä hyvän hallinnon kannalta katsottuna asianmukaisena. Katakri-kriteeristön ja Vahti-ohjeiden soveltuvuus koko julkisen hallinnon käyttöön on rajallinen, koska kuntasektorilla turvallisuusluokittelua ei käytetä eikä Katakrin käytöstä kansallisten turvallisuusluokiteltujen tietojen käsittelyn vaatimusten arvioinnissa ole säädetty.

Nykytilanteessa tietoturvallisuuden vaatimukset/arviointiperusteet koetaan tulkinnanvaraisiksi. Sekä arviointilaitokset että arvioinnin kohteet ovat pyytäneet Liikenne- ja viestintävirastolta Katakri-kriteeristön tulkintoja. Liikenne- ja viestintävirastolle ei kuitenkaan ole säädetty ohjaus- tai valvontatoimivaltaa viranomaisia koskevien kansallisten tietoturvallisuusvaatimusten osalta. Toimintaympäristön muutosten takia nämä arviointiperusteiden tulkintaa tai toteutusten teknisiä yksityiskohtia koskevat linjaukset ja tulkinnat ovat myös olleet vain osin vakiintuneita. Henkilöiden vaihtuvuuden takia tulkinnoissa on myös henkilöriippuvuutta ja että yksittäiset arvioinnit hidastuvat, kun tulkintasuosituksia ei ole saatavilla riittävän nopeasti. Tulkintapyyntöjen on koettu hidastavan merkittävästi niin arviointilaitosten kuin arviointeja tilaavien viranomaisten ja yhteisöjen toimintaa. Palvelujen tuottajille ja käyttäjille arviointien venyminen jopa vuoden mittaiseksi voi aiheuttaa kohtuuttomia haittoja. Muuttuvien tulkintojen takia tietojärjestelmiin joudutaan myös tekemään teknisiä ja toiminnallisia muutoksia ja muutosten takia aiemmin tehdyt arvioinnin osat saatetaan joutua uusimaan.

Tietoturvallisuutta ja tietojärjestelmiä (ja tietoliikennejärjestelyjä) koskevat vaatimukset (ja ns. arviointikriteeristöt) – kehittämiskohteet

On arvioitava, mitä vaatimuksia vasten tietojärjestelmän vaatimustenmukaisuus arvioidaan. Tarvitaanko lakia alemman asteista sääntelyä arviointikriteereistä (esimerkiksi tiedonhallintalain vaatimusten täsmentäminen), jolloin arviointiperusteeksi arviointilakeihin tulisi selvyyden vuoksi lisätä myös tiedonhallintalautakunnan ohjeet/suositukset taikka määräykset (vaikkakin arviointiperusteena voidaan käyttää ”4) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietototurvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita”).

Tietoturvallisuuden vaatimusmäärittelyjen tulisi mahdollisuuksien mukaan perustua kansainvälisiin standardeihin (mm. ISO27001 – Tietoturvallisuuden hallinta, ISO22301 – Jatkuvuuden hallinta, ISO31000 – Riskienhallinta), joita on täydennetty kansallisilla erityisvaatimuksilla. Standardien suoraan (ja osin välilliseenkin) käyttöön liittyy kuitenkin ongelmia, jos ne on tarkoitettu sitovasti noudatettavaksi. Lainsäätäjä ei voi vaikuttaa standardien sisältöön, jolloin standardien sisältöä joudutaan joka tapauksessa arvioimaan kansallisin lainsäädäntötoimin. Standardien käyttöön liittyy myös merkittäviä tekijänoikeudellisia rajoitteita, jolloin niiden saatavuus ja hyödynnettävyys laajasti esimerkiksi julkisessa hallinnossa voi muodostaa erityisen ongelman, jos standardit ovat tosiasiassa sitovaa sääntelyä joko suoraan tai arviointikriteereinä esitettynä. Standardien hyödyntämistä arviointikriteereinäkin voi rajoittaa tekijänoikeudelliset syyt. Myös kielellisten oikeuksien toteutumisesta on huolehdittava siten kuin säädöksissä viitattavien standardien kielestä annetussa laissa (553/1989) säädetään.

Arviointia voi käytännössä olla haastavaa suorittaa yksinomaan säädöksiin sisältyvien melko yleisten vaatimusten perusteella – varsinkin, jollei ole toimivaltaisen viranomaisen yksityiskohtaisempia tulkintoja säännösten sisällöstä. Jotta päästäisiin eroon epävirallisten kriteeristöjen käytöstä vaatimustenmukaisuuden arvioinnissa, tiedonhallintalautakunta valmistelee parhaillaan julkisen hallinnon tietoturvallisuuden arviointikriteeristöä ottaen huomioon myös toiminnan varautumisen ja jatkuvuudenhallinnan asettamat vaatimukset. Tällainen arviointikriteeristö ei ole kuitenkaan sitova eikä sitä voida myöskään arviointien kautta muuttaa ikään kuin se olisi sitova esimerkiksi erilaisia kelpoisuuksia määriteltäessä tai todistuksia annettaessa.

Mikäli laaditaan sitovaa alemman asteista sääntelyä koskien tietojärjestelmien vaatimuksia, on myös arvioitava, mikä on mahdollisen alemman asteisen sääntelyn suhde kuntien itsehallintoon ja itsenäiseen asemaan. Se, että määräyksiä ei olisi pakko noudattaa muutoin kuin silloin, jos ottaa järjestelmän käyttöön, saattaisi olla hyväksyttävä peruste alemman asteiselle sääntelylle esim. kuntiakin koskien. Asiakastietolain mukaiset Terveyden ja hyvinvoinnin laitoksen määräykset koskevat myös kuntia ja Kansaneläkelaitosta.

Vaatimuksissa ja kriteeristöissä olisi huomioitava myös esimerkiksi toiminnan jatkuvuudenhallinta ja varautuminen sekä automaattiseen päätöksentekoon käytettävien tietojärjestelmien olennaiset vaatimukset (ks. jaksot 3 ja 4).

Vaatimuksia asetettaessa ja vaatimustenmukaisuuden osoittamista koskevassa sääntelyssä tulisi ottaa huomioon myös riskienhallinnan merkitys vaatimusten asettamisessa. Voidaan kysyä, tulisiko säätää (riskiarvion perusteella) sallituista poikkeamista.[138] Vai pitäisikö ennemminkin vaatimusten ja kriteeristöjen itsessään olla riskiarviointiin perustuen joustavia. Poikkeamien määrästä ja laadusta riippuen palvelu voitaisiin ottaa käyttöön tai sen käyttöä voitaisiin jatkaa ehdollisesti, jos näin on palvelun vaatimuksia koskevassa säädännössä todettu ja sallittu. Arvioinnin kohteena olevan organisaation mahdollisuuksia hyväksyä digitaalisen turvallisuuden ratkaisut riskienhallinnan keinoin tulisi edistää. Riskienhallintatoimenpiteiden toteuttamisen ja jäännösriskien hyväksyntämenettelyn kautta palvelun käyttöönotto voisi olla sallittua, jos tämä palvelun vaatimuksia koskevassa säädännössä on todettu ja sallittu. Riskienhallinnasta ei kuitenkaan saa muodostua menettelyä, jolla asianmukaiset vaatimukset ohitetaan.

