CSC-Tieteen tietotekniikan keskus Oy

Lausunto

06.09.2021

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

CSC kiittää työryhmää kattavasta nykytilan kuvauksesta. Erilaiset tietojärjestelmät ovat nykyisin olennainen osa kaikkien organisaatioiden toimintaa, joten arvioinnin kohde on laaja ja monitahoinen.

Yhteiskunta on riippuvainen erilaisista tietojärjestelmistä sekä IT-palveluista, ja siksi sääntelyn tulisi olla nykyistä huomattavasti selkeämmin määriteltyä ja vaikutukseltaan kattavampaa ja tehokkaampaa. Teknologia kehittyy lainsäädäntöä nopeammin, joten aikaa kestävien lakien laatiminen on haasteellista. Lisäksi lainsäädännön monialaisuus ja toisaalta tietojärjestelmien erilaiset käyttökohteet asettavat omat haasteensa.

CSC toteaa, että nykytilan kuvauksessa tulisi kiinnittää huomioita järjestelmien ohella erityisesti IT-palveluihin, koska tietojärjestelmät eivät sellaisenaan vielä tuota tai käsittele tietoa. Painopiste on pilvipalveluiden ja ulkoistusten ohella selkeästi siirtynyt järjestelmistä palveluihin. Harvalla viranomaisella on enää kokonaan itse kehitettyjä ja ylläpidettyjä tietojärjestelmiä, vaan niitä toimittavat ja ylläpitävät myös puolijulkiset ja kaupalliset toimijat. Tämä tulee huomioida myös tulevassa lainsäädännössä ja sitä alemman tason sääntelyssä.

Lainsäädäntöä kehitettäessä on huomioitava kasvavista haasteita lieventää tietoturvariskejä nykyisen perinteisen julkisoikeudellisen sääntelyn puitteissa. Esimerkiksi kansainvälisten pilvipalveluiden käyttö julkisen sektorin palvelutuotannossa ja siihen mahdollisesti liittyvä tietojen tosiasiallinen siirtyminen EU-alueen ulkopuolelle on huomioitava ja arvioitava sääntelytarpeen näkökulmasta.

Työryhmä on ansiokkaasti huomioinut myös käynnissä olevat lainsäädäntöhankkeet, esimerkiksi EU:n valmisteilla olevan tekoälyasetuksen, joka tulee osaltaan vaikuttamaan merkittävästi tekoälyn käyttöön myös suomalaisissa viranomaisissa.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Tietojärjestelmiä koskevan lainsäädännön tulee asettaa yleiset periaatteet, rajat ja vaatimukset tietojärjestelmien hyödyntämiselle. Lainsäädännön tulee olla teknologianeutraalia, jolloin se määrittää ensisijaisesti sääntelyllä tavoitellut vaikutukset, ei tapoja tai teknologioita niiden saavuttamiseksi. Tietojärjestelmä on väline tiettyjen asioiden toteuttamiseksi tai tavoitteiden saavuttamiseksi.

Kuten muistiossa todetaan, tietojärjestelmän määritelmä ei ole yksikäsitteinen. Lainsäädäntöä uudistaessa tulee pyrkiä mahdollisimman yksikäsitteiseen määritelmään ja pyrkiä välttämään tulkinnanvaraisuutta. Toisaalta määritelmien tulisi olla niin laveita, että ne kestävät aikaa ja teknologian kehitystä. Määritelmällisesti myös IT-palvelu tulisi tunnistaa sääntelykohteena asianmukaisella kuvauksella.

Kaikkia automaattisen päätöksenteon ja tekoälyn mahdollisuuksia hyvän hallinnon toteuttamiseksi ja kansalaisen oikeusturvan varmistamiseksi sekä oikeutettujen etujen ja palveluiden saamiseksi on tuskin vielä edes mahdollista tunnistaa tai ennakoida. Lainsäädäntö tulee näin ollen rakentaa siitä näkökulmasta, että sen soveltaminen lähtökohtaisesti mahdollistaa myönteisiä asioita, eikä rajoita kansalaisen oikeuksien tai hyvän toteutumista, vaikkei tapoja näiden syntymiseen tietojärjestelmien avulla vielä tunnettaisi.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

Tietojärjestelmien toimintavarmuudessa tulee kiinnittää huomiota erityisesti tietoturvaan ja tietosuojaan. Haavoittuvuudet ja tietovuotojen riskit erityisesti erilaisten kyberuhkien varalta on huomioitava. Digitaalinen toimintaympäristö vaatii toimiakseen keskeytymätöntä sähköä sekä muuta ITC-infrastruktuuria, mikä on huomioitava toimintavarmuuden näkökulmasta.

