Oikeuskanslerinvirasto

Lausunto

02.09.2021 OK V/2005/21/2021

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

Muistion johdanto-osa kuvaa hyvin julkisessa hallinnossa, hallintoasioiden käsittelyssä sekä julkisten palvelujen tuottamisessa käytettäviin tietojärjestelmiin liittyvän sääntelyn hajanaisuutta ja osin vanhentuneisuutta. Myöskään tietojärjestelmistä ei säännellä yhtenäisesti tai vakiintuneesti. Muistion johdanto-osa tuo myös hyvin esille tarpeen jatkoselvittää julkisen hallinnon tietojärjestelmien kehittämisen ja käytön vaatimuksia sekä vaatimuksenmukaisuuden arviointia koskevaa sääntelyä, jolla varmistetaan hyvän hallinnon ja oikeusturvan sekä virkavastuun toteutuminen hallinnon toimintaprosesseissa.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Viittaan yleisesti kysymykseen 1 antamaani vastaukseen. Lisäksi tuon esille laillisuusvalvonnassani tehtyjen havaintojen perusteella seuraavat yleiset seikat:

Tietojärjestelmät ja tietovarannot sekä niissä tehtävät ja tietojärjestelmiin kohdistuvat toiminnot ovat digitalisaation seurauksena yhä laajemmin ja voimakkaammin merkityksellisiä eri oikeuksien toteutumiselle, perusoikeuksien tasapainolle sekä erityisesti hyvän hallinnon ja sitä yleisesti määrittävien hallinnon yleisten oikeusperiaatteiden toteutumiselle. Sama koskee tietovarantoja. Tämän vuoksi perusoikeuksien ja ihmisoikeuksien aktiiviseen toteuttamiseen velvoitetussa oikeusvaltiossa datan ja tiedon käsittelyn infrastruktuuria, tiedonhallintaa ja tietojärjestelmiä sekä niitä koskevia ja niissä tehtäviä toimintoja on tarpeen säädellä lainsäädännössä. Tarvetta osaltaan lisää automaatio, jossa hallinnon asiakas ja varsinkin myös hallinnon sisäiset käyttäjät, asiaa käsittelevät virkamiehet, tulevat teknologisen järjestelmän osiksi. Ihmisen vuorovaikutus tietojärjestelmien kanssa tulee tällöin yhä ratkaisevammaksi palveluperiaatteen toteutumisen sekä hallintotoiminnan laadun ja tuloksellisuuden sekä yleensä oikeuksien toteutumisen kannalta.

Tietojärjestelmät ja tietovarannot ovat nopeasti kehittyviä. ICT-teknologiassa on ominaista jossain määrin se, että tarkkoja ja pitkään ajassa kestäviä määritelmiä osaksi vierastetaan. Siten esimerkiksi tietojärjestelmän, tietovarannon ja tekoälyn käsitteissä on jossain määrin huojuntaa. Tärkeä sääntelylle asetettava vaatimus on tosiasiallinen teknologianeutraalisuus eli se, että sääntely koskee tietojärjestelmiä ja niissä tehtäviä sekä niihin liittyviä ja niihin kohdistuvia toimintoja yleisesti ja siten, etteivät ne ajattelumalleiltakaan liiaksi kiinnity johonkin yksittäiseen osaan. Tietojärjestelmien osalta julkinen hallinto on lisäksi aina jossain määrin riippuvainen markkinoiden tarjonnasta. Näistä syistä johtuen kovin yksityiskohtaista ja asiallisesti tiettyihin teknologisiin ratkaisuihin ja menetelmiin kiinnittyvää sääntelyä on tarpeen varoa. Sääntelyn olisi siten tarpeen olla enemmän yleisten periaatteiden tasolla.

Oikeudellisesti erityisen riskialttiista tietovarannoista ja tietojärjestelmistä tarvitaan muun muassa EU:n yleisen tietosuoja-asetuksen eri artiklojen sekä mahdollisesti EU:n tulevan tekoälysäädöksen ja jo voimassa olevan unionin erityissääntelyn perusteella erityislainsäädäntöä. Esimerkiksi yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan c ja e alakohdat, osaksi 9 artikla ja 22 artikla edellyttävät muun muassa tietosuoja-asetusta täydentävää unionin tai jäsenvaltion lainsäädäntöä, joka Suomessa on useimmiten toimialakohtaista tai tehtäväkohtaista erityislainsäädäntöä, johtuen jo tietosuoja-asetuksen ja

perustuslakivaliokunnan käytännön edellyttämästä sääntelytarkkuudesta. Olisikin siksi tarpeen muodostaa myös selkeä systemaattinen kartta sille, missä määrin kansallisessa sääntelyssä käytetään yleislainsäädäntöä ja mihin kysymyksiin erityislainsäädäntö on tarpeen, jotta oikeusjärjestyksen johdonmukaisuus myös lainsoveltajien kannalta säilytetään.

Yhdyn arviomuistion johtopäätökseen sääntelyn osittaisesta hajanaisuudesta ja tietyistä epäjohdonmukaisuuksista esimerkiksi keskeisten käsitteiden käytössä. Tämä osaltaan korostaa julkisen hallinnon tiedonhallinnasta annetun lain (906/2019; tiedonhallintalaki) merkitystä yleisen oikeudellisen sääntelyn välineenä. Tietojärjestelmiä ja niiden toimintoja sekä tiedon käsittelyä koskevaa sääntelyä ei saisi pirstoa liian moniin säädöksiin, jolloin säädösten soveltamisalat ja keskinäiset suhteet muodostuvat helposti epäselviksi.