9.2.6 Tietojärjestelmän vaatimustenmukaisuuden arviointiprosessi

Arviointilain mukaan Liikenne- ja viestintäviraston tehtävänä on viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden edistämiseksi ja varmistamiseksi arvioida viranomaisen pyynnöstä tämän määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimuksenmukaisuutta ja antaa pyynnöstä tietojärjestelmälle tai tietoliikennejärjestelylle sen hyväksymistä osoittava todistus. Pyynnön voi viranomaisen toimeksiannosta tehdä myös se, joka tekee viranomaisen lukuun hankintoja taikka tuottaa tietojenkäsittely- tai tietoliikennepalveluja taikka hoitaa niiden järjestämiseen liittyviä palvelutehtäviä. Lisäksi säädetään tiedonsaantioikeudesta arvioinnin suorittamiseksi sekä oikeudesta päästä tiloihin ja tietojärjestelmiin. Todistuksen osalta säädetään jälkiseurannasta sekä todistuksen peruuttamisen edellytyksistä.

138 Kansalliset arvioinnit nähdään perustelluksi pitää mahdollisimman yhtenevinä kansainvälisiin arviointeihin nähden. Mikäli kansallisten arviointien käytännöt eriytyisivät kansainvälisten arviointien käytännöistä, niin kansallisten arviointien hyödyntämis- ja hyväksilukemismahdollisuudet suoritettaessa kansainvälisiä arviointeja hankaloituisivat. Tämä johtaisi samojen tietojärjestelmäympäristöjen arviointitarpeeseen aina uudelleen jokaisen kansainvälisen tarpeen näkökulmasta. Tämä hidastaisi kansainvälisen tietoaineiston sähköisen käsittelyn aloittamista sekä aiheuttaisi myös lisäkustannuksia osin päällekkäisistä arvioinneista. Ulkoministeriö näkee, että pyrkimys esimerkiksi enemmän riskipohjaiseen, joustavampaan arviointiin on yhtenäistettäessä hankalampaa.

Arviointilaitoslain mukaan hyväksytty tietoturvallisuuden arviointilaitos antaa selvitysten ja tarkastuksen perusteella todistuksen, jos arvioitavan kohteen toimitilat ja toiminta on selvityksen perustana olleiden arviointiperusteiden mukainen. Laissa ei säädetä todistuksen voimassaolon jälkiseurannasta eikä peruuttamisesta.

Tietojärjestelmän vaatimustenmukaisuuden arviointiprosessi – kehittämiskohteet

Arviointilakien uudistamisen yhteydessä on myös harkittava, tulisiko vaatimustenmukaisuuden arviointiprosessia tarkentaa lainsäädännössä. On muun muassa harkittava, tulisiko arvioinnin tilaajaa koskevaa sääntelyä täsmentää silloin kun arviointia suoritetaan useaa viranomaista/viranomaisen käyttämää tietojärjestelmää koskevien vaatimusten mukaisuuden arvioimiseksi. Arviointien tilaamista koskevaa (arviointilain) sääntelyä tulisi todennäköisesti selkeyttää mm. yhteishankintayksiköiden ja hallinnon yhteisten tietojärjestelmien/tietojärjestelmäpalvelujen osalta.

On myös nähty puutteena, että tilaaja ei saa arviointiviranomaiselta tai -laitokselta riittävän nopeasti riittävän tarkkaa arvioita arvioinnin kustannuksista tai kestosta.

9.2.7 Vastuukysymykset vaatimustenmukaisuuden osoittamisesta ja tietojärjestelmän käytännön toiminnasta

Arviointilain mukaan sen, joka haluaa todistuksen tietojärjestelmän vaatimustenmukaisuudesta, on annettava sitoumus tietoturvallisuustason säilyttämisestä. Todistuksen saaneen on ilmoitettava Liikenne- ja viestintävirastolle sellaisista muutoksista, joilla on vaikutusta tietoturvallisuustasoon, sekä sallittava Liikenne- ja viestintävirastolle pääsy tietojärjestelmiin ja tietoliikennejärjestelyihin sen selvittämiseksi, täyttävätkö ne edelleen todistuksen mukaiset vaatimukset.

Muita vastuuseen viittaavia säännöksiä ei sisälly arviointilakiin tai arviointilaitoslakiin.

Virkavastuuta automatisoitujen prosessien kehittämisessä, käyttöönotossa sekä käytön seurannassa on käsitelty luvussa 7.

Vastuukysymykset toisaalta vaatimustenmukaisuuden osoittamisesta ja toisaalta tietojärjestelmän käytännön toiminnasta – kehittämiskohteet

Viranomainen vastaa päätöksentekoon käytetyn tietojärjestelmän toiminnasta ja päätöstensä lainmukaisuudesta. Vastuusta arviointiprosessissa (vastuu puutteiden ilmoittamisesta sekä mahdollisesta arvioijan vastuusta ym.) voitaneen säätää arviointia koskevassa säädännössä, mutta mahdollisesti tarvitaan muitakin yleisempiä vastuusäännöksiä, esim.

virkavastuun osalta sekä mahdollisesti erityisiä säännöksiä vastuunjakautumisesta (esim. vastaavia kuin asiakastietolaissa). Esimerkiksi voi olla syytä arvioida osavastuun kohdentamista lainsäädännössä myös tietojärjestelmän valmistajaan/tuottajaan.

10 Euroopan unionin valmisteilla oleva sääntely

10.1 EU:n tietoturva/kyberturvasääntelyhankkeet

Ehdotus direktiiviksi kyberturvallisuuden korkean tason varmistamiseksi EU:n alueella (NIS2-direktiivi)

Euroopan komissio antoi 16.12.2020 osana ns. EU:n kyberturvallisuuspakettia ehdotuksen direktiiviksi kyberturvallisuuden korkean tason varmistamiseksi EU:n alueella (jäljempänä NIS2-direktiivi) ja ehdotuksen direktiiviksi kriittisten toimijoiden häiriönsietokyvystä. Ehdotus NIS2-direktiiviksi pohjautuu ensimmäiseen EU:n laajuiseen säädösinstrumenttiin, verkko- ja tieto-turvadirektiiviin (EU) 2016/1148, NIS-direktiivi), jonka tavoitteena oli kehittää EU:n yhteistä kyberturvallisuuden tasoa. Ehdotuksesta NIS2-direktiiviksi on tiedotettu eduskuntaa valtioneuvoston kirjelmällä U 9/2021 vp.

