Janne Salminen 24.9.2024

Perustuslakivaliokunta

Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi (HE 57/2024 vp)

Hallituksen esitys

1. Esityksessä ehdotetaan säädettäväksi kyberturvallisuuslaki, ja lisäksi esityksessä ehdotetaan muutettavaksi lukuisia muita lakeja (julkisen hallinnon tiedonhallinnasta annettu laki, sähköisen viestinnän palveluista annettu laki, ilmailulaki, raideliikennelaki, liikenteen palveluista annettua laki, alusliikennepalvelulaki, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettu laki, sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annettu laki, sähkömarkkinalaki, maakaasumarkkinalaki, energiavirastosta annettu laki, sähkö- ja maakaasumarkkinoiden valvonnasta annettu laki, vesihuoltolaki, sakon täytäntöönpanosta annettu laki, maa-asemista ja eräistä tutkista annettu laki ja vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annettu laki). Ehdotetuilla laeilla pantaisiin täytäntöön Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS2-direktiivi). Esityksellä säädettäisiin NIS2-direktiivin vähimmäistason mukaiset kyberturvallisuuden riskienhallinta- ja raportointivaatimukset sen soveltamisalaan kuuluville toimijoille. Samalla kumottaisiin edeltävää verkko- ja tietoturvadirektiiviä (NIS1-direktiivi) täytäntöönpanevat säännökset, koska direktiivi on kumottu NIS2-direktiivilllä. Direktiivin edellyttämistä velvollisuuksista säädettäisiin kyberturvallisuuslaissa, ja julkisen sektorin osalta velvoitteista säädettäisiin myös julkisen hallinnon tiedonhallinnasta annetussa laissa. Valtioneuvoston esityksen mukaan direktiivi implementoitaisiin vähimmäistasollaan ja kansallinen liikkumavara kokonaisuudessaan hyödyntäen.

2. Hallituksen esityksen mukaan lait on tarkoitettu tulemaan voimaan 18.10.2024.

3. Hallitus on arvioinut, että lakiehdotukset voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä. Sen mukaan esitys kuitenkin sisältää muun muassa ehdotuksen haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelystä ja arvion eräiden valtioelinten ja viranomaisten asemasta, minkä vuoksi hallitus pitää suotavana, että perustuslakivaliokunta antaisi asiasta lausunnon.

Arviointia

4. Hallituksen esityksessä on suhteellisen laajasti ja yksityiskohtaisesti arvioitu esityksensuhdetta lukuisiin Suomen perustuslain säännöksiin. Esityksessä on katsottu, että se sisältää perustuslain kannalta merkityksellisiä ehdotuksia suhteessa perustuslain 2.3 §:ssä säädettyyn julkisen vallan käytön lakisidonnaisuuteen, perustuslain 10 §:ssä turvattuun yksityiselämän, henkilötietojen ja luottamuksellisen viestinnän suojaan, perustuslain 15 §:ssä turvattuun omaisuudensuojaan, perustuslain 18 §:ssä turvattuun elinkeinovapauteen, perustuslain 21 §:ssä turvattuun oikeusturvaan, perustuslain 80 §:ssä asetuksen antamisesta ja lainsäädäntövallan siirtämisestä säädettyyn sekä perustuslain 124 §:ssä hallintotehtävän antamisesta muulle kuin viranomaiselle säädettyyn.

5. Valtiosääntöoikeudelliselta kannalta keskeiset ehdotukset sisältyvät uuteen yleislainluonteiseen kyberturvallisuuslakiin ja julkishallinnon toimijat kyberturvallisuussääntelyn piiriin tuovilla muutoksilla julkisen hallinnon tiedonhallintalakiin.

6. Hallituksen esitys tarkoittaa varsin laajaa ja monimutkaista sääntelykokonaisuutta, joka on merkittävä useiden perustuslaissa turvattujen perusoikeuksien kannalta ja perustuslain kannalta myös muutoin. Ainakin osin esityksen hankala hahmotettavuus liittyy sen teknislaatuisuuteen. Pääosin hallituksen esityksessä on huolellisesti arvioiden esitetty ehdotettujen säännösten perusoikeusulottuvuuksia. Osa tarkastelusta, esimerkiksi siltä osin kuin esitystä käsitellään suhteessa elinkeinovapauteen, on perustuslakivaliokunnan, hallituksen esityksessä viitatun lausuntokäytännön valossa vailla ongelmia. En myöskään pidä esitystä säätämisjärjestysperusteluissa käsitellyin osin omaisuudensuojan kannalta ongelmallisena. Käsitelen tässä esityksestä kolmea asiakokonaisuutta, jotka käsitykseni mukaan kuitenkin ovat problemaattisia.

