Lausunto

06.09.2021

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

Arviomuistio vaikutti kattavalta ja informatiiviselta katsaukselta nykylainsäädäntöön esim. vastuiden ja käsitteiden määritelmien osalta. Otsikoinnista (tietojärjestelmät) huolimatta muistiossa arvioitiin mielestämme myös laajalti tiedonhallinnan sääntelyn nykytilaa.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Kiinnostavaa oli pohdinta siitä, onko toimintaprosessi ensisijainen ja tietojärjestelmät toimintaprosessin eräs toteuttamisen apuväline, jolloin missä määrin vastuut kohdistuisivat itse asiassa prosessille ja sen lopputulemille ja mikä on puolestaan tietojärjestelmän rooli itsenäisenä prosessista riippumattomana vastuun ja sääntelyn kohteena. Eittämättä tietojärjestelmiin liittyy omia, niiden tukemista prosesseista erillisiä kysymyksiä, mm. asianmukaisuudesta sekä vastuista tietojärjestelmien suunnittelun ja kehittämisen sekä käyttöönoton ja ylläpidon/operoinnin osalta. Näitä olisi hyvä säädellä niin selkeästi kuin mahdollista - ottaen huomioon niitä selkeyden tavoittamisen haasteita, joita muistio nostaa esiin.

Tietojärjestelmän eri määritelmiä lainsäädännössä oli nostettu esiin ottamatta kantaa niiden välillä. Eri sääntelytarpeissa onkin ehkä tarve eri määritelmillle (esim. rikoslaki). Tähän kontekstiin riittänee tietojärjestelmän määrittely julkisen hallinnon tiedonhallinnan näkökulmasta? Jolloin tietojärjestelmää voisi ehkä tarkastella lainsäädännön näkökulmasta hallinnollisena kokonaisuutena, johon voi kuulua erilaisia teknologisia komponentteja ja niiden ympärillä tapahtuvaa työtä ja käyttöä. Tietojärjestelmää määrittelisivät ainakin tietyt käyttötarkoitukset, tietty joukko sen tallentamia tietoja sekä yksilöitävissä oleva vastuu tästä kokonaisuudesta. Vastuun jakautuessa

usean toimijan kesken löytynee juridiikasta esimerkkejä miten tällaisia usean toimijan yhteisvastuita voidaan pyrkiä täsmentämään. Toisaalta esim. meillä on tilanne, että vastuuta jakautuu organisaation sisällä eri tahoille sisällöllisen vastuun ja teknisen vastuun osalta.

Keskeistä olisi ehkä saada yksi tietojärjestelmä hallinnollisessa mielessä selkeärajaiseksi, vähän kuin kuntaraja maantien laidassa. Sekä mikä osa ICT-teknologiainfrastruktuuria jäisi näin katettujen tietojärjestelmien ulkopuolelle.

Selkeästi osoitettu vastuu tietojärjestelmästä ei vielä ratkaise sitä haastetta, tekeekö vastuullinen taho riittäviä toimenpiteitä, jotta tietojärjestelmä palvelisi asianmukaisesti ko. järjestelmää hyödyntävien ja siitä mahdollisesti riippuvien tahojen toiminnallisia tarpeita. Hypoteettisena esimerkkinä voidaan ottaa vaikkapa kunnan sähköiset palvelut ja Suomi.fi-palvelut. Vaikka tiedettäisiinkin vastuu Suomi.fi-palvelun tietojärjestelmistä, tämä ei varmaankaan vielä takaisi sitä, että ko. järjestelmiä tosiasiallisesti kehitetään vastaamaan mm. kunnan sähköisen asioinnin tarpeisiin, ellei tästä sidosryhmien huomioinnista ja osallistamisesta ole säädetty erikseen. Sama tilanne toistunee muiden yhteisiä palveluja tarjoavien tietojärjestelmien kohdalla.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

Jos tällaisia vaatimuksia pitäisi luetella, eräs keino näiden tunnistamiseksi voisi olla tarkastella sopivalla otannalla julkisten tietojärjestelmähankintojen ei-toiminnalisia vaatimuksia sekä erilaisia kirjattuja arkkitehtuuriperiaatteita läpi ja katsoa, olisiko niistä yleistettävää lainsäädännön tasolle. Haasteena toki saada näistä teknologiariippumattomia ja aikaa kestäviä. Standardeihin nojaamisessakin on omat haasteensa, kuten muistiossa esitettiin.