Tietojärjestelmiä ja tietovarantoja sekä niissä tehtäviä ja niihin kohdistuvia toimintoja ei voida pitää kovinkaan tarkasti erossa hallinnon toimintaa sekä yksityisten oikeuksia ja velvollisuuksia koskevasta substanssilainsäädännöstä. Sen vuoksi tietojärjestelmäsääntelyä tulee aina tarkastella yhdessä hallintolain (434/2003) ja viranomaisten toiminnan julkisuudesta annetun lain (621/1999) sekä niiden kehittyvien tulkintojen kanssa, kuten arviomuistiossa on tehtykin. Sääntelykokonaisuudeksi muodostuvatkin tietojärjestelmät ja tietovarannot sekä tietojärjestelmiin kohdistuvat toiminnot kuten järjestelmien suunnittelu, kehittäminen, testaaminen, käyttöönottoon hyväksyminen sekä ylläpito ja toiminnan valvonta sekä elinkaaren päässä alasajo ja tietojen sekä toimintojen siirtäminen uusiin järjestelmiin.

Tietojärjestelmissä tehtäviin toimintoihin puolestaan vaikuttaa olennaisella tavalla hallintolaki ja sektorikohtainen substanssilainsäädäntö. Oikeudellisesta näkökulmasta on yhtäältä niin, että

automaatioon ja tietojärjestelmien käyttöön aina liittyy toimintaprosessin mallintaminen hallintolain ja asiaa koskevan substanssilainsäädännön pohjalta sekä toimintaprosessiin liittyvän informaatioprosessin määrittely. Oikeudellisessa sääntelyssä informaatioprosessia ei voida kuitenkaan ottaa toimintaprosessista erillisen sääntelyn kohteeksi kuin vain joiltain osin. Sosiaali- ja terveydenhuollon potilas- ja asiakastiedon käsittelyä koskevan lainsäädännön uudistus (HE 212/2020 vp – StVM 11/2021 vp – EV 71/2021), jota koskeva lainsäädäntö vahvistettiin 27.8.2021 ja jossa säädettiin uusi laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021), kertoo osaltaan siitä, että substanssiin liittyvästä kattavasta ja erillisestä potilastietoon liittyvän informaatioprosessin sääntelystä oli muun muassa yleisen tietosuoja-asetuksen johdosta perusteltua luopua. Muutos näkyy erityisesti siinä, että yksittäistapauksellisen suostumuksen sijasta henkilötietojen käsittelyperusteena on tietoteknisesti varmistettu asiakas- tai hoitosuhde (lain 15 §).

Tietojärjestelmiä ja tietovarantojen hyödyntämistä koskevat yksityiskohdat sekä erityisesti viranomaiselle kuuluva asian selvittämisvelvollisuus ja siihen liittyvä vuorovaikutus asiakkaan kanssa ovat osaksi erilaisia massahallinnossa ja yksilöllisiä hallintopäätöksiä tehtäessä. Suomen nykyisessä lainsäädännössä kaikki mukautukset suhteessa hallintolakiin tehdään alakohtaisessa erityislainsäädännössä, jossa säädellään massahallinnon erityispiirteistä. Tämä systematiikka voi osaltaan johtaa erityislainsäädännössä yksilön oikeusturvan kannalta yleishallinto-oikeutta heikommin perusteltaviin ratkaisuihin sekä helposti perusteettomaankin hajanaisuuteen ja epäyhtenäisyyteen tietojärjestelmiä koskevassa sääntelyssä. Ilmiö on havaittu valtioneuvoston oikeuskanslerin laillisuusvalvontakäytännössä niin yksittäisten kanteluasioiden käsittelyn kautta kuin ennakollisessa säädösvalvonnassa. Vaikka asia ei suoraan kuulu valtiovarainministeriön tietojärjestelmäsääntelyä arvioivalle työryhmälle, olisi perusteltua myös arvioida oikeusministeriön kanssa sitä, pitäisikö esimerkiksi Saksan näiltä osin vuonna 2016 osittain uudistetun hallintolain (Verwaltungsverfahrensgesetz, VwVfG) tapaan Suomessakin sisällyttää joitain yleisempiä massahallinnon erityisvaatimuksia hallintolakiin. Riittävän yhtenäinen ja sisällöltään kattava yleislainsäädäntö on myös perusta tietojärjestelmiä koskeville yleisille vaatimuksille.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

Toiminnalliset vaatimukset johtuvat pitkälti perustuslain 21 §:stä ja muista perustuslain perusoikeussäännöksistä sekä hallintolain yleissäännöksistä, samoin kuin julkisen vallan yleisestä, perustuslain 22 §:ssä säädetystä velvollisuudesta turvata ja toteuttaa perusoikeudet. Kovin yksityiskohtaisia erityisiä toiminnallisia vaatimuksia ei voida asettaa, vaan yleisempinä vaatimuksina dokumentoitu käyttötarkoitus ja sopivuus käyttötarkoitukseensa, käyttötarkoitukseen liittyvän yleis- ja erityislainsäädännön täyttäminen, käyttäjäystävällisyys ja käytettävyys sekä se, että järjestelmän toiminnoissa voidaan ilman suurempia vaikeuksia toteuttaa hallintolain palveluperiaate ja hallinnon yleiset oikeusperiaatteet sekä menettelyä koskevat säännökset ja se, että järjestelmä täyttää tietosuojalainsäädännön vaatimukset. Toiminnallisia vaatimuksia johtuu myös siitä erityislainsäädännöstä, jonka mukaisiin tehtäviin

tietojärjestelmää käytetään. Kommentoin tätä kysymystä tarkemmin kohdassa 4 olevan kysymyksen yhteydessä.