On huomattava, että viranomaisten tietojärjestelmät sisältävät paljon henkilötietojen kasautumia ja yksityisyydensuojaan kuuluvaa tietoa kansalaisista. Tällaisenkin tiedon käsittelyä ja hallintoa ohjaa tiedonhallintalaki ja tietosuoja-asetus. Tällaisten aineistojen käsittelyssä on noudatettava erityistä huolellisuutta, ja sen säilyttäminen ja käsittely tulisi rajata suomalaisille toimijoille, joiden palvelimet ja konesalit sijaitsevat Suomessa.

Tietojärjestelmien yhteentoimivuus tulee huomioida keskeisenä edellytyksenä laajalle tiedon hyödyntämiselle yhteiskunnassa. Tämä ei tarkoita pelkästään teknisten järjestelmien yhteentoimivuutta, vaan lisäksi tarvitaan myös semanttista, organisatorista ja lainsäädännöllistä yhteentoimivuutta, eurooppalaisen yhteentoimivuusviitekehyksen* mukaisesti. Yhteentoimivuuden eri tasojen systemaattinen tarkasteleminen on tärkeää, jotta esimerkiksi eri sektoreiden tekniset järjestelmät keskustelevat keskenään, niissä liikkuva data on kaikille käyttäjille semanttisesti ymmärrettävässä muodossa, jotta ihmiset ja organisaatiot tekevät yhteistyötä, ja jotta lainsäädäntö ei muodosta esteitä datan liikkuvuudelle. Myös tietoturvan varmistamisen osalta tulee noudattaa yhteentoimivia normeja ja parhaita käytäntöjä.

Yhteentoimivuuden edellytyksistä CSC haluaa kiinnittää erityistä huomiota tietojärjestelmissä käsiteltävien aineistojen metatietojen yhdenmukaistamiseen kautta linjan julkisessa hallinnossa. Edelleen myös asiakirjaa pienemmillä yksiköillä, tiedon osilla, tulisi olla oma pysyvä tunnisteensa, jotta niiden yksiselitteinen käsittely eri toimijoissa olisi mahdollista.

Asianmukaisuus käsitteenä saattaa olla sopiva termi viittaamaan tunnettuihin parhaisiin ylläpito- ja tietoturvakäytäntöihin. Vaarana kuitenkin on, että sääntely jää tylpäksi koska ylätason abstrakteja periaatteita ei edellytetä toteutettavaksi käytännön tasolla, jolloin asianmukaisuus jää vain periaatteelliseksi tavoitteeksi. Näin ollen asianmukaisuus tulee vähintään lainvalmistelun esitöissä määritellä tarpeeksi tarkasti, jottei sen sisällöstä synny tulkinnanvaraisuutta.

* https://ec.europa.eu/isa2/eif_en

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

Teknisten vaatimusten tulee perustua teknisiin ja operatiivisiin standardeihin ja vaatimuskriteereihin, joiden toteutumisesta tulee voida varmistua. Hyvä esimerkki vaatimuskriteeristä on tietoturvallisuuden arviointikriteeristö Katakri, jonka vaatimusten toteuttaminen valitettavasti on kuitenkin liian raskasta, kallista ja hidasta jotta se olisi käyttökelpoinen myös muun kuin turvallisuusluokitellun tiedon suojaamiseen. Perustason hallintoasioiden tietojärjestelmille ja IT-palveluille tulee siksi luoda joustavampi ja tehokkaampi vaatimusmäärittely, esimerkiksi samoilla tavoitteilla kuin VAHTI 2/2011 ja VAHTI-100 -ohjeissa, joista edellä mainittu viittasi suoraan jo kumottuun tietoturva-asetukseen.

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

Vaatimusten tulee lähtökohtaisesti olla toiminnallisia, eikä niiden tule keskittyä liikaa dokumentaatioon. Vaatimusten tulee viitata teknisiin ja operatiivisiin vaatimuskriteereihin sekä toteutusten jatkuvaan parantamiseen. Riittävä dokumentaatio on kuitenkin tärkeää etenkin silloin, kun järjestelmiä hankitaan ulkopuolisilta toimittajilta, käytännössä yksityisiltä palveluntuottajilta.

Avoimen lähdekoodin käyttöä edistämällä lisätään päätöksenteon näkyvyyttä myös siinä mielessä, että näin ehkäistään niin sanottu vendor lock-in -tilanne, jossa palvelun tilaaja on sidottu yhteen toimittajaan.

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

Lainsäädännössä tulee määrittää velvoitteita testata järjestelmien ja palveluiden toiminnallisuutta niiden koko elinkaaren ajan, myös poikkeamien käsittelyn harjoittelusta tulee varmistua.

Automaattisessa päätöksenteossa henkilökohtainen virkavastuu ei välttämättä ole mahdollista nykyisessä muodossaan. Tällöin on entistä tärkeämpää, että päätöksen kohteena olevalla henkilöllä on tosiasiallinen mahdollisuus saada riittävästi tietoa päätöksen perusteista, siihen vaikuttaneista häntä itseään koskevista seikoista, sekä mahdollisuus saattaa asiansa uudelleen arvioitavaksi tai valittaa päätöksestä.