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

Teknisiä vaatimuksia voi olla haasteellista kirjata lakitekstiin niin, ettei säätely vanhene nopeasti tai hankaloita tekemistä tarpeettomasti (teknologioiden nopea kehitys).

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

Julkisissa kilpailutuksissa olisi eduksi, jos voitaisiin viitata jossakin kuvattuihin yleisiin tietojärjestelmäratkaisujen dokumentointivaatimuksiin. Tiedossamme ei ole suoraan tällaiseen käyttöön sopivaa yleiskäyttöistä järjestelmädokumentaatioiden kuvausta. Pohjamaterialaia sellaiseen voisi löytyä esim. systeemityömalleista. Haasteeksi muodostuu, mikä on tällöin ehdottomasti vaadittavaa ja mikä on soveltuvin osin vaadittavaa. Yhdet ja samat dokumentointikäytännöt eivät sovi kaikkiin tietojärjestelmähankintoihin. Kattava viitekehys, josta voitaisiin "rastittaa ruutuun" edellytettäväksi vain tietyt dokumentit vähimmäissisältövaatimuksineen riippuen siitä, mitä ollaan hankkimassa, voisi toimia. Tämä edelyttäisi tosin hankinnan toteuttajalta riittävää perehtyneisyyttä rastittaa oikeat ruudut. (Vastaava haaste on esim. JHS-179 kokonaisarkkitehtuuriviitekehyksen soveltamisessa: viitekehyksessä on paljon hyödyllistä materiaalia erilaisiin arkkitehtuurin kuvaamistarpeisiin, kunhan viitekehystä osataan hyödyntää kulloiseenkin tarpeeseen soveltuvin osin eikä pakollisena sapluunana. Toisaalta

esim. rakennusteollisuudessa taidetaan olla pidemmällä kypsyystasolla siinä, että tietyt kuvaukset osataan tietyn tyyppisisissä rakennuskohteissa vaatia löytyvän suunnitelmista.)

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

Viranomaisen ja muiden toimijoiden vastuut ja ohjeet tulisi täsmentää kun järjestelmä vanhenee, poistetaan käytöstä tai käyttötarkoitus muuttuu alkuperäisestä. Koko järjestelmän elinkaari tulisi huomioida.

Miten vahingonkorvausvastuut määräytyvät jos useita toimijoita vastuussa järjestelmästä ja prosessista. Monitoimijaympäristöissä toimivien viranomaisten ja eri toimijoiden vastuut ja ohjeet järjestelmän kehittämisessä, testaamisessa, käyttöönotossa ja ylläpidossa ja alas ajossa/sulkemisessa monitoimijaympäristössä tulisi selventää.

Rekisterinpitovastuu, kun useita toimijoita. Nyt verkostomaisesti tuotetuissa ja käytetyissä digitaalisissa ratkaisuissa, joissa sisällöllisestä omistajuudesta ja laadusta vastaavat useat eri organisaatiot, on "pakotettu" nimeämään yksi organisaatio rekisterinpitovastuuseen kun tosiasiallisesti rekisterinpitovastuu on aidosti useilla organisaatioilla, ei yhdellä. Toisin sanoen selventää lainsäädäntöä ja ohjeistusta kun on kyseessä useita rekisterinpitäjiä, sisällöllisiä omistajaorganisaatioita saman järjestelmän piirissä.