Ensimmäisen NIS-direktiivin mukaan jäsenvaltiot olivat vastuussa toimijoiden identifioinnista keskeisiksi palveluntarjoajiksi. Uuden direktiiviehdotuksen mukaan jäsenvaltioiden ei tarvitsisi enää kansallisesti tunnistaa keskeisiä toimijoita, koska kriteerejä yhdenmukaistettaisiin koko EU:n laajuisesti siten, että kaikki kriittisten sektoreiden suuret ja keskisuuret toimijat olisivat jokaisen jäsenmaan osalta sääntelyn piirissä. Toimijoiden kategorisointi jaettaisiin ehdotuksen mukaan keskeisiin (essential) ja tärkeisiin (important) riippuen toimijan kriittisyydestä ja keskinäisriippuvuudesta muihin sektoreihin ja toimijoihin. Sekä keskeisiin että tärkeisiin kategorioihin kuuluviin toimijoihin sovellettaisiin samoja riskienhallinta- ja raportointivelvollisuuksia. Kuitenkin valvonta- ja seuraamusjärjestelmät olisivat tiukempia keskeisten toimijoiden kuin tärkeiden osalta. Aiemmassa direktiivissä ei tehty eroja kriittisten toimijoiden välillä.

Ehdotuksen mukaan direktiivin soveltamisalaa laajennettaisiin aiemmasta soveltamisalan laajuudesta koskemaan eräitä keskeisiä sektoreita. Uutena keskeisenä sektorina direktiivin soveltamisalaan tulisi myös julkishallinto, kuten keskushallinnon toimijat sekä alueelliset hallinnot sellaisina kuin ne on määritelty asetuksessa (EU) 1059/2003 liitteessä I esitettyjen luokitustasojen NUTS 1 ja NUTS 2 tavalla. Asetuksen (EU) 1059/2003 liitteiden II ja III mukaan luokitustasot koskettaisivat Suomessa valtionhallintoa ja sen alaisia valtakunnallisia virastoja ja laitoksia sekä maakuntia ja kuntia. Ehdotuksen 4 artiklan 23 kohdan mukaan ne julkishallinnon toimijat, jotka toimivat yleisen turvallisuuden, lainvalvonnan, puolustuksen ja kansallisen turvallisuuden aloilla eivät lukeudu soveltamisalaan. Lisäksi

direktiiviehdotuksen 2 artiklan 3 kohdan mukaisesti direktiivi ei vaikuta jäsenvaltioiden toimivaltaan, joka koskee yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden ylläpitämistä. Direktiivin soveltamisalan laajeneminen julkishallintoon on keskeistä viranomaisten tietojärjestelmiä koskevan kansallisen lainsäädännön osalta. Direktiivin vaikutuksia julkishallinnon toimintaan tulee täsmentää jatkossa.

Jäsenvaltioiden tasolla ehdotus sisältää toimia, joiden tavoitteena on kehittää valmiuksia korkean kyberturvallisuuden tason varmistamiseksi. Komission uuden ehdotuksen mukaan jäsenvaltioiden tulisi laatia kansalliset kyberturvallisuusstrategiat, vahvistaa valvovien viranomaisten valvontatehtäviä ja toimijoiden tulisi lisäksi ottaa käyttöön ehdotuksessa esitettyjä riskienhallintatoimia. Ensimmäinen NIS-direktiivi loi pohjan kyberturvallisuusvalmiuksien kehittämiselle edellyttämällä jäsenvaltioita laatimaan kansalliset tietoturvastrategiat ja edellyttämällä keskeisiltä palveluntarjoajilta tietoturvallisuusvelvoitteiden noudattamista.

Ehdotus asettaisi uutena elementtinä toimintatavat *haavoittuvuuksien tunnistamiselle,* jossa CSIRT-toimija (computer security incident response teams) toimisi koordinoivana tahona. Ehdotuksen mukaan toimijan haavoittuvuuksista tulisi ilmoittaa CSIRT-toimijalle, jotta nämä haavoittuvuudet voitaisiin korjata. Haavoittuvuuksien tunnistamiseksi jäsenvaltioiden tulisi tarkastella ja asettaa tarvittavia toimintalinjauksia. Lisäksi jäsenvaltioiden tulisi *perustaa toimintalinjaukset laajamittaisten kyberturvallisuusriskien* varalle. Jokaisen jäsenvaltion tulisi tunnistaa valmiudet, resurssit ja prosessit, jotka voidaan käynnistää ja ottaa käyttöön ehdotuksen mukaisissa tilanteissa. Jäsenvaltioiden tulisi määrittää yksi tai useampi valvova viranomainen, joka olisi vastuussa laajamittaisten kyberturvallisuushäiriöiden ja -kriisien operatiivisesta johtamisesta.

Riskienhallintatoimenpiteiden tulisi sisältää toimet, joilla voidaan tunnistaa riskit mahdollisiin häiriöihin sekä tunnistaa ja käsitellä näitä ja lieventää niiden vaikutuksia. Näitä toimia olisi ehdotuksen mukaan muun muassa riskianalyysit ja tietojärjestelmien turvallisuustoimet, häiriöiden käsittely, liiketoiminnan jatkuvuus ja kriisinhallinta, tuotantoketjujen kyberturvallisuus, kyberturvallisuus verkko- ja tietojärjestelmien hankinnoissa sekä niiden kehityksessä ja ylläpidossa. Komissio esittää ehdotuksessaan, että kyberturvallisuuden riskienhallintavelvoitteiden tulisi olla suhteessa kunkin toimijan kohdalla arvioituihin riskeihin. Ehdotus laajentaisi riskienhallintatoimia koskettamaan myös toimijoiden tuotantoketjuja.

Ehdotus asettaisi kaksiportaisen *raportoinnin* nopean tiedonkulun sekä syvällisemmän raportoinnin varmistamiseksi. Toimijoiden tulisi raportoida valvovalle viranomaiselle ensimmäisen kerran 24 tunnin kuluessa siitä, kun merkittäväksi arvioitu häiriö tai kyberloukkauksen uhka on tullut toimijan tietoon. Tämän jälkeen toimijan tulisi toimittaa valvovalle viranomaiselle loppuraportti kuukauden kuluessa häiriöstä. Ehdotuksen mukaan

jäsenvaltiot voivat vaatia toimijoita *sertifioimaan* tietyt ICT-tuotteet, -palvelut ja -prosessit perustuen Euroopan kyberturvallisuussertifiointijärjestelmiin kyberturvallisuusasetuksen (2019/881) 49 artiklan nojalla. Komissio voisi myös pyytää Euroopan unionin kyberturvallisuusvirasto ENISAa valmistelemaan vaihtoehtoisen sertifiointijärjestelmän, mikäli tähän tarkoitukseen ei löytyisi sopivaa sertifiointijärjestelmää. Kuten ensimmäisessä NIS-direktiivissä, myös tämän ehdotuksen mukaan tulisi kannustaa jäsenvaltioita hyödyntämään EU:ssa ja kansainvälisesti hyväksyttyjä verkko- ja tietojärjestelmästandardeja.