4. Millaisia olennaisia teknisiä vaatimuksia hallintoasioita käsitteleville tietojärjestelmille pitäisi lainsäädännöllä säätää?

Arviomuistion mukaan tietojärjestelmien toiminnallisia ja teknisiä vaatimuksia määritellään tyypillisesti viranomaisten omissa ohjeissa, hankinta-asiakirjoissa sekä tietylle alalle kohdennetuissa standardeissa. Yleislainsäädännössä ei ole säädetty tietojärjestelmän olennaisista vaatimuksista asian käsittelyn asianmukaisuuden ja selvittämisvelvollisuuden toteuttamisessa. Työryhmän näkemyksen mukaan tällaisista tietojärjestelmien olennaisista vaatimuksista voitaisiin säätää lailla. Arviomuistiossa tuodaan lisäksi esille, että sääntelykohteena tietojärjestelmissä käytettävä tieto- ja viestintäteknologia on nopeasti

muuttuvaa, joten sääntelynkin on oltava joustavaa, teknologianeutraalia ja joltain osin abstraktilla tasolla. Tietojärjestelmien vaatimuksien yhdenmukaistamisessa ovat tärkeitä laissa säädetyn lisäksi lakia alemman tasoinen sääntely sekä alan soft law –tyyppinen itse- tai myötäsääntely.

Yhdyn arviomuistiossa esitettyihin näkemyksiin siitä, että perustuslain 21.1 §:ssä säädetyt asian käsittelyn asianmukaisuuden sekä hallintolain 7.1 §:ssä säädetyt asian käsittelyn ja palvelun asianmukaisuuden vaatimukset luovat välttämättömän ja ehdottoman perustan myös hallinnon tietojärjestelmiltä ja viranomaisen digitaalisilta palveluilta edellytettäville kriteereille. Viranomaisten tietojärjestelmien ja sähköisten palvelujen toimivuus ja niiden vaikutus asiakkaiden perusoikeuksien ja hyvän hallinnon periaatteiden toteutumiseen on noussut ja nousee toistuvasti esille oikeuskanslerille tehdyissä kanteluissa. Laillisuusvalvonnassa on havaittu puutteita esimerkiksi TE-hallinnon ja Kansaneläkelaitoksen (Kelan) järjestelmissä ja palveluissa.

Esimerkkinä viittaan päätökseeni kanteluasiassa OKV/338/1/2018, jossa työ- ja elinkeinohallinnon työnhakijoille tarjoamia verkkopalveluja ei ollut sovitettu kaikille mobiililaitteille. Kaikki työnhakijat eivät siten välttämättä kyenneet käyttämään verkkopalveluja yhtä laajasti, vaan palvelujen laajuus riippui siitä, minkälainen laite heillä on käytettävissään. Työ- ja elinkeinohallinto oli uudistamassa sähköistä palvelujärjestelmäänsä. Totesin päätöksessäni, että uudistustyössä sähköistä asiointia tulisi edistää asiakaslähtöisesti. Verkkopalveluissa tulisi pyrkiä mahdollisimman suureen laiteriippumattomuuteen, eli digitaalisen asioinnin pitäisi olla mahdollista myös yleisesti käytössä olevilla mobiililaitteilla ja niissä käytettävillä sovelluksilla. Tähän velvoitti myös tuolloin pian voimaan tulossa ollut laki digitaalisten palvelujen tarjoamisesta.

Ratkaisussa OKV/1179/10/2020 oli puolestaan kysymys Kelan sähköisestä asiointipalvelusta. Palvelussa käytettävien sähköisten lomakkeiden käyttämiseen ja täyttämiseen liittyi ominaisuuksia, jotka saattoivat vaikeuttaa erityisesti vammaisten ja sairaiden asiointia verkkopalvelussa. Näin oli erityisesti toimeentulotukea koskevien lomakkeiden kohdalla. Apulaisoikeuskansleri totesi, että digitaalisten palvelujen tarjoamista koskevan lain esitöissä on korostettu julkisen sektorin digitaalisten palvelujen saavutettavuutta osana perustuslaissa turvattua yhdenvertaisuuden toteuttamista. Digitaalisten palvelujen saavutettavuudella edistetään myös perustuslaissa säädettyjen hyvän hallinnon takeiden toteuttamista, johon kuuluu jokaisen oikeus saada viranomaisilta asianmukaisia palveluita ja neuvontaa. Apulaisoikeuskanslerin mukaan Kelalla on toimeentulotuen osalta erityisen korostunut velvollisuus ja vastuu varmistaa digitaalisten palvelujen ja sähköisen asioinnin saavutettavuus ja käytettävyys erilaisten asiakasryhmien haasteet, kyvyt ja tarpeet huomioon ottaen.

Tässä yhteydessä tuon esille, että sosiaali- ja terveysministeriön keväällä 2021 asettamassa työryhmässä on tarkoitus muun ohessa kartoittaa digitalisaation mahdollisuuksia sosiaaliturvajärjestelmän toimeenpanossa ja toteutuksessa. Tässä kesken olevassa hankkeessa on tuotu esille sosiaaliturvajärjestelmän digitalisaatioon, tiedonhallintaan ja tietojärjestelmiin liittyviä haasteita ja selvitystarpeita sekä viitattu muun ohessa käynnissä oleviin TE-hallinnon ja Kelan sähköisten asiointikanavien ja tietojärjestelmien uudistustyöhön; https://stm.fi/-/sosiaaliturvan-digitalisaation-lahtokohdat.