Järjestelmän toimimattomuuden, ongelmatilanteen varautumissuunnitelman vastuissa ja ohjeistuksessa lisättävä vaihtoehtoisen tiedon välityksen ja asiankäsittelyn menettely jos järjestelmä ei ole toimintakunnossa, tietoliikenneyhteydet alhaalla ns. varasuunnitelma.

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

Useiden organisaatioiden yhteiset tietovarannot ja tietojen hyödyntäminen näiden välillä ohjeet ja vastuut selvennettävä. Myös tietojen yhteisomistus ja hyödyntäminen tulisi määritellä. Kertyneen ja jalostetun tiedon IPR voitaisiin näin jakaa eri organisaatioiden kesken.

Vaatinee tarkempaa tiedon elinkaaren ja siihen liittyvien prosessien kuvaamista ja näiden prosessien noudattamisen valvomista sekä tiedon alkuperän (data lineage) tuntemista. Mistä kaikkialta uusi tieto voi syntyä tai olemassa oleva muuttua, kuka vastaa mistäkin muutoksesta. Vaatii parempaa laatua myös tietosisältöjen määrittelyiltä ja niiden kuvausten saatavuudelta tarvitsijoiden käyttöön (nykyisin joidenkin yhteiskäyttöisten rajapintojen kuvaukset voivat olla ylimalkaisia tai vanhentuneita ja vasta haetussa datassa näkee tosiasiallisen vastauksella tulevan arvojoukon tms.; tiedon laatua koskevaa metatietoa ei useinkaan ole annettu).

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

Lainsäädäntöä pitäisi kehittää kattamaan tietoturvallisuuden ja henkilötietojen tietosuojan minimitaso, johon jokaisen järjestelmän tulisi kuntahallinnossa päästä. Mitä vaatimuksia järjestelmän tulee toteuttaa ja mitä järjestelmä ei ainakaan saisi tehdä, jotta se olisi asianmukainen. Esim. käynnykkäsovelluksien tietoaineistojen myynti kolmansille osapuolille joka ei nyt laitonta mutta hyvin kyseenalaista. Erityisesti jos kyseiset kuntapalvelut ovat välttämättömiä kuntalaiselle. Kyse ei välttämättä ole jo nykyisin arkaluontoiseksi luokitellusta tiedosta vaan kuinka tietoa käytetään. Myös tietojärjestelmän toimittajan"tuotevastuu" tässä mielessä.

Tietoturvallisuuden arviointia ja arviontijärjestelmää voisi kehittää Kyberturvallisuuskeskuksen kybermittarin viittoittamalta pohjalta, jossa myös kuntien ja arviointitahoje saatavilla on selkeä mittaristo, jonka perusteella arvioida ja pisteyttää omaa toimintaa ja omia tietojärjestelmiä. Mikäli pisteytykset olisivat esimerkiksi julkisessa kansallisessa rekisterissä, niin kuntien tietoturvan tilannetta olisi mahdollista numeerisesti vertailla toisiinsa. Tietoturva on kaikille kunnille yhteinen tarve, siitä huolimatta kaikki kunnat tekevät sen työn nyt toisistaan irrallaan. Arvioinnilla ja arviointijärjestelmällä voitaisiin luoda kehikkoa kuntien väliselle tietoturvallisuuden yhteistyölle. Nykyisellään kybermittaristo on tähän liian laaja, pitäisi alkaa pienestä ja helposta siitä edetä kohti hienojakoisempaa erittelyä. Kuitenkin siten, että jo alusta lähtien kuntien väliset erot on havaittavissa.

Viranomaisten vastuun kohdentumista eri toimijoiden kesken mm. monitoimittajapalveluissa voisi selkeyttää.