Ehdotus direktiiviksi kriittisten toimijoiden häiriönsietokyvystä (CER-direktiivi)

Direktiiviehdotuksen tarkoituksena on parantaa välttämättömien palvelujen tarjontaa sisämarkkinoilla keskittymällä toimiin, jotka sekä ylläpitävät että parantavat yhteiskuntien kannalta kriittisten toimijoiden häiriönsietokykyä. Toimet kattavat monia aloja, ja niillä pyritään puuttumaan nykyisiin ja tuleviin verkossa ja sen ulkopuolella esiintyviin riskeihin johdonmukaisella ja toisiaan täydentävällä tavalla.

Direktiiviehdotuksen soveltamisala koskee kymmentä sektoria: energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveydenhuolto, juomavesi, jätevesi, digitaalinen infrastruktuuri, julkishallinto ja avaruus. Direktiivillä tavoitellaan keinovalikoiman laajentamista pelkistä suojaustoimista elintärkeiden toimintojen jatkuvuudenhallintaa kehittäviin toimiin. Suojaustoimien ohella keskeisiksi toimiksi on nostettu mm. riskienhallinta ja toipumiskyky häiriöistä.

Direktiiviehdotus edellyttää jäsenvaltioiden tunnistavan sektorikohtaiset elintärkeät toiminnot ja nimeävän niitä tarjoavat kriittiset toimijat yhteisten eurooppalaisten kriteerien ja kansallisen riskiarvion pohjalta. Jäsenvaltioilta myös edellytetään kansallista strategiaa kriittisten toimijoiden häiriönsietokyvyn vahvistamiseksi. Jäsenvaltioiden tunnistamilta kriittisiltä toimijoilta direktiivi edellyttää puolestaan omien riskiarvioiden ja kriisinkestävyyssuunnitelmien laadintaa.

Direktiivin mukaan jäsenvaltioiden on tunnistettava täsmällisesti kriittiset toimijat direktiivin määrittämillä toimialoilla. Artikla määrittää identifiointiprosessissa huomioon otettavia seikkoja, kuten esimerkiksi sen, että jäsenvaltioiden on ylläpidettävä ajantasaista luetteloa kansallisesti tunnistetuista, direktiivin mukaisista kriittisistä palveluista ja niihin liittyvistä toimijoista. Samoin jäsenvaltioita edellytetään informoimaan toimijoille asetetuista direktiivin edellyttämistä velvoitteista. Direktiivi asettaa jäsenvaltioille velvollisuuden ilmoittaa komissiolle merkittävästä kriittisen toimijan häiriötilanteesta.

Kriittisten toimijoiden on säännöllisesti arvioitava tunnistetut ja merkittävät riskit toimialallaan huomioiden kansallinen riskiarvio ja muut asiaankuuluvat tietolähteet. Direktiivissä säädetään toimijoiden toteuttamista teknisistä ja organisatorisista toimenpiteistä

kriisinkestävyyden parantamiseksi, sisältäen raportointivelvoitteet ja komissiolle myönnettävän oikeuden antaa täytäntöönpanosäädöksiä. Kriittisillä toimijoilla olisi oikeus pyytää turvallisuusselvityksiä henkilöstöstään, jotka työskentelevät sensitiivisissä tehtävissä tai joita harkitaan rekrytoitavaksi näihin tehtäviin. Direktiivissä säädetään jäsenvaltioiden tasolla toteutettavasta järjestelystä, jolla varmistetaan, että kriittiset toimijat ilmoittavat viipymättä toimivaltaiselle viranomaiselle merkittävistä häiriötilanteista tai tilanteista, jotka saattavat eskaloitua merkittäväksi häiriötilanteeksi. Lisäksi direktiivissä säädetään erityisen merkittävien eurooppalaisten kriittisten toimijoiden tunnistamisesta ja niiden suojaukseen liittyvistä toimenpiteistä.

10.2 EU:n asetusehdotus tekoälystä

10.2.1 Soveltamisala ja määritelmät

Euroopan komissio antoi ehdotuksen asetukseksi harmonisoiduista säännöistä tekoälylle 21.4.2021. Asetusehdotuksen tavoitteena on muodostaa EU:sta tekoälyn kehittämiselle ja soveltamiselle suotuisa ympäristö, joka edistää investointeja ja vahvistaa yritysten kansainvälistä kilpailukykyä. Asetusehdotuksen tavoitteena on lisäksi vahvistaa EU:ta turvallisena, luotettavana, ihmiskeskeistä ja -oikeuksia kunnioittavana toimintaympäristönä. Asetus on suoraan sovellettavissa EU:n jäsenvaltioissa, mutta asetuksen myötä luotavat uudet menettelyt ja viranomaistehtävät voivat luoda tarpeen sovittaa yhteen kansallista sääntelyä asetuksen kanssa. Asetusehdotuksesta on tiedotettu eduskuntaa valtioneuvoston kirjelmällä (U 28/2021 vp).

Asetus koskisi tekoälyjärjestelmän markkinoille asettamista, käyttöön ottoa sekä käyttämistä EU:ssa ja sitä sovellettaisiin yksityisen ja julkisen sektorin toimijoihin sekä EU:n toimielimiin. Komission mukaan asetuksen on tarkoitus kattaa kaikenlaiset tekoälyjärjestelmät, ja tekoälyjärjestelmän määritelmän on tarkoitus olla mahdollisimman neutraali. Asetusehdotuksen 3(1) artiklassa tekoälyjärjestelmä määritellään seuraavasti:

'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

Tekoälyn määritelmä on sidonnainen liitteessä I mainittuihin tekoälytekniikoihin. Komission mahdollista muuttaa liitettä I tekoälytekniikoista delegoitujen säädösten avulla, jotta asetuksessa voidaan huomioida tekoälyn kehitys tulevaisuudessa. Liitteen I b-kategoria logiikka- ja tietopohjaisista tekniikoista voi olla merkityksellinen myös julkisella sektorilla käytettävien tietojärjestelmien osalta:

Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems

Tekoälyjärjestelmän määritelmää on tarpeen selventää asetusehdotuksen jatkokäsittelyssä, jotta vaikutuksia julkisen hallinnon toimintaan pystytään edelleen arvioimaan. Nykyisen asetusehdotuksen perustella ei voida vielä selkeästi arvioida esimerkiksi sitä, millä tavalla asetusehdotus koskee sääntöpohjaista hallintoautomaatiota ja erilaisia laskenta-algoritmeja, joita viranomaisissa jo laajalti käytetään esimerkiksi valvontatehtävien ja päätöksenteon tukena.

10.2.2 Korkean riskin tekoälyjärjestelmät

Asetusehdotuksessa tekoälyjärjestelmät luokitellaan eri riskikategorioihin:

1. Kielletyt tekoälyn käyttötavat;
2. Korkean riskin tekoälyjärjestelmät;
3. Tekoälyjärjestelmät, joita koskevat läpinäkyvyysvaatimukset; ja
4. Vähäisen tai olemattoman riskin tekoälyjärjestelmät.