Luottamuksellisen viestin suoja

7. Ehdotetun kyberturvallisuuslain 28.2 §:n mukaan valvovalla viranomaisella on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta välitystieto, sijaintitieto sekä tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten. Valvovan viranomaisen tämän momentin nojalla saamat tiedot on pidettävä salassa. Samasisältöien säännös ehdotetaan sisällytettäväksi lisäksi julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta annetun lain 18.2 i §:ään.

8. Perustuslain 10.1 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslain 10.2 §:n mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. # momentin mukaan Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lisäksi perustuslain 10.4 §:n mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Mahdollisuudet rajoittaa luottamuksellisen viestinnän suojaa säädetty perustuslakiin

tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54, PeVM 25/1994 vp, PeVL 33/2013 vp). Vastaavasti EU:n perusoikeuskirjan 7 artiklassa on säädetty jokaisen oikeudesta siihen, että hänen viestejään kunnioitetaan. Lisäksi Euroopan ihmisoikeussopimuksen 8 artiklan mukaan jokaisella on oikeus nauttia kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen paitsi, kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraaliin suojaamiseksi tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

9. Käsitykseni mukaan valtiosääntöoikeudellinen ongelma ei perustuslakivaliokunnan aikaisemman käytännön valossa tässä liity sähköisen viestin välitystietoihin (ks. PeVL 36/2018 vp, PeVL 18/2014 vp). Ongelmallisena ei lähtökohdiltaan esitettyjen perustelujen valossa vaikuta myöskään kyberturvallisuustietojen vapaaehtoinen jakamisjärjestely. Valtiosääntöoikeudellisesti pulmallinen tulkintatilanne sen sijaan liittyy kysymykseen siitä, missä määrin kyberhyökkäyksen toteuttamiseksi luotu haitallisen tietokoneohjelman tai käskyn sisältävä ”viesti”, jonka ainoa funktio on toimittaa saajan laitteistoon tai tietoverkkoon ym. haitallinen tietokoneohjelma tai käsky, saa perustuslain 10.2 §:ssä tarkoitettua luottamuksellisen viestin suojaa. Sinänsä kysymys voi olla myös koneellisesti laadittu viesti, mutta säännöksissä tiedonsaantioikeus viedään niin pitkälle, että se koskee myös viestin sisältöä (”haitallisen tietokoneohjelman ja käskyn sisältävä viesti”). Lähtökohtaisesti viestin sisältö saa perusoikeussuojaa ja yksityisen viestin sisältö on viestinnän luottamuksellisuuden suojan ydinalueella (PeVL 36/2018 vp). Kannanotto vaikuttaa siihen, miten arvioidaan valvovan viranomaisen tiedonsaantioikeutta. Havaintojeni mukaan perustuslakivaliokunnan aikaisemmassa käytännössä ei ole arvioitu aivan vastaavaa tilannetta.

10. Kuten hallituksen esityksestä käy ilmi, luottamuksellisen viestin salaisuuden suojan ulkopuolelle käytännössä on rajattu viestinnän pääasiallisen luonteen vuoksi liikenteenohjauksessa syntyvä puhe- ja viestiliikenne (PeVL 62/2010 vp) ja ainakin vieraan valtion sotilas- tai muu viranomaisorganisaation viestintä (PeVM 4/2018 vp). Lisäksi postinkulun varmistamiseksi eli viestin lähettäjän ja vastaanottajan viestinnällisten oikeuksien toteutumiseksi on lailla voitu säätää suljetun kirjeen avaamisesta (PeVL 56/2010 vp).

11. Haitallisen tietokoneohjelman ja käskyn sisältävän viestin, usein myös teknisesti laaditun, lähettäminen ja vastaanottaminen on vähintäänkin epätyypillistä kommunikaatiota, jolla ei itse asiassa tavoitella viestintää lähettäjän ja viestinsaajan välillä, lähinnä kysymyksessä on toimi, toki viestinä toiselle lähetetty, joka tähtää kohteensa tietojärjestelmän murtamiseen tai tietojen hankkimiseen siitä jne.