Erityislainsäädännössä, kuten uudessa laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021), säädetään sosiaali- tai terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja valtakunnallisten tietojärjestelmäpalveluiden olennaisista vaatimuksista. Kyseisen lain mukaan sosiaali- tai terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja hyvinvointisovellusten tulee dokumentoidusti täyttää sille määriteltyä käyttötarkoitusta koskevat olennaiset vaatimukset sekä lisäksi yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä olennaiset vaatimukset. Laissa on myös tietojärjestelmäpalveluiden käytettävyyttä koskevia vaatimuksia. Laki edellyttää järjestelmät luokiteltavan niille asetettavien vaatimusten perusteella A ja B luokkaan kuuluviksi. Luokittelu johtaa myös eritasoisiin sertifioinnin ja testauksen vaatimuksiin. Laki edellyttää myös tietoturvallisuuden ja tietosuojan omavalvontaa, tietoturvasuunnitelmia sekä tietoturvallisuuden todentamista.

Uuden sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 34 §:ssä on varsin seikkaperäinen säännös tietojärjestelmälle ja hyvinvointisovellukselle asetettavista olennaisista vaatimuksista. Asiakastietojen käsittelyssä käytettävän tietojärjestelmän ja hyvinvointisovelluksen tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset. Hyvinvointisovelluksen tulee täyttää saavutettavuusvaatimukset. Vaatimusten on täytyttävä käytettäessä tietojärjestelmää sekä itsenäisesti että yhdessä muiden siihen liitettäviksi tarkoitettujen tietojärjestelmien kanssa. Palvelunantajan käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän muodostaman kokonaisuuden kautta. Tietojärjestelmä täyttää olennaiset vaatimukset silloin, kun se on suunniteltu, valmistettu ja toimii tietoturvaa ja tietosuojaa koskevien lakien ja niiden nojalla annettujen säännösten sekä yhteentoimivuutta koskevien kansallisten määrittelyjen mukaisesti. Toiminnallisuutta koskevat olennaiset vaatimukset täyttyvät, jos tietojärjestelmällä pystytään suorittamaan käyttötarkoituksen mukaisessa asiakas- ja potilastietojen käsittelyssä lakien ja niiden nojalla annettujen säännösten edellyttämät toiminnot. Laissa edellytetään vaatimustenmukaisuuden osoittamista sertifioinnilla tai sertifioinniksi luettavalla tietojärjestelmän valmistajan selvityksellä sekä luokan A järjestelmissä lisäksi vielä yhteentoimivuuden testauksella ja tietoturvallisuuden arvioinnilla tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti.

Myös esimerkiksi laissa vahvasta sähköisestä tunnistamisesta (617/2009) on säännöksiä sähköisen tunnistamisen järjestelmille asetettavista vaatimuksista. Vaatimuksiin sisältyy muun ohessa tunnistusjärjestelmän turvallisuus ja luotettavuus.

Tiedonhallintalaissa ei ole varsinaisia säännöksiä tietojärjestelmille asetettavista toiminnallisista tai teknisistä vaatimuksista. Laki kuitenkin sisältää muun ohessa säännökset tietoaineistojen ja –järjestelmien tietoturvallisuudesta, tietojen siirtämisestä verkossa, tietoaineistojen turvallisuuden varmistamisesta, tietojärjestelmien käyttöoikeuksien hallinnasta ja lokitietojen keräämisestä. Laissa on myös säädetty tiedonhallintayksikön velvollisuudesta ylläpitää tiedonhallintamallia palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi.

Näen tietojärjestelmille asetettavien yleisten toiminnallisuuksien tai teknisten vaatimusten säätämiselle laintasoisessa sääntelyssä haasteita. Toimijoiden kirjo on moninainen, ja eri viranomaisten toimivaltaan kuuluvien hallintoasioiden käsittely ja päätöksenteko sekä niissä käytettävät tietojärjestelmät eroavat toisistaan.

Yhdyn arviomuistiossa esitettyyn huomioon siitä, että tietojärjestelmissä käytettävän tieto- ja viestintäteknologian nopean kehittymisen vuoksi sääntelynkin tulisi olla riittävän joustavaa ja teknologianeutraalia. Tähän nähden laintasoinen sääntely ei ole arvioni mukaan soveliain säädösperusta ainakaan tietojärjestelmille asetettaville yksityiskohtaisille vaatimuksille. Toiseen suuntaan painavana näkökohtana voidaan kuitenkin ottaa huomioon, että yleinen ja kaikilla julkishallinnon aloilla sovellettava sääntely tietojärjestelmien laatua koskevista vähimmäisvaatimuksista voisi tuoda vahvempaa velvoittavuutta sekä yhtenäisyyttä ja selkeyttä nyt osin hajanaiseen sääntelyyn.

Käsitykseni mukaan tiedonhallintalakiin voisi harkita sisällytettäväksi joitakin yleisluonteisia periaatteita vaatimustenmukaisuudesta. Uudemman erityislainsäädännön ja Euroopan unionin lainsäädännön säännöksistä saa yleiselle tasolle vietynä johtoa siihen, minkä tyyppisiä periaatteita ja velvoitteita voitaisiin nostaa lain tasolle. Kovin tarkka tai yksityiskohtainen sääntely ei nähdäkseni liene teknologianeutraalisuuden vaatimuksen, tietojärjestelmien laajan kirjon ja hyvin erilaisten käyttötarkoitusten sekä erityislainsäädännön vaatimusten vuoksi oikeudellisesti mahdollista eikä liene tarkoituksenmukaistakaan. Onkin korostettava sitä, että hallinnon lainalaisuuden vaatimuksesta ja hallintolaista esimerkiksi johdetaan käytännön tietojärjestelmähankkeita ja –hankintoja varten kutakin järjestelmää koskevat vaatimukset.