Korkean riskin tekoälyjärjestelmät on määritelty artiklassa 6 sekä liitteissä II ja III. Komission on mahdollista muuttaa liitettä III delegoitujen säädösten avulla tekoälyjärjestelmien lisäämiseksi korkean riskin kategoriaan. Delegoitujen säädösten tarkoituksena varmistaa, että tekoälyn käytön kehitys voitaisiin huomioida. Delegoitujen säädösten avulla voidaan myös laajentaa asetusehdotuksen ulottuvuutta korkean riskin tekoälyjärjestelmien osalta.

Liitteen III mukaan korkean riskin kategoriaan kuuluu monia tekoälyjärjestelmiä, jotka ovat merkityksellisiä julkisen sektorin kannalta. Kyseiseen kategoriaan kuuluvat muun muassa tekoälyjärjestelmät, jotka koskevat julkisen hallinnon palveluiden ja etuuksien käyttöä. Tällaisten tekoälyjärjestelmien avulla voidaan arvioida henkilön kelpoisuutta saada sosiaalisia etuuksia ja palveluita, tai myöntää tai hylätä pääsy etuuksiin tai palveluihin. Edelleen korkean riskin tekoälyjärjestelmiksi luokitellaan järjestelmät, joiden avulla voidaan päättää pääsystä koulutuslaitoksiin, rekrytoida tai valikoida työhön henkilöitä tai käsitellä turvapaikka-, viisumi- ja oleskelulupahakemuksia ja näihin liittyviä valituksia. Tekoälyjärjestelmillä on muun muassa mahdollisuus todentaa matkustusasiakirjojen aitous. Korkean riskin kategoriaan kuuluvat myös oikeuslaitoksessa ja demokraattisissa prosesseissa käytettävät järjestelmät, kuten tosiseikkojen selvittämisessä ja lain tulkinnassa ja soveltamisessa

käytettävät järjestelmät. Näin ollen korkean riskin tekoälyjärjestelmillä voidaan tehdä hallintopäätöksiä ja niitä voidaan käyttää tosiasiallisessa hallintotoiminnassa, hallintopäätösten valmistelevissa toimissa ja muussa asian selvittämisessä.

Asetusehdotuksella olisi mahdollisesti vaikutuksia kansallisten viranomaisten, kuten Kansaneläkelaitoksen, Rajavartiolaitoksen ja Maahanmuuttoviraston, toiminnassa käytettäviin tekoälyjärjestelmiin. Julkisen hallinnon alaan kuuluvia tehtäviä, joissa käytetään korkean riskin tekoälyjärjestelmiä, koskevaa ehdotettua sääntelyä tulee kuitenkin selkeyttää ja tarkentaa asetusehdotuksen jatkokäsittelyssä. Asetusehdotus jättää avoimeksi esimerkiksi sen, miltä osin verotusmenettely kuuluu korkean riskin tekoälyjärjestelmiin. Jatkossa tulee myös täsmentää, miltä osin sääntely tulisi koskemaan viranomaisten käytössä olevia tekoälyä käyttäviä neuvonta- ja tukijärjestelmiä, kuten keskustelurobotteja (chatbotteja), joiden toiminnassa hyödynnetään liitteessä I mainittuja teknologioita, ja jotka voivat toimia jonkin liitteessä III määritellyn käyttötarkoituksen neuvonta- ja tukipalveluna. Yhtenä esimerkkinä tästä on Kansaneläkelaitoksen keskustelurobotti, joka käyttää koneoppimista kirjoitetun kielen ymmärtämiseen, ja joka neuvoo asiakkaita sosiaalietuuksien hakemisessa.

10.2.3 Korkean riskin tekoälyjärjestelmiä koskevat vaatimukset

Asetusehdotuksen artikloissa 9–15 korkean riskin tekoälyjärjestelmille asetetaan erityisiä vaatimuksia. Tekoälyjärjestelmän suunniteltu käyttötarkoitus tulee ottaa huomioon varmistaessa, että tekoälyjärjestelmä vastaa asetuksen vaatimuksia. Tekoälyjärjestelmiä varten on otettava käyttöön *riskinhallintajärjestelmä*, joka on käytössä järjestelmän koko elinkaaren ajan. Riskinhallintajärjestelmässä on tunnistettava tekoälyn asianmukaisesta käytöstä tai ennakoitavissa olevasta väärinkäytöstä aiheutuvat mahdolliset riskit ja suunniteltava näiden riskien hallinta sekä minimointi. Sopivia riskienhallintatoimenpiteitä määriteltäessä on muun muassa varmistettava, että riskejä vähennetään tekoälyjärjestelmän riittävän suunnittelun avulla. Riskinhallintajärjestelmään kuuluu asianmukainen ja riittävä testaaminen, jotta sopivimmat riskinhallintatoimenpiteet voidaan tunnistaa ennalta sekä varmistaa, että tekoälyjärjestelmä vastaa asetuksen vaatimuksia. Testaus tulee suorittaa viimeistään ennen tekoälyjärjestelmän markkinoille asettamista tai käyttöönottoa.

Lisäksi korkean riskin tekoälyjärjestelmiä varten on otettava käyttöön *datanhallintatoimenpiteitä*, joilla varmistetaan järjestelmien koulutuksessa, validoinnissa ja testauksessa käytettävän datan laatu. Datanhallintatoimenpiteet koostuvat esimerkiksi järjestelmän suunnittelusta, datan keräämisestä ja esikäsittelystä sekä datassa olevien mahdollisten poikkeaminen (bias) tutkimisesta. Koulutus-, validointi- ja testausdataan tulee soveltaa sopivia datanhallintatoimenpiteitä. Asetusehdotuksen mukaan koulutukseen, validointiin

ja testaamiseen käytettävän datan on oltava asianmukaista, edustavaa, virheetöntä ja kattavaa. Datan on otettava huomioon maantieteelliset, käyttäytymiseen liittyvät tai muut käyttöpaikkaan liittyvät erityisominaisuudet.

Ennen korkean riskin tekoälyjärjestelmän markkinoille asettamista tai käyttöön ottoa on varmistettava järjestelmän riittävä *tekninen dokumentaatio*, jolla osoitetaan se, että järjestelmä vastaa asetuksen vaatimuksia. Tekninen dokumentaatio tulee pitää ajantasaisena. Teknisen dokumentaation tarkemmat vähimmäisvaatimukset on kuvattu asetuksen liitteessä IV. Tekoälyjärjestelmiä varten tulee perustaa *lokijärjestelmä*, joka vastaa yleisiä standardeja ja jonka avulla voidaan seurata ja jäljittää tekoälyjärjestelmän toimintaa. Tekoälyjärjestelmä on suunniteltava niin, että se on riittävän *läpinäkyvä* järjestelmän käyttäjille, jotta he voivat ymmärtää järjestelmän toimintaa ja käyttää sitä oikein. Tekoälyjärjestelmän mukana on toimitettava kattavat ja selkeät *käyttöohjeet*, joissa tulee mainita muun muassa tekoälyjärjestelmän keskeisimmät ominaisuudet.