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

Lainsäädäntöä ja sääntelyä laadittaessa tulisi tämä tehdä niin että se ei tartu lillukanvarsiin, eli on ”mahdollistava” eikä mene turhiin yksityiskohtiin ja toisaalta kun asetetaan valvonta-, seuranta- ym. vastuista niin nämä vaativat resursseja ja osaamista. Julkisissa hankinnoissa voisi olla eduksi, että teknologian ja tiedon väärinkäytöksistä olisi riittävät sanktiot, taloudelliset sanktiot, toimintakiellot ja toimintakieltoon asetettujen organisaatioiden tiedot tulevat olla julkisia.

10. Muut yleiset kommentit arviomuistiosta

Arviomuistiossa keskityttiin tarkastelemaan pitkälti asiankäsittelyyn liittyviä tietojärjestelmiä hallintolain näkökulmasta, mikä on ymmärrettävää kun keskiössä on ollut automaattisen päätöksenteon asettamien asianmukaisuusvaatimusten pohtiminen. Kuitenkin kunnan tietojärjestelmäkannassa on paljon myös palveluiden tiedonhallintaan liittyviä järjestelmiä, joista osassa voi asianhallinta olla sivuroolissa (esim. opetuksen järjestelmät). Millaisia asianmukaisuusvaatimuksia palvelun tiedonhallintaa toteuttaviin tietojärjestelmiin liittyy? Vaikkapa hammashoidossa, perusopetuksessa tai katujen kunnossapidon ohjauksessa? Toki esim. tekoälyyn liittyvissä kysymyksissä vastuut ym. määrittynevät näitä tehtäviä ja prosesseja sekä niiden lopputuloksia koskevan sääntelyn kautta, kuitenkin joitakin asianmukaisuusvaatimuksia kohdistunee tietojärjestelmiinkin.

Säännösten toimeenpanoon liittyvien tarpeiden ja muutosten vaikutukset pitäisi arvioida laajemmin kuin taloudellisilla vaikutuksilla: mm. vaikutukset kuntalaisiin, ympäristöön, organisaatioon ja henkilöstöön.

Vaikutuksia tulee arvioida sekä lyhyellä että pitkällä aikajänteellä.

Tekoälyn seurannan ja valvonnan vaikeuteen (blackbox) tulisi säännellä input ja outputia. Eli velvoittaa jäljitettävyys sille, mitä tietoa tekoälylle tarjotaan ja mitä saadaan tuotokseksi, tuotoksen laadun varmistamisen edellyttäminen esim. automaattisessa päätöksenteossa. Jotta automaattisen päätöksenteon valvonta ei olisi pistokoemaista vaan säännönmukaista, säännöllistä. Tulee myös miettiä tarkoin mitkä ovat seuraukset tekoälyn käytöstä johtuvista virheistä, virheellisistä päätöksistä. Johtuuko virhe lähtötiedon virheellisyydestä, tiedon laatu heikko, vai järjestelmä/algoritmin ohjelmointivirheestä. Vastuut, viestintä ja sanktiot määriteltävä näiden osalta.

Millainen on hyvässä uskossa viranomaiseen päätökseen luottavan kansalaisen tai muun oikeussubjektin vastuu tarkistaa viranomaisen automaattisen päätöksenteon lopputulemat? Päätöksen saajalle voi aiheutua vahinkoa esim. saaduksi oletetun edun menetyksestä myöhemmässä tarkastelussa. Olisiko viranomaisen tällöin tullut olla huolellisempi jo lähtökohtaisesti.

Tarkistusvaatimuksessa esim. asiakkaan pyynnöstä vastuu/ohjeet missä tilanteissa viranomaisen on tarkistettava ja missä ei tarvitse tarkistaa. Tarkistustoiminta kuormittaa, vaatii resursseja tämä huomioitava. Lisäksi voi esiintyä häiriökäyttäytymistä, jolloin asiakas voi viranomaiselta vaatia jatkuvasti tarkistusta. Perustelut tarkistukselle.

Wollsten Piia
Espoon kaupunki - Kokonaisarkkitehtuurityöryhmä