5. Millaisia vaatimuksia, kuten dokumentointivaatimuksia, tietojärjestelmien kehittämiselle pitäisi lainsäädännöllä säätää?

Arviomuistiossa todetaan, että yleislainsäädännössä ei ole esitetty kehittämisen vastuisiin ja dokumentointiin liittyviä vaatimuksia. 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.

Näkemykseni mukaan tietojärjestelmien kehittämisessä on perusteltua painottaa oikeuksien ja hyvän hallinnon toteutumisen ennakollisuutta ja varmistaa tietojärjestelmän asianmukaisuus jo suunnittelu- ja kehittämisvaiheessa sekä käyttötarkoituksen ja siihen sopivuuden sekä käyttöönottamisen hyväksynnän dokumentoitua todentamista. Tiedonhallintalaissa on jo nykyisellään säädetty tiedonhallintayksikön tehtävästä arvioida tietojärjestelmiä käyttöönotettaessa näihin kohdistuvat muutokset ja niiden vaikutukset suhteessa tiedonhallinnan vastuisiin, tietoturvallisuusvaatimuksiin ja -toimenpiteisiin, tietoaineistojen

muodostamista ja luovutustapaa koskeviin vaatimuksiin, asianhallinnan ja palvelujen tiedonhallinnan vaatimuksiin sekä muualla laissa säädettyihin asiakirjojen julkisuuteen, salassapitoon, suojaan ja tiedonsaantioikeuksiin. Tiedonhallintayksikön on tiedonhallinnan muutosten arvioinnissaan myös otettava huomioon tietovarantojen yhteentoimivuus sekä niiden hyödynnettävyys tietoaineistoja muodostettaessa ja käytettäessä.

Edellä kuvaamallani tavalla suunnittelun vaatimuksia voidaan kuitenkin välillisesti johtaa sovellettavaksi tulevasta yleis- ja erityislainsäädännöstä. Digitaalisessa toimintaympäristössä korostuvat tietojärjestelmien asianmukaisen suunnittelun, testauksen ja käyttöön hyväksynnän samoin kuin asianmukaisen datan ja sen käsittelyn varmentaminen, osassa järjestelmiä asianmukainen opetusdata sekä järjestelmän virheettömän ja asianmukaisen toiminnan jatkuva valvonta ja varmentaminen, joka monimutkaisemmissa tai riskialttiimmissa järjestelmissä edellyttää myös auditointeja. Automaattisessa päätöksenteossa yksittäisen hallintopäätöksen tekemisen sijasta päätöksenteko- tai päättelysääntöjen ohjelmointi, testaus ja hyväksyntä nousevat päätöksen esittelyn ja ratkaisemisen rinnalle huomattaviksi hallinnon toiminnan oikeudelliseen asianmukaisuuteen vaikuttaviksi toimiksi.

Työryhmän muistion luvussa 5 ei ole erikseen nostettu tarkasteltavaksi tietojärjestelmien toimivuuden jatkuvaan valvontaan liittyviä tehtäviä. Näkisin kuitenkin, että tietojärjestelmien toimivuuden ja datan käsittelyn jatkuva sisäinen valvonta tai omavalvonta on olennainen osa hyvää hallintoa. Sitä koskevia yleisiä kysymyksiä ja mahdollisia sääntelytarpeita kannattanee pohtia tarkemmin vielä jatkovalmistelussa. Yleisesti ottaen sisäinen valvonta on ohuesti ja

lähinnä vain taloudellisesta näkökulmasta säänneltyä niin valtion talousarviosta annetussa laissa ja asetuksessa kuin kuntalaissa ja hyvinvointialuelaissa.

Tietojärjestelmien kehittämistä, käyttöönottoa ja testausta sekä hyväksyntää käyttötarkoitukseensa samoin kuin jatkuvaa valvontaa koskevista yleisluontoisista vaatimuksista ja vastuista onkin harkittava työryhmän arviomuistiossa hahmotellulla tavalla jatkovalmistelussa sääntelyn mahdollisuuksia ja tarpeita.

6. Miten lainsäädännöllä tulisi varmistua virkavastuun toteutumisesta ja kohdistumisesta, mitä tulee tietojärjestelmien kehittämiseen, käyttöönottoon ja käyttöön, sekä tietovarantojen käyttöön?

Pidän virkavastuun toteuttamiseen ja kohdistamiseen liittyvien kysymysten ja lainsäädännön selkiyttämistä ensiarvoisen tärkeänä. Olen tuonut selvitystarpeen esille muun ohessa Kelan

automaattista päätöksentekoa koskevassa ratkaisussani OKV/131/70/2020 sekä useissa lausunnoissani, kuten lausunnossani koskien hallinnon automaattisen päätöksenteon sääntelyalaa (OKV/1698/21/2021) sekä arviomuistiota hallinnon automaattisen päätöksenteon

yleislainsäädäntötarpeista (OKV/1348/21/2020). Virkavastuuseen ja virkamiesten esteellisyyteen liittyviä kysymyksiä tulisikin näkemykseni mukaan tarkastella jo/myös oikeusministeriön asettamassa työryhmässä, joka parhaillaan selvittää hallinnon automaattisen päätöksenteon sääntelytarpeita.

Kuten arviomuistiossa on kuvattu, tietojärjestelmien suunnittelu-, valmistelu-, kehittämis-, testaus-, ylläpito- ja valvontatehtäviin osallistuu eri henkilöitä ja toimijoita, joiden vastuut ja roolit ovat hyvin erilaiset. Laissa ei kuitenkaan tällä hetkellä erikseen säädetä virkamiehen roolista tietojärjestelmän kehittämisen valvonnassa ja ominaisuuksien ja toiminnallisuuksien määrittelyssä, testaamisessa tai käyttöönotossa.

