Olli Mäenpää
7.4.2026

Perustuslakivaliokunnalle

Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi (U 17/2026 vp)

Valtioneuvoston kirjelmä koskee komission 20.1.2026 tekemää ehdotusta uudeksi kyberturvallisuusasetukseksi, jolla kumottaisiin aikaisempi kyberturvallisuusasetus (2019). Tarkoituksena on vastata paremmin kasvaviin ja muuttuviin kyberturvallisuuden uhkiin ja kyberhyökkäyksiin sekä yhdenmukaistaa ja yksinkertaistaa jäsenvaltioiden käyttämiä keinoja kyberturvallisuuden häiriöihin ja uhkiin vastaamiseksi. Samassa yhteydessä komissio ehdottaa NIS 2-direktiiviin muutoksia, joiden tarkoituksena on laajentaa direktiivin soveltamisalaa merenalaisen tiedonsiirtoinfrastruktuurin tarjoajiin, energia- ja kemianteollisuuden toimijoihin sekä eurooppalaisten digitaalisten identiteetti- ja yrityslompakoiden tarjoajiin

Oikeusperusta

Oikeusperustan arviointi ei kuulu perustuslakivaliokunnalle perustuslaissa osoitettuihin tehtäviin. Oikeusperustan asianmukaisuus on EU-oikeudellinen kysymys, jonka ratkaisee viime kädessä EU-tuomioistuin (esim. PeVL 47/2022 vp, kappale 15). Valiokunta on pitänyt kuitenkin tärkeänä, että unionilainsäädäntöä kehitetään ensisijaisesti perussopimusten puitteissa (esim. PeVL 61/2016 vp).

Asetusehdotuksen ja direktiivimuutoksen oikeusperustana olisi Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artikla, joka mahdollistaa sisämarkkinoiden toteuttamista ja toimintaa koskevien toimenpiteiden antamisen. Oikeusperustaa voidaan pitää asianmukaisena, kun otetaan huomioon, että erityisesti kyberturvallisuuteen liittyvien ei-teknisten riskien kannalta kansallisen lainsäädännön hajanaisuus voisi johtaa sisämarkkinoiden pirstoutumiseen.

Toissijaisuus- ja suhteellisuusperiaate

Asetusehdotuksen ja direktiivimuutoksen toissijaisuus- ja suhteellisuusperiaatteen mukaisuus on EU-oikeudellinen kysymys. Näiden periaatteiden noudattamisen arvioinnin kannalta keskeiset seikat voivat kuitenkin olla merkityksellisiä myös arvioitaessa ehdotuksen suhdetta perusoikeuksiin. Valtioneuvosto pitää alustavasti ehdotusta pääosin näiden periaatteiden mukaisena, mutta kiinnittää huomiota sääntelyn täsmentämiseen jatkoneuvottelujen perusteella. Tähän arvioon ei ole huomauttamista, sillä kyberturvallisuuteen kohdistuvat uhat voisivat heikentää koko unionin tasolla kyberturvallisuuden resilienssiä ja luotettavuutta ja toisaalta jäsenvaltiot eivät yksin pysty tehokkaasti varmistamaan ICT-toimitusketjujen turvallisuutta.

Perusoikeudet

Perustuslakivaliokunta on vakiintuneesti todennut, että perustuslain 1 §:n 3 momentti yhdessä perustuslain 22 §:ssä säädetyn perus- ja ihmisoikeuksien turvaamisvelvollisuuden kanssa merkitsee, että valtioneuvoston tulee osallistua EU-säädösehdotusten valmisteluun tavalla, joka turvaa perus- ja ihmisoikeuksia Suomen lisäksi koko Euroopan unionissa (esim. PeVL 15/2022, kappale 5). Valiokunnan mukaan on selvää, että Suomen perustuslain tulee ohjata valtioneuvoston kannanmuodostusta EU-lainsäädännön valmistelussa (PeVL 20/2017 vp, s. 6).