Tekoälyjärjestelmä on suunniteltava ja kehitettävä niin, että ihminen voi tehokkaasti valvoa järjestelmää sen käytön aikana. *Ihmisvalvonnan* tarkoituksena on oltava minimoida käytöstä aiheutuvat haitat ja riskit. Ihmisvalvojan pitää voida havaita järjestelmässä aiheutuvat virheet, vääristymät tai poikkeamat, sekä tarvittaessa puuttua järjestelmän toimintaan tai pysäyttää se kokonaan. Henkilöllä on oltava valvonnan suorittamiseen tarvittava pätevyys.

Tekoälyjärjestelmät on suunniteltava niin, että ne toimivat riittävällä *tarkkuuden tasolla*. Järjestelmien tulee olla myös *viansietokykyisiä*, jotta järjestelmä pystyy torjumaan järjestelmässä tai sen toimintaympäristössä tapahtuvia virheitä. Jos tekoälyjärjestelmä pystyy jatkamaan oppimista markkinoille asettamisen jälkeen, mahdolliset järjestelmän tuottamat poikkeamat (bias) tuloksissa tulee pystyä estämään. Lisäksi tulee varmistaa tekoälyjärjestelmien *kyberturvallisuus* teknisillä toimenpiteillä. Järjestelmien tulee pystyä estämään kolmansien osapuolten yritykset muuttaa järjestelmän käyttöä tai suorituskykyä hyväksikäyttäen järjestelmän haavoittuvaisuuksia.

Asetusehdotuksen sääntely voi olla osittain päällekkäistä kansallista tietojärjestelmien toimintaa koskevan sääntelyn kanssa. Suomessa tietojärjestelmien toimintaan kohdistuu hallintolain mukaiset hyvän hallinnon perusteet, jotka velvoittavat viranomaiset järjestämään tiedonhallintansa asianmukaisesti. Tehokas tiedonhallinta edistää myös viranomaisen toiminnan tuloksellisuutta, mikä kuuluu myös hyvän hallinnon perusteisiin. Hallintolaissa asetetaan myös vaatimuksia asiankäsittelymenettelylle, jotka koskevat muun muassa hallintoasian vireilletuloa, käsittelyyn kohdistuvia vaatimuksia, hallintoasian selvittämistä ja ratkaisuntekoa.

Uudet vaatimukset voivat luoda uusia sääntelytarpeita viranomaisten toimintaan, sillä kansallinen sääntely ja unionin sääntely voivat perustua erilaisiin lähestymistapoihin, soveltamisaloihin ja määritelmiin, vaikka niiden tavoitteet olisivatkin lopulta samat. Valtioneuvoston kirjelmässä todetaankin, että asetusehdotuksen valmistelussa tulisi huolehtia, ettei asetuksesta synny julkisen sektorin toimijoille tarpeetonta sääntelytaakkaa (U 28/2021 vp, s. 23).

10.2.4 Viranomaisen roolit asetusehdotuksen näkökulmasta

Asetusehdotuksessa asetetaan velvollisuuksia korkean riskin tekoälyjärjestelmien tuotantoketjuun kuuluville tahoille sekä järjestelmien käyttäjille. Velvollisuudet kohdistuvat tekoälyjärjestelmien maahantuojiin, jakelijoihin, kolmansiin osapuoliin sekä unionin ulkopuolelle sijoittuneisiin palveluntarjoajiin.

Velvollisuudet kohdistuvat ensinnäkin tekoälyjärjestelmien *tarjoajiin* (provider), jolla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista tai muuta tahoa, joka kehittää tekoälyjärjestelmän tai jonka tavoitteena on asettaa kehitetty tekoälyjärjestelmä markkinoille tai ottaa se käyttöön omissa nimissään. Asetusehdotuksen mukaan korkean riskin tekoälyjärjestelmien tarjoajien on huolehdittava, että tekoälyjärjestelmät ovat vaatimusten mukaisia ja niiden käytössä on laadunhallintajärjestelmä. Tarjoajien on myös laadittava korkean riskin tekoälyjärjestelmän tekninen dokumentaatio, huolehdittava testausmenettelyistä sekä asianmukaisesta vaatimustenmukaisuuden arviointimenettelystä ennen tekoälyjärjestelmän markkinoille saattamista tai käyttöönottoa. Tarjoajien on noudatettava rekisteröintivelvoitteita sekä toteutettava tarvittavat korjaavat toimet, jos korkean riskin tekoälyjärjestelmä ei ole asetettujen vaatimusten mukainen. Lisäksi on huolehdittava ilmoituksista viranomaisille vaatimustenvastaisuudesta ja toteutetuista korjaavista toimista, kiinnitettävä CE-merkintä korkean riskin tekoälyjärjestelmiin sekä kansallisen toimivaltaisen viranomaisen pyynnöstä osoitettava, että korkean riskin tekoälyjärjestelmä on asetettujen vaatimusten mukainen.

Korkean riskin tekoälyjärjestelmien *käyttäjien* velvollisuudet ovat lievemmät kuin muihin tekoälyjärjestelmien tuotantoketjuun kuuluvien tahojen velvollisuudet. Asetusehdotuksessa käyttäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista tai muuta elintä, jonka alaisuudessa tekoälyjärjestelmää käytetään pois lukien henkilökohtainen, ei-ammattimainen käyttö. Käyttäjien on käytettävä järjestelmiä niiden käyttöohjeiden mukaisesti ja seurattava järjestelmän toimintaa ohjeiden perusteella. Jos on syytä katsoa, että käyttöohjeiden mukainen käyttö voi muodostaa riskin järjestelmän käytölle, heidän on ilmoitettava asiasta tarjoajalle tai jakelijalle ja keskeytettävä järjestelmän käyttö. Käyttäjien on myös ilmoitettava tarjoajalle tai jakelijalle, jos he ovat

havainneet vakavan vaaratilanteen tai toimintahäiriön ja keskeyttäneet tekoälyjärjestelmän käytön. Käyttäjien on lisäksi säilytettävä kyseisen korkean riskin tekoälyjärjestelmän luomat lokit tietyin ehdoin.

Viranomaisiin kohdistuvat velvollisuudet asetusehdotuksen nojalla riippuvat siitä, missä roolissa viranomainen toimii tekoälyjärjestelmän tuotantoketjussa. Tekoälyjärjestelmien tarjoajien velvollisuudet kohdistuvat viranomaiseen, jos tämä osallistuu tekoälyjärjestelmän kehittämiseen tai käyttöön ottoon. Viranomaisen on mahdollista toimia tekoälyjärjestelmän käyttäjän roolissa tai tietyissä tapauksissa myös tekoälyjärjestelmiä valvovana tahona. Asetusehdotuksessa eri toimijoiden velvollisuudet ja vastuut vaativat edelleen täsmentämistä asetuksen jatkovalmistelussa.

