Perustuslakivaliokunnalle

Perustuslakivaliokunta on pyytänyt asiantuntijalausuntoa puhemiesneuvoston ehdotuksesta eduskunnan työjärjestyksen väliaikaisesta muuttamisesta (PNE 3/2020 vp), joka koskee eduskunnan täysistunnon ja valiokuntien mahdollisten etäyhteyksin tapahtuvan päätöksenteon järjestämistä. Esitän lausuntonani asiassa kunnioittavasti seuraavan.

Totean aluksi lausuntoni lähtökohdista, että keskityn arvioimaan ehdotusta tietosuoja- ja -turvalainsäädännön näkökulmista. Otan lausunnossani huomioon asiaan liittyviä valtiosääntöoikeudellisia näkökulmia, joita asiantuntijat ovat antaneet ehdotuksen valmistelun aikana.

Tietosuoja eduskunnan valtiopäivätoiminnassa

EU:n yleistä tietosuoja-asetusta (jäljempänä tietosuoja-asetus) alettiin soveltaa 25.5.2018, ja tietosuoja-asetusta täydentää ja täsmentää kansallisesti säädetty tietosuojalaki (1050/2018). Tietosuojalain eduskuntakäsittelyssä perustuslakivaliokunta otti hallintovaliokunnalle antamassaan lausunnossaan kannan, että ”[v]aliokunnan käsityksen mukaan eduskunnan valtiopäivätoiminta ei kuulu unionin oikeuden soveltamisalalle” ja edellytti, että eduskunnan asemasta ylimpänä valtioelimenä ja EU-oikeuden rajatusta soveltamisalasta seuraa, että esityksessä oleva tietosuojalakiehdotusta on muutettava siten, että eduskunnan valtiopäivätoiminta rajataan pois tietosuojalain soveltamisalalta, jotta lakiehdotus voidaan käsitellä tavallisen lain säätämisjärjestyksessä (PeVL 14/2018 vp, s. 11). Hallintovaliokunta huomioi perustuslakivaliokunnan kannan siten, että tietosuojalain 2 §:ään lisättiin uusi 2 momentti, joka rajaa eduskunnan valtiopäivätoiminnan tietosuojalain soveltamisalan ulkopuolelle.

Käsitykseni mukaan henkilötietojen suoja ei ole kuitenkaan vailla merkitystä valtiopäivätoiminnassakaan, sillä perustuslain 10 §:n 1 momentissa turvattu yksityiselämä ja

henkilötietojen suoja kohdistuvat myös valtiopäivätoimintaan. Yksityiselämän ja henkilötietojen suojaa on huomioitu eduskunnan työjärjestyksen 43 a §:n 2 momentissa, jonka mukaan ”Salassa pidettäviä ovat myös asiakirjat, jotka sisältävät tietoja […] henkilön terveydentilasta tai hänen taloudellisesta asemastaan, jos tiedon antaminen niistä aiheuttaisi merkittävää haittaa tai vahinkoa, jollei huomattava yhteiskunnallinen tarve vaadi niiden julkisuutta.”

EU-tuomioistuin on antanut 9.7.2020 tuomion (C-272/19 VQ v Land Hessen), jossa tuomioistuin totesi, että Saksan Hessenin osavaltion parlamentin vetoomusvaliokuntaa on pidettävä tietosuoja-asetuksen tarkoittamana rekisterinpitäjänä. Tuomiossa todetaan, että vetoomusvaliokunta osallistuu parlamentaariseen toimintaan välillisesti ja sen toiminnan luonne on sekä poliittista että hallinnollista (C-272/19, kohta 71). Tuomiossa ei suoranaisesti ja yksiselitteisesti todeta, että yksinomaan parlamentaarisen toiminnan yhteydessä tulee tietosuoja-asetus sovellettavaksi. Toisaalta tuomion perusteluissa korostetaan tietosuoja-asetuksen laajaa ja yleistä aineellista soveltamisalaa, josta tehtävää poikkeamisperustaa on tulkittava suppeasti (C-272/10, kohdat 67 ja 68). Näin ollen ei voida myöskään yksiselitteisesti poissulkea tulkinta-vaihtoehtoa, etteikö tietosuoja-asetus voisi tulla sovellettavaksi myös parlamentaarisen toiminnan yhteydessä tapahtuvaan henkilötietojen käsittelyyn.