Tältä kannalta on erityisen merkityksellistä, että ehdotettu sääntely kohdistuisi perusoikeutena suojattujen yksityiselämän ja omaisuuden suojan kannalta merkityksellisiin seikkoihin. Sääntelyllä on merkitystä myös elinkeinovapauden kannalta. Ehdotusten suhdetta perustuslakiin sekä perus- ja ihmisoikeuksiin on kirjelmässä arvioitu varsin yleisellä tasolla.

Yksityiselämän suoja

Ehdotus kohdistuu sellaisiin yhteiskunnan kannalta kriittisiin toimialoihin, jotka toiminnassaan käsittelevät laajasti erilaisia tietoja, mukaan lukien henkilötietoja sekä välittävät luottamuksellista viestintää. Ehdotetuilla muutoksilla on siten merkitystä perustuslain 10 §:n 1 momentissa turvatun henkilötietojen suojan ja 10 §:n 2 momentissa määritellyn luottamuksellisen viestin suojan kannalta. Ehdotuksen mukaan kyberturvallisuushuolia aiheuttavien maiden korkean riskin toimittajat voisivat aiheuttaa ICT-toimitusketjuissa erilaisia riskejä, kuten tietojen vuotamisen tällaisiin maihin. Ehdotuksen mukaisilla toimenpiteillä komissio pyrkisi ennaltaehkäisemään tämäntyyppisiä riskejä (s. 20).

Valtioneuvosto arvioi ehdotuksella voivan olla myönteisiä vaikutuksia yksityiselämän ja luottamuksellisen viestinnän suojan kannalta, mihin arvioon voidaan yhtyä. Jatkovalmistelussa olisi kuitenkin perusteltua arvioida edelleen huolellisesti sääntelyn suhdetta perustuslain 10 §:ään sekä varmistua sääntelyn yhteensopivuudesta kyseisen säännöksen ja sitä koskevan perustuslakivaliokunnan lausuntokäytännön kanssa ottaen huomioon myös luottamuksellisen viestin salaisuuden.

Asetusehdotuksen mukainen tietojen luovuttaminen voisi edellyttää salassa pidettävien tietojen luovuttamista EU:n Kyberturvallisuusvirastolle, komissiolle ja muille jäsenmaille. Ehdotuksessa ei ole tarkemmin arvioitu salassa pidettävien tietojen ja tiedonvaihdon merkitystä. Valtioneuvosto kiinnittää tältä osin jatkovalmistelussa huomiota tiedonvaihtoon liittyvän sääntelyn tarkkarajaisuuteen ja täsmällisyyteen. Sääntelyä tulisi tältä osin mahdollisesti täydentää jatkovalmistelussa.

Omaisuuden suoja ja elinkeinovapaus

Asetusehdotuksen 103 artiklan 1 ja 7 kohdassa perustettaisiin komissiolle toimivallalle kieltää NIS2-direktiivin toimialoihin kuuluvia toimijoita käyttämästä, asentamasta ja integroimasta missään muodossa korkean riskin toimittajien ICT-komponentteja käytettäväksi tuotteidensa ja palvelujensa tarjoamiseksi unionissa.

Käytännössä tämä merkitsisi, että komissio voisi jäsenvaltioita kuultuaan täytäntöönpanoasetuksilla sulkea tietyt toimittajat ulos EU:n markkinoilta ilman lainsäätämisjärjestyksessä käytävää prosessia, jos se on välttämätöntä kyberturvallisuuden varmistamiseksi.

Pelkästään komission täytäntöönpanoasetuksella voitaisiin siten tehdä merkittäviä oikeuksia rajoittavia päätöksiä. Ehdotusta ei tältä osin voida pitää täysin ongelmattomana, sillä ainakin yksilön oikeuksin ja velvollisuuksien perusteista tulee säätää lainsäätämisjärjestyksessä hyväksyttävän asetuksen tasolla (ks. myös PeVL 50/2022 vp, kappaleet 20-21 ja PeVL 37/2021 vp, kappaleet 41-42). Kieltopäätöksen tekoa koskevaa komission itsenäistä päätösvaltaa olisi perusteltua tarkastella tältä kannalta jatkovalmistelussa.