12. Hallituksen esityksessä on katsottu, että kyberhyökkäyksen toteuttamiseksi luotu haitallisen tietokoneohjelman tai käskyn sisältävä viesti ei kuulu *viestinnän luottamuksellisuuden suojan ydinalueelle, etenkään sen teknisten haittaohjelmaan liittyvien ominaisuuksien taikka automatisoidusti luodun sisällön osalta, viestinnän osapuoliksi luettavien luonnollisten henkilöiden välisen sisällön puutteen vuoksi*. Tämän vuoksi kysymys ei olisi perustuslain 10.2 §:n luottamuksellisesta viestinnästä eli sen käsittelystä voitaisiin säätää perustuslain 10.4 §:stä riippumatta. Tällöin haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevaa sääntelyä arvioidaan perustuslain yleisten rajoitusedellytysten kannalta, jolloin voidaan päätyä siihen, että sääntely on välttämätöntä, asianmukaista ja oikeasuhtaista sillä tavoiteltavien hyväksyttävien ja painavan yhteiskunnallisen tarpeen mukaisten tavoitteiden toteuttamiseksi. Käsitykseni mukaan on tulkinnanvaraista missä määrin tällainen epäviesti, jolla ei

ole mitään muuta tarkoitusta, kuin mahdollistaa haitallinen tekninen hyökkäys ylipäätään on perustuslain 10.2 §:n alalla.

Kysymys eduskunnan ja sen virastojen asemasta julkishallinnon toimijoina

13. Julkisen hallinnon tiedonhallinnasta annetun lain 4 a luvussa säädettäisiin kyberturvallisuutta koskevat velvollisuudet ja niiden noudattamisen valvonta. Lain soveltamisala on määritelty ehdotetussa 3 §:ssä. Se noudattelee julkisuuslain 4.1 §:n sääntelylogiikkaa, joka tarkoittaa, että sääntely tulisi sovellettavaksi myös eduskunnan virastoihin.

14. Perusteluna tälle esitetään käsitys siitä, että käsillä olisi sellainen hallinnon yleislaki, joita koskevat säännökset ulottuvat vastaavasti myös eduskunnan virastoihin. Direktiivin perusteella ei vaikuta yksiselitteiseltä, että se nimenomaisesti ulottaisi soveltamisalavaatimuksen myös parlamentin valtiopäivätoimintaan liittyviin ja sitä tukeviin virastoihin.

15. Eduskunnan valtiosääntöinen asema ylimpänä valtioelimenä edellyttää tässä mielestäni sitä, että myös eduskunnan virastot, jotka kuitenkin tämän sääntelyn kannalta ovat kiinteässä yhteydessä eduskunnan valtiopäivätoimintaan ja oletettavasti myös jakavat samat tietoverkot ja tietojärjestelmät, eivät olisi kyseisen lain soveltamisalalla. Se, että ehdotettava muutokset tehdään hallinnon yleislakiin ei tässä sääntely-ympäristössä edellytä, että se tässä sääntely-ympäristössä ulottuisi myös eduskunnan virastoihin. Erityistä merkitystä annan tässä sille, että eduskunnan virastojen kuuluminen lain soveltamisalalle merkitsisi sitä, että ne ovat valtioneuvoston alaisen viranomaisvalvonnan kohteena. Tällainen ratkaisu olisi perustuslain 2 §:ään palautuvan valtiojärjestyksen perusteisiin kuuluvan institutionaalisen perusratkaisun kannalta ongelmallinen. Lainsäädäntövaltaa käyttävä ja valtiontaloudesta päättävä eduskunta on ylimpänä valtioelimenä erotettu hallitusvaltaa käyttävästä valtioneuvostosta. Ellei EU:n oikeus nimenomaisesti edellytä eduskunnan virastojen sisällyttämistä lain soveltamisalalle, mietintövaliokunnan tulisi poistaa ne sieltä. Pidän kysymystä tätä tavallisen lain säätämisjärjestyksen käyttämisen edellytyksenä. (Ks. PeVL 46/2010 vp.)

Lainsäädäntövallan delegointi ja viranomaisen määräyksenantovaltuudet

16. Kyberturvallisuuslain 3.4 §:ään sisältyy ehdotus, jonka nojalla valtioneuvoston asetuksella voitaisiin tarkentaa lain 3 §:n 3 momentissa tarkoitettuja kriteerejä, joiden perusteella liitteessä I tai II tarkoitettua toimintaa harjoittava toimija voisi poikkeuksellisesti kuulua lain soveltamisalaan, vaikka se olisi kooltaan keskisuurta yritystä pienempi.