Eduskunnan täysistunnon etä-äänestystä ja valiokuntien etäyhteyksillä tapahtuvaa päätöksentekoa koskeva ehdotus koskee yksinomaan eduskunnan valtiopäivätoimintaa. Katson, että perustuslain 10 §:n 1 momentin mukainen suoja koskee ehdotettuja uusia menettelyjä koskevaan toimintaan ja sen yhteydessä tapahtuvaan henkilötietojen käsittelyyn on sovellettava yleisiä tietosuojaperiaatteita, joita on määritelty mm. Euroopan unionin perusoikeuskirjan 8 artiklassa, kuten henkilötietojen käsittelyn asianmukaisuusvaatimus ja käyttötarkoitussidonnaisuus.

Tietoturva eduskunnan valtiopäivätoiminnassa

Julkisen hallinnon tiedonhallinnasta annettua lakia (906/2019, jäljempänä tiedonhallintalaki) sovellettaneen myös valtiopäivien toimintaa tukeviin tietojärjestelmiin, joiden järjestäminen kuuluu eduskunnan kanslian tehtäviin luoda eduskunnalle edellytykset hoitaa sille valtioelimenä kuuluvat tehtävät (eduskunnan työjärjestys 74 §:n 1 momentti). Tiedonhallintalain 3 §:n 1 momentin soveltamisalan mukaisesti ”tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja, jollei muualla laissa

toisin säädetä” kuitenkin 3 §:n 3 momentissa mainituin rajauksin eduskunnan kansliaan ei sovelleta lain 3 lukua.

Valtiopäivätoimintaa tukevien tietojärjestelmien tietoturvallisuudesta ei ole erikseen säädetty, eikä toisaalta liene tarkoituksenmukaista, että niiden sääntely jäisi julkisen hallinnon tiedonhallintaa koskevien tietoturvavaatimusten ulkopuolelle, joten lähtökohtaisesti lain 4 luvun tietoturvaa koskeva säännöksiä sovellettaisiin eduskunnan täysistunnon etä-äänetyksiin ja valiokuntien etäkokouksiin, jollei erikseen lailla toisin säädettäisi. (Ks. myös kunnallisen päätöksentekojärjestelmän etäjärjestelyn mahdollistavan väliaikainen lainmuutos, HaVM 7/2020 vp, s. 4)

Tiedonhallintalain 4 luvussa ei oteta kantaa tietoturvallisuuden tasoon, vaan se on mukautettava kulloisten uhka- ja riskiarvioiden perusteella tapauskohtaisesti (ks. riskiperusteisesta arvioinnista tiedonhallintalain 13 §:n 1 momentti). Tietojärjestelmien tietoturvallisuutta arvioitaessa on hyvä huomata, että täysin tietoturvallista kokonaisuutta ei ole mahdollista saavuttaa. Tietojärjestelmän tietoturvallisuusvaatimustason noustessa, nousevat yleensä järjestelmän suunnittelu-, rakennus- ja ylläpitokustannukset. Tietojärjestelmän riittävä tietoturvallisuustaso voidaan kuitenkin määrittää järjestelmään kohdistuvalla uhka- ja riskiarvioinnilla.

Arvioin, että tiedonhallintalain tietoturvavaatimukset luovat hyvän pohjan eduskunnan valtiopäivätoimintaa tukevien tietojärjestelmien tietoturvallisuuden arvioinnille säännösten yleisluonteisuuden ja riskiperusteisen lähestymistavan vuoksi.

Tietojärjestelmien tietoturvallisuuden arviointiin on olemassa viranomaisten ohjeistuksia ja suosituksia, joissa kaksi keskeisintä ja nyt käsittelyssä olevaan ehdotukseen soveltuvaa ovat:

1. Tietoturvallisuuden auditointityökalu viranomaisille – KaTaKri 2015: https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille
2. Pilvipalveluiden turvallisuuden arviointikriteeristö – PiTuKri v. 1.1 (maaliskuu 2020): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Edellä mainittujen ohjeistusten perusteella on kiinnitettävä huomioita täysistunnon etä-äänestyksessä ja valiokuntien etäyhteyksien järjestämisessä ainakin jäljempänä esiteltyihin seikkoihin.