Vastuuasemien selkeä erottelu ja määrittely olisi virkavastuun oikeanlaisen kohdentamisen kannalta keskeistä. Totean, että tiedonhallintalaissa on säännökset tiedonhallintayksikön johdon velvoitteista muun ohessa määritellä tiedonhallintaan liittyvien tehtävien vastuut, huolehtia ajantasaisista ohjeista mm. tietojärjestelmien käytöstä ja tietoturvallisuustoimenpiteistä, tarjota asiaan liittyvää koulutusta ja asianmukaiset työvälineet sekä järjestää riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta. Pidän oikeuskäytännön valossa jossain määrin tulkinnallisena, onko

mainituista säännöksistä mahdollista johtaa selkeää virkamieheen kohdistettavaa ja virkavastuun muodostavaa toimintavelvollisuutta.

Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Pykälän oikeusvaltioperiaatetta koskevan 3 momentin ensimmäinen virke edellyttää, että julkisen vallan käyttäjällä on oltava aina viime kädessä eduskunnan säätämään lakiin palautettavissa oleva toimivaltaperuste. Lakisidonnaisuus puolestaan edellyttää, että julkisessa toiminnassa noudatetaan kaikkia voimassaolevia oikeusnormeja ja vakiintuneita oikeusperiaatteita ja toimitaan niiden määrittelemissä rajoissa. Lakisidonnaisuus edellyttää myös, että julkisessa toiminnassa otetaan huomioon perus- ja ihmisoikeudet.

Rikosoikeudellisen virkavastuun osalta lisäksi perustuslain 8 §:n rikosoikeudellinen laillisuusperiaate asettaa varsin tiukkoja vaatimuksia rikosoikeudellisen vastuun perustavan normikokonaisuuden selkeydelle, ymmärrettävyydelle, velvoitteiden ennakoitavuudelle sekä tarkkarajaisuudelle ja täsmällisyydelle. Rikosoikeudellinen virkavastuu tulee kysymykseen toimittaessa vastoin velvoittavasta ja yksilöidystä säännöksestä tai määräyksestä suoraan ilmenevää velvollisuutta tai vastoin velvollisuutta, joka asian laatuun nähden on riittävän täsmällisesti ennalta pääteltävissä virantoimituksessa virkamiestä velvoittavista säännöksistä ja määräyksistä. Korkeimman oikeuden käytännössä on korostettu, että virkavelvollisuuden sisältö tulee rikosoikeudellisen virkavastuun tulemiseksi kysymykseen määritellä virkatoiminnassa noudatettavissa säännöksissä ja määräyksissä riittävän tarkkarajaisesti ja siten, että säännösten soveltaminen on ennakoitavissa. Sääntelyn

avoimuus ja tapauskohtaisen sisällön harkinnanvaraisuus ei kuitenkaan vielä sellaisenaan johda siihen, että normia olisi pidettävä luonteeltaan vain ohjeellisena tai ettei sen noudattamatta jättämiseen voisi liittyä rikosoikeudellista vastuuta (ks. perustuslakivaliokunnan mietintö PeVM 26/2020 vp, s. 22-23 ja KKO 1999:46, KKO 2008:42, KKO 2017:92, KKO 2018:90, KKO 2019:104 ja KKO 2020:13).

Näillä perusteilla onkin huomiota vielä kiinnitettävä siihen, onko säännöksissä tai määräyksissä asetettu kaikilta osin riittävän ennakoitavia ja täsmällisiä velvoitteita olennaisimpien tiedonhallintaan ja tietojärjestelmiin liittyvien velvollisuuksien osalta. Tämä koskee niin tiedonhallintalain nykyisiä, sinänsä hyvin hyvää hallintoa tietohallinnossa toteuttavia velvoitteita kuin työryhmän pohdinnassa olevia uusia säännöksiä eri lakeihin.

Virkavastuuta koskevien säännösten tulee perustuslakivaliokunnan useampaan kertaan toistamien ja arviomuistiossa hyvin tunnistettujen kannanottojen mukaisesti säilyä merkityksellisinä. Virkavastuulla voidaan nähdä hallinnon toiminnan oikeudellista asianmukaisuutta eli erityisesti oikeusvarmuutta sekä luottamusta sitä kohtaan varmistava funktio. Lisäksi virkavastuu toteuttaa laajempaa julkisen vallan käytön vastuunalaisuuden ja osoittamisvelvollisuuden periaatteita. Virkavastuun merkityksellisyys edellyttää sitä koskevan oikeuskäytännön ja laillisuusvalvontakäytännön valossa ensinnäkin sitä, että virkavastuu voidaan palauttaa riittävän täsmällisiin ja konkreettisiin oikeusnormeihin. Toiseksi se edellyttää sitä, että osoittamisvelvollisuus ja oikeusvarmuutta varmentavat ja toteuttavat toimenpiteet kohdentuvat virheiden, riskien ja tietojärjestelmässä tehtävien toimintojen kannalta kaikkein olennaisimpiin kysymyksiin. Tämä edellyttää siten sitä, että yksittäisen hallintopäätöksen esittelyn ja ratkaisemisen sekä siihen liittyvien kirjaamis- ja muiden yksittäistoimien rinnalla koko järjestelmän toimivuuden kannalta keskeiset järjestelmätason ratkaisut ovat huolellisesti valmisteltuja ja dokumentoituja sekä selkeästi tunnistettavissa olevien toimijoiden ja näille selkeästi määriteltyjen vastuiden piirissä.