17. Perustuslain 80.1 §:n mukaan tasavallan presidentti, valtioneuvosto ja ministeriö voivat antaa asetuksia tässä perustuslaissa tai muussa laissa säädetyn valtuuden nojalla. Lailla on kuitenkin säädettävä yksilön oikeuksien ja velvollisuuksien perusteista sekä asioista, jotka perustuslain mukaan muuten kuuluvat lain alaan.

18. Hallituksen esityksen perustelujen valossa asetuksenantovaltuus ei sinänsä vaikuta perustelulta, mutta se on tällaisenaan, siis nimenomaan soveltamisalaan puuttuvana, käsitykseni mukaan myös ongelmallinen perustuslain 80 §:n kannalta.

19. Perustuslakivaliokunta on käytännössään katsonut, että lain soveltamisalan sääntely asetuksella ei ole perustuslain 80 §:n ja säädösten hierarkkisten suhteiden näkökulmasta täysin

ongelmatonta. (Ks. PeVL 14/2005 vp). Käytännössä on pidetty ongelmallisena sitäkin, että asetuksenantovaltuus on laissa säädettyjen kriteerien valossa voinut merkitä sitä, että asetuksenantovaltuutta käyttäen lain soveltamisala on rajoittunut tai supistunut, ks. PeVL 4/2000 vp. (Ks. lisäksi PeVL 8/2002 vp, PeVL 26/2001 vp). Pääosin tilanteisiin on suhtauduttu käytännössä torjuvasti.

20. Perustuslain 2.3 §:n tarkoittaman laillisuusperiaatteenkin kannalta olisi ottaen huomioon lakiin sisältyvät viranomaistoimivaltuudet välttämätöntä, että laista ilmenee sen soveltamisala. Tässä asetuksenantovaltuus voisi perustelujensa mukaan merkitä sitä, että toimija asetuksessa määriteltyjen kriteerien perusteella ”voisi poikkeuksellisesti kuulua lain soveltamisalaan”. Pidän tällaista järjestelyä perustuslain 80 §:n kannalta ongelmallisena, kun lisäksi otan huomioon myös sen, mitä velvollisuuksia toimijalle lain soveltamisalalla olemisesta seuraisi.

21. Kyberturvallisuuslain 9.4 §:n nojalla valvova viranomainen valtuutettaisiin antamaan tarkempia teknisiä määräyksiä kyberturvallisuuden riskienhallinnassa huomioitavista toimialakohtaisista erityispiirteistä sekä kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen riskinarviointien tuloksien huomioimisesta toimialakohtaisessa riskienhallinnassa. Samoin valvovalle viranomaiselle annettaisiin määräyksenantovaltaa kyberturvallisuuslain 11.5 §:n nojalla niin, että valvovalla viranomaisella olisi toimialallaan mahdollisuus antaa tarkempia teknisiä määräyksiä, joilla tarkennetaan 11–15 §:n nojalla tehtävän ilmoituksen, tiedotuksen tai raportin tietosisältöä, teknistä muotoa tai menettelyä. Vielä määräyksenantovaltuus sisältyisi kyberturvallisuuslain 41.4 §:ään. Sen mukaan valvova viranomainen voisi antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta toimijaluetteloon, jota se ylläpitää.

22. Perustuslain 80.2 §:n mukaan myös muu viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä määrätyistä asioista, jos siihen on sääntelyn kohteeseen liittyviä erityisiä syitä eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella. Tällaisen valtuutuksen tulee olla soveltamisalaltaan täsmällisesti rajattu.

23. Käytännössä tällaiset määräyksenantovaltuudet ovat aina poikkeuksellisia (PeVM 10/1998 vp). Perustuslakivaliokunnan käytännössä kuitenkin rajatun erityisalan teknisluonteiset, sisällöltään tekniset määräyksenantovaltuudet on hyväksytty, kun perustuslain 80.2 §:n muut edellytykset ovat täyttyneet. (Ks. esim. PeVL 17/2004 vp ja PeVL 16/2003 vp). Arvioni mukaan olisi valtiosääntöoikeudellisesti mahdollista sisällyttää lakiin nyt ehdotetulla tavalla valtuudet muulle viranomaiselle antaa oikeussääntöjä määrätyistä asioista. Käsitykseni mukaan tässä olisi samanlaisia sääntelyn kohteeseen liittyviä erityisiä syitä, joiden perusteella perustuslakivaliokunnan aikaisemmassa käytännössä on hyväksytty valtuus vastaavaan teknisluonteiseen normiantoon, kun se on soveltamisalaltaan laissa täsmällisesti rajattu, kuten tässä.