Fyysinen turvallisuus ja julkisuus

Eduskuntatalon täysistuntosali ja valiokuntien kokoushuoneet tarjoavat fyysisen turvallisuuden monin eri tavoin. Missä määrin eduskunnan rakennusten ulkopuolisen tilan on täytettävä fyysisen turvallisuuden kriteerejä rakennuksen turvajärjestelyjen ja rakenteiden osalta? Miten varmistetaan, että edustaja voi toimia vapaasti ilman ulkopuolista fyysistä uhkaa tai painostusta? Voidaanko edustajan koti tai muu paikka varmistaa tilaturvallisuuden osalta riittävästi? Onko tarpeen asettaa maantieteellisiä tai muita tilaan liittyviä rajoitteita, missä etäosallistuminen voi tapahtua, esimerkiksi Suomen valtion rajojen sisällä ja ylipäätään sisätiloissa? Miten tämä voidaan kontrolloida ja todentaa?

Eduskunnan täysistunnot ovat lähtökohtaisesti julkisia perustuslain 50 §:n 1 momentin mukaisesti. Millä tavalla täysistunnon etä-äänestyksissä on huomioitava julkisuusvaatimus, kun säännönmukaisesti eduskunnan täysistuntoa ja yksittäisten edustajien toimintaa täysistunnossa voi seurata täysistuntosalin yleisölehteriltä taikka verkkolähetyksen kautta?

Edustajan tunnistaminen

Mitkä keinot olisivat riittäviä, jotta voidaan varmistua edustajan henkilöllisyydestä etäjärjestelyissä? Ovatko biometrinen tunnistus (esimerkiksi koneellinen kasvotunnistus), vahva tunnistaminen (pankkitunnukset, mobiilivarmenne tai toimikortti) tai virkamiehen tekemä henkilöllisyyden varmistaminen tai joidenkin näiden yhdistelmät riittäviä keinoja?

Vahvan tunnistamisen välineistä voi todeta, että tunnistusvälineiden antaminen toisen henkilön käyttöön on vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 23 §:ssä ja tunnistusvälineitä koskevissa sopimusehdoissa kielletty. Kiellon kontrollointi on kuitenkin käytännössä vaikeaa.

Tietoliikenneturvallisuus

Mitä vaatimuksia asetetaan käytettävälle tietoliikenneyhteydelle ja yhdyskäytäväratkaisulle? Onko varayhteys oltava, jos ensisijainen tietoliikenneyhteys ei ole käytettävissä? Mikäli etäosallistuminen on mahdollista omasta kodista tai muusta edustajan valitsemasta paikasta, käytettävissä olevan verkkoyhteyden saatavuutta ja laatua ei voida aina varmentaa.

Onko täysistunnon etä-äänestykseen osallistuvan edustajan voitava seurata verkkolähetyksen kautta, miten täysistunnon asiankäsittely ja äänestys etenevät? Entä jos seuraaminen ei onnistu teknisessä yhteydessä tai verkkolähetyksessä olevan vian takia?

Tietojärjestelmä pilvipalveluna

Voidaanko etä-äänestys ja valiokunnan kokouksen etäjärjestely toteuttaa kokonaan tai osittain kolmannen osapuolen palveluna ns. yksityisessä tai julkisessa pilvipalvelussa eduskunnan ulkopuolisessa konesalissa (vrt. nykyinen täysistunnon salijärjestelmän ratkaisu)? Onko mahdollisen pilvipalvelun sijainnille asetettava maantieteellisiä tai muita rajoitteita? Suomen rajojen ulkopuolella tapahtuva tietojenkäsittely asettaa riskejä palvelun saatavuudelle (esimerkiksi ulkomaan internet-yhteydet eivät käytössä tai kapasiteettia ei saatavilla poikkeustilanteessa) ja luottamuksellisuudelle (esimerkiksi tietojen käsittely ulkomaisen yrityksen palvelimelle, johon voidaan soveltaa vieraan valtion lainsäädäntöä).