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

Erityisesti automaattisessa päätöksenteossa tietojen oikeellisuus on tärkeää. Kansalaisella tulee olla mahdollisuus tarkistaa itseään koskevat tiedot, joiden perusteella häntä koskeva automaattinen päätös on tehty. Automaattisen profiloinnin osalta tietosuojalainsäädäntö asettaa erityisiä vaatimuksia. Alaikäisten lasten kohdalla vastaava mahdollisuus tulee olla heidän huoltajillaan.

Lainsäädännössä tulee asettaa velvoitteita, jotta voidaan varmistua tietovarantojen laadusta, turvallisuudesta ja käytettävyydestä automaattisten testauksen sekä testausmetriikkaan reagoinnin avulla.

Yhteentoimivuus muiden tietovarantojen kanssa ja tarvittava tietoturva tulee huomioida jo siinä vaiheessa, kun uusia tietovarantoja suunnitellaan. Jo olemassa olevien tietovarantojen osalta yhteentoimivuutta tulee aktiivisesti kehittää.

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

Viranomaisten tietojärjestelmiä tulee arvioida ja auditoida ulkopuolisen tahon toimesta. Kuitenkin ensisijaista on tietoturvallisuus- ja tietosuojanäkökohtien huomioiminen jo suunnitteluvaiheessa, jota varten tulee määritellä selkeä velvoite ja varmistusmekanismi

Perustason järjestelmille tulee luoda ketterät tietoturvallisuuden ja tietojärjestelmien arviointikriteerit. Testaus tulee suorittaa vakiomuotoisesti pääasiassa kaupallisten arviointilaitosten toimesta. Tavoitteena tulee olla, että pienempien kokonaisuuksien osalta testaus voidaan yleensä tehdä muutamassa päivässä viikkojen tai kuukausien sijaan.

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

Sääntelyn tulee olla selkeää ja yhdenmukaista. Teknologia kehittyy lainsäädäntöä nopeammin, joten lähtökohtana tulisi olla tästäkin näkökulmasta aikaa kestävä sääntely. Prosessien digitalisoituminen, automaattinen päätöksenteko ja tekoäly tuovat julkiseen hallintoon ja viranomaistoimintaankin mahdollisuuksia, joita on jo osittain tunnistettu. Kaikkia teknologian kehityskulkuja on kuitenkin mahdoton ennakoida. Lainsäädäntöä tulee siksi kehittää teknologianeutraalisti ja mahdollistamisen näkökulmasta siten, että sääntely ei mene tarpeettoman yksityiskohtaiselle tasolle esimerkiksi tiettyihin teknologioihin sitoutuen, vaan antaa vahvan kehikon, jonka sisällä uusien palveluiden ja toimintamallien kehittäminen on mahdollista.

Teknologinen kehitys tuo mukanaan myös uudenlaisia tietoturvaan ja kyberturvallisuuteen liittyviä uhkia. Esimerkiksi kvanttiteknologia, joka sinänsä avaa valtavia mahdollisuuksia, tulee muuttamaan myös tietoturvaan kohdistuvia vaatimuksia. Kvanttiturvallisia salausmenetelmiä on jo kehitetty, mutta toisaalta jotkin nykyiset salausmenetelmät ovat purettavissa kvanttitietokoneilla. Tällaisiin näkökohtiin tulee lainsäädännössä varautua ennakkoon.

10. Muut yleiset kommentit arviomuistiosta

Haluamme tuoda esiin, että tietojärjestelmien kehittämisessä tarvitaan teknisen infrastruktuurin lisäksi toimialaspesifiä osaamista, jolla varmistetaan eri toimialojen substanssikysymysten huomioiminen tietojärjestelmien rakentamisessa. Järjestelmiä tulee aina kehittää loppukäyttäjän eli ihmisen näkökulmasta. Ylipäänsä tulee huomioida, että ICT-järjestelmät eivät koskaan ole pelkkää tekniikkaa, vaan aina tarvitaan ympärille ihmisiä ja osaamista, jotta järjestelmistä saadaan odotettu hyöty ja lisäarvo yhteiskunnalle.

CSC Tieteen tietotekniikan keskus Oy kiittää mahdollisuudesta saada lausua arviomuistiosta julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista, ja antaa mielellään asiantuntemustaan myös jatkokehittämiseen. CSC on suomalainen ammattikorkeakoulujen, yliopistojen ja valtion omistama erityistehtäväyhtiö, joka tuottaa kansainvälisesti korkeatasoisia ICT-asiantuntijapalveluita tutkimukselle, koulutukselle, kulttuurille, julkishallinnolle ja yrityksille.

Hyppölä Jenni
CSC-Tieteen tietotekniikan keskus Oy