10.2.5 Tekoälyjärjestelmien vaatimustenmukaisuuden valvonta ja jälkivalvonta

Ennen korkean riskin tekoälyjärjestelmän markkinoille asettamista tai käyttöönottoa on suoritettava vaatimustenmukaisuuden arviointi, josta säädetään asetusehdotuksen 43 artiklassa. Tekoälyjärjestelmän vaatimuksenmukaisuus varmistetaan joko sisäisellä tai ulkoisella tarkastuksella. Kun kyseessä on liitteen III 2–8 kohdassa tarkoitettu tekoälyjärjestelmä, järjestelmän tarjoajan on monissa tapauksissa suoritettava sisäinen vaatimustenmukaisuuden arviointi[139]. Kyseiset tekoälyjärjestelmät ovat merkityksellisiä viranomaisten käytössä olevien järjestelmien kannalta. Näiden tekoälyjärjestelmien vaatimustenmukaisuuden arvioinnin yksityiskohtia koskee asetusehdotuksen liite VI. Komission on mahdollista muuttaa asetusta delegoidulla säädösillä niin, että ulkoinen tarkastus on pakollinen.

Jos tekoälyjärjestelmää muutetaan merkittävästi, sille täytyy suorittaa uusi vaatimustenmukaisuuden arviointi. Jos tekoälyjärjestelmä jatkaa oppimista käyttöön oton jälkeen, on suoritettava uusi vaatimustenmukaisuuden arviointi, jos järjestelmään tulee muutoksia tavalla, jotka poikkeavat alkuperäisestä vaatimustenmukaisuusarviointiprosessista ja jotka eivät aiemmin olleet määriteltävissä. Vaatimustenmukaisuuden arvioinnin jälkeen korkean riskin tekoälyjärjestelmät tulee rekisteröidä komission ylläpitämään EU-rekisteriin, joka on julkinen.

Markkinoille asettamisen jälkeen tekoälyjärjestelmän tarjoajan tulee perustaa jälkivalvontajärjestelmä tekoälyjärjestelmille. Jälkivalvontajärjestelmän tulee kerätä ja analysoida tekoälyjärjestelmän käyttämää dataa sen elinkaaren aikana ja joka mahdollistaa

139 Asetuksessa säädetään kuitenkin biometrista tunnistamista ja luottolaitoksia koskevista poikkeuksista vaatimustenmukaisuuden arvioinnin osalta.

korkean riskin tekoälyjärjestelmille asetettujen vaatimusten jatkuvan valvonnan. Jälkivalvontajärjestelmää varten tulee laatia erityinen suunnitelma, joka on osa järjestelmän teknistä dokumentaatiota. Järjestelmää koskevista vakavista vioista on ilmoitettava markkinavalvontaviranomaiselle artiklan 62 mukaan.

10.3 Johtopäätökset

Tässä arviomuistiossa on kuvattu EU:n säädösehdotuksia kyberturvallisuudesta ja tekoälystä. Arviomuistion kirjoitushetkellä näitä säädöksiä ei ole vielä hyväksytty EU-tasolla, ja EU:n neuvosto ja Euroopan parlamentti voivat esittää niihin muutosehdotuksia. Tekoälyä koskevan asetusehdotuksen käsittelyn on ennakoitu olevan pitkä EU-tasolla johtuen asetuksen laajuudesta ja monimutkaisuudesta. Näin ollen tekoälyä koskevaa asetusehdotusta on mahdollista ottaa huomioon vain rajallisesti kansallisen sääntelyn valmistelussa. On myös huomattava, että asetusehdotus tekoälystä ei vastaa perustuslakivaliokunnan esiin nostamiin huomioihin automaattisen päätöksenteon valtiosääntöisistä kysymyksistä, vaan näihin on mahdollista vastata kansallisen sääntelyn valmistelussa.

Tekoälyä koskevan asetusehdotuksen soveltamisalaan ja keskeisiin käsitteisiin, kuten tekoälyn määritelmään ja korkean riskin käyttötapauksiin, sekä eri toimijoiden rooleihin ja vastuun jakautumiseen liittyy monia täsmennystarpeita ehdotuksen jatkokäsittelyssä. Näiden seikkojen täsmentäminen on tärkeää, jotta vaikutuksia julkisen hallinnon toimintaan ja tietojärjestelmiin voidaan edelleen arvioida. Julkishallintoon kohdistuvaa sääntelyä tulisi tarkastella kokonaisuutena huomioiden julkisen sektorin toimijoiden roolien moninaisuus asetusehdotuksen näkökulmasta.

Myös NIS2-direktiivin vaikutuksia julkishallintoon tulee tarkastella jatkokäsittelyssä.

11 Sääntelykohteiden kehittämisen arviointi

Työryhmän näkemyksen mukaan tietojärjestelmien kehittämistä, käyttöönottoa ja käyttöä koskevaa sääntelyä on tarkennettava, jotta hallinnon lainalaisuus, hyvä hallinto, oikeusturva, läpinäkyvyys ja julkisen vallan käytön vastuullisuus (virkavastuu) voidaan varmistaa käytettäessä tietojärjestelmiä joko kokonaan tai osittain automatisoiduissa toimintaprosesseissa, joissa käsitellään hallintoasioita tai jotka liittyvät muuten automatisoituu palvelujen tuottamiseen digitaalisissa palveluissa.

Sääntely kohteena olisivat siten hallintoasiat, joita käsitellään joko kokonaan tai pääosin automatisoidusti tietojärjestelmissä ja tosiasiasiallinen hallintotoiminta digitaalisia palveluja käytettäessä. Kehitettävä sääntely olisi sidoksissa hallintolain soveltamisalaan, jolloin sääntelyn ulkopuolelle jäisivät lainkäyttö, ulosotto, poliisitutkinta ja esitutkinta. Toisaalta siltä osin kuin kysymys olisi yleisesti viranomaisten käyttämien tietojärjestelmien olennaisista vaatimuksista sitomatta sitä hallintoasioihin, sääntely voisi tulla sovellettavaksi tiedonhallintalaissa säädetyn mukaisesti. Lisäksi kehitettävä sääntely ei sisältäisi muuta palveluautomaatiota tai robotiikan käyttöä koskevia säännöksiä kuin digitaalisissa palveluissa tarjottavat automatisoidut toiminnallisuudet. Siten eri toimialoilla käytettävät palveluautomaatit ja erilaisiin laitteisiin perustuva robotiikka jäisivät erityissääntelyn varaan. Sääntelyssä ei voida myöskään ennakoida Euroopan unionissa valmisteilla olevaa tekoälyn käyttöön liittyvää sääntelyä, vaan tämä jää myöhempien lainsäädäntötoimien varaan siltä osin kuin unionin tuleva lainsäädäntö mahdollistaa kansallisen liikkumavaran.