Perustuslain 15 § määrittelee omaisuuden suojan ja 18 § elinkeinovapauden. Vastaavasti EU:n perusoikeuskirjan 16 artiklassa turvataan elinkeinovapaus ja 17 artiklan 1 kohdan mukaan keneltäkään ei saa riistää hänen omaisuuttaan muutoin kuin yleisen edun sitä vaatiessa laissa säädetyissä tapauksissa ja laissa säädettyjen ehtojen mukaisesti ja siten, että hänelle suoritetaan kohtuullisessa ajassa oikeudenmukainen korvaus omaisuuden menetyksestä. Omaisuuden käyttöä voidaan säännellä lailla siinä määrin kuin se on yleisen edun mukaan välttämätöntä. Lisäksi perusoikeuskirjan 52 artiklan 1 kohdan mukaan siinä turvattujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Kieltotoimivallan komissiolle perustavan sääntelyn edellytyksenä olisi ehdotuksen mukaan komission ja jäsenvaltioiden laatima riskiarviointi, josta olisi kuultava täytäntöönpanoasetuksen kohdetta. Rajoituspäätöksen perusteena edellytettäisiin näyttö siitä, että kolmas maa aiheuttaisi vakavan ja rakenteellisen ei-teknisen riskin ICT toimitusketjuille. Näitä edellytyksiä voidaan riittävän täsmällisesti määriteltynä pitää sinänsä hyväksyttävänä ja oikeasuhtaisena perusteena kaikkien jäsenvaltioiden kyberturvallisuutta vahvistavan kieltotoimivallan käytölle myös siltä osin kuin sillä puututaan omaisuuden suojaan ja elinkeinovapauteen.

Asetusehdotuksessa tai sitä koskevassa vaikutustenarvioinnissa ei kuitenkaan ole arvioitu mahdollisia korvausjärjestelyjä tai -vastuita, jotka voivat aiheutua korkean riskin toimittajien ICT-komponenttien käyttökiellosta. Tähän tulisi jatkovalmistelussa kiinnittää huomiota. Tosin korvaukselle vakavan ja rakenteellisen kyberturvallisuusriskin aiheuttamista koskevasta kiellosta ei välttämättä ole esitettävissä erityisen vahvoja oikeudellisia perusteita. Viime kädessä asetuksessa säädetyn kiellon aiheuttaman korvausvelvollisuuden perusteet määrittelisi unionin tuomioistuin.

Seuraamusjärjestelmä

Jäsenvaltioiden olisi asetusehdotuksen 115 artiklan mukaan säädettävä komission täytäntöönpanoasetuksen rikkomisesta määrättävistä seuraamuksista, joiden on oltava tehokkaita, oikeasuhteisia ja varoittavia. Artiklassa määritellään seuraamusten – käytännössä seuraamusmaksujen – enimmäismäärät, jotka ovat huomattavan korkeat, enimmillään seitsemän prosenttia liikevaihdosta. Artiklan perusteella jäsenvaltioilla olisi kuitenkin merkittävää harkintavaltaa niiden ankaruuden määrittelyssä, koska seuraamusten vähimmäismäärää ei määritellä. Tätä voidaan pitää asianmukaisena seuraamusten sääntelyn lähtökohtana. Asetusehdotuksen 103 artiklan säännöksiä, jotka on sanktioitu seuraamusmaksuilla, voidaan myös pitää riittävän täsmällisinä ja ennakoitavina (ks. myös PeVL 7/2026 vp, kappaleet 20-21, PeVL 37/2021 vp, kappale 33).