Tiedonhallintalaissa voitaneen harkita tästä tarkempia yleisiä säännöksiä ja automaattisen päätöksenteon osalta näitä harkittaneen osaksi hallintolakia.

Arviomuistion sivulla 43 nostetaan esille hyvin olennainen kysymys, joka sivuaa virkavastuuta, nimittäin tehokkaan oikeussuojan mahdollistavien menettelyiden riittävyys ja niiden riittävä ajantasaisuus. Tämä on vähintäänkin yhtä olennainen kysymys kuin virkavastuun kohdentuminen, ja osaksi kohdistuu valtiovarainministeriön asettaman työryhmän tehtävänannon ulkopuolelle ja enemmän oikeusministeriön vastuulla olevaan yleislainsäädäntöön. Laillisuusvalvontaan perustuvan käsitykseni mukaan niin oikaisumenettelyssä kuin hallintovalituksessa on automaation yhteydessä tarvetta yhä

enemmän arvioida esikysymyksenä tietojärjestelmien ja datan hyödyntämisen ja sen prosessien oikeudellista virheettömyyttä ja muuta asianmukaisuutta. Tämän lisäksi ylimpien laillisuusvalvojien suorittamalla valvonnalla on selkeä tarve ja täydentävä rooli oikeusturvan toteuttamisessa sen lisäksi mitä tietosuoja-asetuksessa ja tietosuojalaissa säädetään tietosuojaan kiinnittyvien vaatimusten toteuttamisessa oikeusturvasta.

7. Mitä edellytyksiä tietovarannoille, niiden laadulle tai niiden käytölle tulisi lainsäädännössä asettaa, jotta niitä voidaan käyttää osin tai täysin automaattisessa päätöksenteossa?

Arviomuistion mukaan 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. Työryhmä katsoo, että tietovarantojen vastuiden ja tietojen käytön vastuiden osalta automaattinen päätöksenteko edellyttäisi nykyistä tarkempaa sääntelyä.

Hyvän hallinnon periaatteiden toteutuminen edellyttää, että hallinnon päätöksenteossa käytettävät tietovarannot ja niiden sisältämät tiedot ovat ajantasaisia, kattavia ja sisällöllisesti virheettömiä. Tiedon ja datan sisällöillä ja virheettömyydellä onkin suuri merkitys päätöksenteon ja tietojen hyödyntämisen oikeudellisen asianmukaisuuden kannalta. Samoin yleinen tietosuoja-asetus edellyttää rekisterinpitäjän vastuiden selkeää kohdentamista. Vastaavalla

tarkkuustasolla on myös tarpeen säännellä ja määritellä käytettävän datan ja tietovarantojen virheettömyyttä koskevat vastuut sekä myös vastuut ja mahdollisuus virheellisten tietojen korjaamiseen. Oikeuskanslerin laillisuusvalvontakäytännössä on kohdattu useampaan kertaan tilanteita, joissa virheellisten tietojen korjaamisesta ei ole riittävästi säädetty tai sitten se ei ole teknisesti mahdollista.

Arviomuistiossa viitataan tietojen laatua koskevan sääntelyn osalta Tiedon hyödyntäminen ja avaaminen –hankkeeseen, jossa on laadittu alustavat tiedon laatukriteerit, jotka perustuvat kansainväliseen ISO 25012 –standardiin. Laatukriteerien on tarkoitus valmistua vuoden 2021 loppuun mennessä. Yhdyn työryhmän näkemykseen siitä, että tietojen laatu ei ole vain automaattisesta päätöksenteosta johtuva vaatimus tietojen hyödyntämiselle, vaan päätöksenteossa käytettävän tiedon oikeellisuuden ja virheettömyyden selvittämisvelvollisuus sisältyy yleisesti hallintoasioiden valmisteluun. Yleisellä tasolla hahmotellut laatuperiaatteet ovat nähdäkseni oikeaan osuneita ja olennaisia.

Olen tiedon avaamista ja hyödyntämistä koskevasta hankkeesta antamassani lausunnossa (OKV/827/21/2021) ja lausunnossani koskien luonnosta hallituksen esitykseksi avoimen datan direktiivin täytäntöönpanosta (OKV/2147/21/2020) tuonut esille myös sen, että laillisuusvalvonnassa ja hallinnon seurannassa saadun käsityksen perusteella avoimen datan ja sitä toteuttavien rajapintojen käyttöönotto riippuu viranomaisten ja muiden velvoitteen piirissä

olevien julkisten yksiköiden osalta siitä, että näillä on tähän tarvittavat resurssit sekä riittävä kiinnostus toteuttaa rajapintoja.

8. Miten tietoturvallisuuden arviointia ja arviointijärjestelmää koskevaa lainsäädäntöä tulisi kehittää? Entä erityisesti viranomaisten tietojärjestelmien arvioinnin osalta?