Työryhmän näkemyksen mukaan tietojärjestelmien kehittämistä, käyttöönottoa ja käyttöä sekä tietojärjestelmän olennaisia vaatimuksia ja niiden arviointia koskevaa sääntely voitaisiin kehittää siten, että tiedonhallintalakiin sisällytettäisiin tietojärjestelmien olennaisia vaatimuksia koskevat säännökset. Tiedonhallintalakia tulisi myös päivittää viranomaisen toiminnan varautumista koskevilla säännöksillä sekä tarkentaa tietojen laadun varmistamista koskevia säännöksiä. Sääntely rakentuisi osittain riskiperusteisen arvioinnin pohjalta tapahtuvaan viranomaisen harkintaan, mutta osa olennaisista vaatimuksista täysin automatisoiduissa toimintaprosesseissa voisivat olla sitoviakin. Koska sääntely tulisi olemaan osittain teknisluonteista, voisi sitovaa sääntelyä mahdollisesti delegoida perustuslain 80 §:ssä säädetyissä rajoissa lakia alemmantasoiseen sääntelyyn esimerkiksi lakiin perustuvista teknisluonteisista arviointikriteeristöistä. Tällainen uusi tehtävä kytkeytyisi läheisesti monialaiseen yhteistyöhön perustuvan tiedonhallintalautakunnan voimassa olevaan sääntelyyn pohjautuviin tehtäviin.

Työryhmän näkemyksen mukaan digitaalisiin palveluihin sisältyvät automaattiseen neuvontaan ja palveluohjaukseen liittyvien toiminnallisuuksien asianmukaisuus tulisi varmistaa hyvän hallinnon ja oikeusturvan varmistamiseksi. Tältä osin tulisi harkita täydentävää ja täsmentävää sääntelyä digitaalisten palvelujen tarjoamisesta annettuun lakiin.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annettu laki tulisi uudistaa työryhmän näkemyksen mukaan kokonaisuudessaan, koska voimassa oleva säädös on sidottu pelkästään tietoturvallisuuden arviointiin. Uudessa tietojärjestelmien olennaisten vaatimusten toteuttamisen dokumentointia, varmistamista ja arviointia koskevassa laissa olisi säännökset viranomaisen tietojärjestelmien testaamisesta/tarkastamisesta, itsearvioinnista, käyttöönoton edellytyksistä, laadunvalvonnasta, vastuiden määrittelystä ja dokumentoinnista sekä ulkoisen arviointiviranomaisen tehtävistä, toimivallasta sekä tilanteista, jolloin tietojärjestelmästä vastuussa olevan viranomaisen tulee pyytää tietojärjestelmälleen ulkoinen arviointi ennen käyttöönottoa. Ulkoinen arviointi voisi koskea vain teknisluonteisten vaatimusten todentamista. Mahdollisesti käyttöönoton edellytyksistä, laadunvalvonnasta, vastuiden määrittelystä sekä dokumentoinnista voitaisiin säätää myös erityislainsäädännössä tai tarvittavilta osin tiedonhallintalaissa. Näin on tehty esimerkiksi asiakastietolaissa ja toisiolaissa sekä julkisen hallinnon turvallisuusverkkoa koskevassa sääntelyssä.

Arviointilaitoksia koskevaan lakiin tehtäisiin vain välttämättömiä päivityksiä ja sen kokonaisuudistus jäisi myöhemmin muun muassa EU:n kyberturvallisuusasetuksen ja tietosuoja-asetuksen perusteella kehittyvien sertifiointimekanismien perusteella tehtävän uudelleenarvioinnin varaan. Viranomaiset voisivat käyttää edelleen arviointilaitoksia arviointilaitoslain perusteella tietoturvallisuuden arvioinnissa siltä osin kuin arvioinnit eivät kuulu viranomaisille säädettyihin tehtäviin. Vaihtoehtoisesti kaikki tietojärjestelmien ulkoiset arvioinnit voitaisiin antaa arviointilaitosten tehtäväksi, mutta tämä edellyttäisi arviointilaitoksia koskevien vaatimusten merkittävää uudistamista.

Uuden lainsäädännön valmistelussa on eri akkreditointia, sertifiointia ja muuta vaatimustenmukaisuuden toteamista koskeva sääntely (tietosuoja-asetus, NLF-asetus, kyberturvallisuusasetus ja kansallinen sääntely) ja eri säädösten suhteet toisiinsa selkeytettävä – samoin viranomaisten toimivaltuudet.

Tässä arviomuistiossa esitettyjen kehittämisehdotusten edistäminen edellyttää vielä yhteensovittamista ainakin hallintolain kanssa. Tätä yhteensovittamista tehdään yhteistyössä oikeusministeriön asettaman automaattisen päätöksenteon yleislainsäädäntöä kehittävän työryhmän kanssa.

Muutosten taloudellisia vaikutuksia voidaan arvioida siinä vaiheessa, kun sääntelykohteet ja sääntely ovat tarkentuneet. Uusi lainsäädäntö arviointien toteuttamisesta sekä mahdolliset uudet olennaiset vaatimukset edellyttävät myös taloudellisia panostuksia, joskin sääntely ei olisi kaikilta osin pakottavaa, vaan perustuu tietojärjestelmien toiminnallisuuksiin, kuten automatisoitujen toimintaprosessien käyttöönottoon.

12 Työryhmä

Työryhmän tiedot ja asiakirjat ovat saatavilla valtiovarainministeriön verkkosivuilta osoitteessa https://vm.fi/hanke?tunnus=VM059:00/2021.

Työryhmä

Tomi Voutilainen, valtiovarainministeriö (puheenjohtaja)
Tommi Oikarinen, valtiovarainministeriö (varapuheenjohtaja)
Johanna Erkkilä, Kyberturvallisuuskeskus
Mikko Hakuli, Verohallinto
Mervi Kuittinen, valtiovarainministeriö, varajäsen Ville Koponen
Miska Lautiainen, valtiovarainministeriö
Erika Leinonen, tietosuojavaltuutetun toimisto (asiantuntijajäsen)
Piia Nyström, liikenne- ja viestintäministeriö, varajäsen Erica Karppinen
Sirpa Sillstén, työ- ja elinkeinoministeriö
Ida Sulin, Kuntaliitto, varajäsen Tommi Karttaavi
Risto Suominen, kansallinen akkreditointielin FINAS
Niklas Vainio, oikeusministeriö

Sihteeristö

Antti Helin, valtiovarainministeriö
Maria Kekäläinen, valtiovarainministeriö
Tuija Kuusisto, valtiovarainministeriö
Eeva Lantto, valtiovarainministeriö
Niko Mäkilä, valtiovarainministeriö
Hilda Mäkinen, valtiovarainministeriö
Anna-Mari Rusanen, valtiovarainministeriö

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN 978-952-367-693-0 (pdf)

Syyskuu 2021