EU-tuomioistuin antoi 16.7.2020 tuomion C-311/18 (Data Protection Commissioner v. Maximillian Schrems ja Facebook Ireland), joka koskee henkilötietojen siirtomekanismeja EU:sta kolmansiin maihin. Tuomiossa todetaan, että EU:n ja Yhdysvaltojen välinen henkilötietojen siirtoa koskeva Privacy Shield -mekanismi on mitätön, koska Yhdysvaltojen tiedustelulainsäädäntö ei takaa riittävää tietosuojan tasoa. Euroopan tietosuojaneuvosto ei ole toistaiseksi antanut lisätietoja, millä lisätoimilla henkilötietojen siirtoa Yhdysvaltoihin olisi mahdollista jatkaa EU-tuomioistuimen edelleen päteväksi todetun mallisopimuslausekkeita koskevien järjestelyiden puitteissa.

Muita havaintoja

Monimutkainen tietojärjestelmä- ja päätelaitekokonaisuus on helposti vikaantuva kokonaisuus, eikä 100 %:n käytettävyys- ja toimintavarmuutta voida taata. Vaikka täysistuntosalin salijärjestelmä on käytettävyydeltään erittäin korkea, voi siihenkin tulla vika- ja virhetilanteita. Näitä tilanteita varten on varajärjestelyjä, ja äänestysten osalta voidaan toimittaa lippuäänestys koneäänestyksen estyttyä teknisen syyn vuoksi (eduskunnan työjärjestys 61 §:n 3 momentti). Mikäli etä-äänestys ei teknisen tai muun vian vuoksi ole käytettävissä, jääkö ainoaksi vaihtoehdoksi keskeyttää ja siirtää äänestystä? Onko tämä hyväksyttävää?

Minkälainen tukipalvelu on annettava, jotta voidaan ratkaista erilaiset edustajan käyttämät päätelaite- ja verkko-ongelmat (laiterikkoutumiset, tietoliikenneyhteyden hetkelliset katkokset ym.)? Voidaanko hyväksyä, että etäosallistuminen voi estyä niin teknisistä kuin käyttäjän virheistä? Käyttökoulutukseen ja opastukseen on varattava sitä enemmän mitä monimutkaisemmasta käytettävyydestä on kysymys. Myös erilaisiin, osin kaupallisiin ja suljettuihin järjestelmiin ja päätelaitteisiin (älypuhelimet, tabletit ja tietokoneet) liittyvät verkkoyhteydet luovat avoimessa verkossa laajan hyökkäyspinta-alan ulkopuolisille häirintä- ja hakkerointiuhille.

Lopuksi

Etäjärjestelyjä tukevien järjestelmien valinnassa ja rakentamisessa on onnistumisen kannalta tärkeää, että voidaan ensin tunnistaa kaikki valtiosääntöoikeudelliset vaatimukset, joiden on välttämätöntä toteutua etäjärjestelyissä. Sen jälkeen kaikki tunnistetut vaatimukset tulee muodostaa teknisiksi ja toiminnallisiksi vaatimuksiksi tai erilaisten vaihtoehtoisten vaatimuskokonaisuuksien joukoiksi, minkä jälkeen voidaan arvioida kokonaisuuden toteutuskelpoisuus sekä suunnitteluun, rakentamiseen, testaamisen ja käyttöönottoon varattava aika. Näin menettelemällä voidaan jo suunnitteluvaiheessa huomioida mahdollisimman kattavasti tietoturva- ja suojavaatimukset, joiden huomioiminen myöhemmin rakentamis- ja käyttöottovaiheessa ovat vaikeampia tai jopa mahdottomia toteuttaa.

Arvioin, että tietoturvallisin ja teknisesti helpoiten toteutettavissa oleva etätyöskentelymalli perustuisi siihen, että edustajat osallistuisivat täysistunnon äänestyksiin ja valiokuntien kokouksiin eduskunnan tiloissa olevista työhuoneistaan. Etätyöskentely voitaisiin myös järjestää eduskunnan ulkopuolisissa ja ennakkoon valituissa etätyöskentelypisteissä, joihin järjestetään video- ja ääniyhteydet eduskuntaan. Etätyöskentelypisteisiin perustuva malli lienee tietoturvallisesti toteutettavasti, mutta yksityiskohtaisten järjestelyiden suunnittelu ja toteutus veisi jonkin verran aikaa. Tieturvallisesti haastavin toteutustapa olisi, että edustaja voisi vapaasti valita etätyöskentelypaikkansa, erityisesti fyysiseen turvallisuuteen ja henkilön tunnistamiseen liittyvistä syistä.

tietosuojavastaava Mikko Virtanen
eduskunnan kansliassa 1.9.2020