Tietoturvallisuuteen liittyviä yleisempiä näkökohtia ja yhteiskunnan informaatioresilienssi:

Pidän tietoturvallisuuteen ja tietosuojan varmistamiseen liittyvien kysymysten selvittämistä myös tämän hankkeen yhteydessä erittäin tärkeänä ja olennaisena. Totean, että liikenne- ja viestintäministeriön asettama työryhmä on selvittänyt yhteiskunnan kriittisten toimialojen tietoturvan ja tietosuojan tasoa, jota työryhmän loppuraportin (1.2.2021) mukaan tulisi nostaa lisäresursseilla ja tehokkaammalla yhteistyöllä. Raportissa todetaan digitaalisen yhteiskunnan koostuvan monista toisistaan riippuvaisista toimijoista, joiden toiminta edellyttää luotettavia ja turvallisia yhteyksiä ja tietojärjestelmiä. Erityisen tärkeää tämä on yhteiskunnan kriittisten palvelujen toiminnassa, kuten terveydenhuolto, energiahuolto, finanssiala, vesihuolto sekä liikenne ja digitaalinen infrastruktuuri ja sen palvelut. Näillä toimialoilla yksittäisetkin tietoturvaa ja tietosuojaa koskevat loukkaukset ja häiriöt voivat vaikuttaa suoraan kansalaisten elämään ja kansantalouden toimintaan.

Olen edellä mainitun työryhmän väliraportista antamassani lausunnossa (OKV/2881/21/2020) pitänyt raportin ehdotuksia poliittisiksi linjauksiksi kannatettavina. Viranomaisten ja kriittisten toimialojen tiedon turvaaminen on olennaisen tärkeä osa yhteiskunnan tehokkaan toiminnan ja myös yksilön perusoikeuksien suojan varmistamista. Tietoturvan ja tietosuojan parantaminen on välttämätöntä yhä enemmän digitalisoituneessa yhteiskunnassa. Tätä osoittavat viime aikoina esiin tulleet ja uutisoidut tietomurrot ja tietosuojaloukkaukset, muun muassa https://www.mtvuutiset.fi/artikkeli/kolmeen-valtionhallinnon-palvelimeen-ehka-tunkeuduttu-vakavan-haavoittuvuuden-avulla-kattavaa-korjauspaivitysta-ei-ole-olemassa/8124314. Myös valtionhallinnon tietojärjestelmien tekninen haavoittuvuus on tullut esille yllättävälläkin tavalla, https://yle.fi/uutiset/3-12031335 ”Yksi kaivinkoneen kauhaisu lamaannutti valtionhallinnon tietoliikenteen päiväksi”).

Asiaan liittyy keskeisesti häiriötilanteisiin varautuminen. Työryhmä esittää arviomuistiossaan, että tiedonhallintalaissa 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. Työryhmän mukaan viranomaisen on pystyttävä suorittamaan tehtävänsä myös tilanteissa, joissa tietojärjestelmää ei voida käyttää.

Edellä mainittuihin näkemyksiin on helppo yhtyä. Jatkovalmistelussa tulisi kuitenkin pohtia, mikä olisi soveliain säädös edellä mainittujen vaatimusten asettamiselle. Kuten edellä olen todennut, tiedonhallintalaissa on jo nykyisellään säännökset muun ohessa tietojärjestelmien ja tietoaineistojen tietoturvallisuudesta sekä tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden varmistamisesta testauksilla. Tärkeää on myös, että tietoturvallisuuden ja vaatimustenmukaisuuden todentamisen menettelyt ovat riskeihin nähden oikeasuhtaisia.

Lisäksi kiinnitän huomiota datan ja tiedon sekä tietojohtamisen ja tiedolla johtamisen yleiseen yhteiskunnalliseen merkitykseen erilaisiin häiriötilanteisiin varautumisessa. Esimerkiksi covid-19 – pandemian yhteydessä on ilmennyt tilanteita, joissa ei ole ollut riittävän nopeasti saatavissa yhteiskunnan ja valtion kriisi- ja turvallisuusjohtamisen kannalta tärkeää, eduskunnan perustuslakivaliokunnan edellyttämää tietoa ja dataa. Yhteiskunnan tietovarantoihin, dataan ja

tietoon sekä tietojärjestelmiin liittyvä häiriönsieto- ja palautumiskyky (informaatioresilienssi tai tiedollinen resilienssi; tästä on käytetty myös ilmaisua tiedollinen huoltovarmuus) on jatkoa ajatellen tärkeä kehittämiskohde, jonka riittäviä oikeudellisia puitteita ja sääntelytarpeita olisi myös perusteltua tarkastella.

Tietoturvallisuuden ja vaatimuksenmukaisuuden arviontijärjestelmistä:

Pidän tärkeänä, että yhtäältä vaatimustenmukaisuutta ja toisaalta tietoturvallisuutta arvioidaan ja voidaan arvioida pätevien ulkoisten arvioitsijoiden toimesta riittävän laajasti ja kattavasti. Arvioinnissa ja tieto- ja kyberturvallisuuteen kohdistuvien riskien tunnistamisessa ja arvioinnissa tärkeää on myös hyvä yhteistyö ja tietojenvaihto tiedusteluviranomaisten kanssa. Samoin tarvitaan niin tieto- ja kyberturvallisuuden kuin tietojärjestelmien olennaisten vaatimusten täyttymiseen myös selkeälle oikeudelliselle perustalle perustuvat arviointikriteeristöt, joita myös pidetään ajantasaisesti yllä.

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

-

10. Muut yleiset kommentit arviomuistiosta

Arviomuistiossa käsitellään kattavasti, ajantasaisesti ja monipuolisesti julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeita. Arviomuistiossa on tunnistettu keskeiset kehitystä vaativat kohdat ja esitetty perusteltuja näkemyksiä ja ratkaisuehdotuksia esille tuotuihin kysymyksiin. Muistion vahvuutena on myös se, että siinä on hyvin kuvattu ylimpien laillisuusvalvojien eli valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen tietojärjestelmiä koskevaa ja sinänsä varsin laajaa laillisuusvalvontakäytäntöä. Muistio toimii erinomaisena pohjana asian jatkovalmistelulle.

Karjalainen Tuula
Oikeuskanslerinvirasto