25.3.2026

Eduskunnan liikenne- ja viestintävaliokunnalle

Huawei Technologies Oy (Finland) Co., Ltd. (“Huawei”) kiittää mahdollisuudesta antaa lausuntonsa valtioneuvoston kirjelmästä eduskunnalle koskien ehdotusta Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) sekä NIS2-muutosdirektiiviksi (U-17/2026 vp).

CSA2-asetus merkitsisi huomattavaa muutosta jäsenvaltioiden ICT-toimitusketjujen sääntelyyn. Ehdotuksen mukaan komissio voisi täytäntöönpanosäädöksillään velvoittaa teleoperaattorit poistamaan huomattavan määrän verkkolaitteita viestintäverkoistaan vain kolmen vuoden siirtymäajan puitteissa ns. ”ei-teknisten riskien vuoksi”. Komissio on arvioinut, että toimenpiteistä aiheutuisi miljardien eurojen ylimääräiset vuosittaiset kustannukset eurooppalaisille teleoperaattoreille useiden vuosien ajalle. Huawein näkemyksen mukaan komission vaikutusarvio on puutteellinen.

Esityksestä ei käy tarkemmin ilmi, mitä laitteita vaikutusarviossa esitetyt toimenpiteet koskisivat. Komission mahdollisuus antaa täytäntöönpanosäädöksiä ei rajoittuisi esimerkiksi 5G-keinovalikoimassa tunnistettuihin kriittisiin verkkoelementteihin, vaan ne voisivat koskea mitä tahansa laitetta viestintäverkoissa – jopa passiivisia laitteita. Jäsenvaltioille ei jäisi mahdollisuutta päättää tapauskohtaisista joustoista eikä ylipäätään arvioida komission täytäntöönpanosäädöksessä määrätyn toimenpiteen välttämättömyyttä.

Ehdotettu sääntely mahdollistaa komission puuttumisen ei-tekniseen riskiin siten, että laitteen omistajalta kielletään oman teknisen laitteistonsa käyttö. Komissio ei siis arvioisi esimerkiksi yksittäisen teleoperaattorin verkkoarkkitehtuuria tai sitä onko laitteen omistaja jo poistanut tai tehokkaasti vähentänyt komission tunnistamat ”ei-tekniset riskit” tietoturvaratkaisuilla tai muilla tavoilla.

Komission ehdottoma täytäntöönpanosäädöksille perustuva malli poikkeaa seurauksiltaan merkittävästi EU:n muista vastaavista toimivaltuuksista. Esimerkiksi kauppapoliittisten instrumenttien seurauksena voidaan päättää korotettuista tullimaksuista, mutta ketään ei velvoiteta hävittämään jo hankittua omaisuutta. Päätös omaisuutta koskevasta käyttökiellosta tulisi etenkin laitteen omistajan oikeusturvan ja toimenpiteen suhteellisuuden varmistamiseksi vuoksi toteuttaa kansallisena hallinnollisena päätöksenä eikä yleisenä täytäntöönpanoasetuksena.

5G-verkkoja on rakennettu vuodesta 2018 lähtien, eikä niissä ole havaittu turvallisuusongelmia. Suomessa 5G-verkkojen rakentaminen on laajalti valmista. Muualla Euroopassa 5G-verkon peitto kattaa jo yli 90 prosenttia väestöstä. CSA2-asetus koskisi viesintäverkkojen lisäksi myös muita pitkäaikaisille investoinneille perustuvia toimialoja. Investointeihin kohdistuvilla epävarmuustekijöillä olisi huomattavia taloudellisia vaikutuksia, joihin tulisi kiinnittä huomiota komission esitystä arvioitaessa.

Liitämme lausuntoomme Geradin Partners Asianajotoimisto Oy:n Huawein toimeksiannosta laatiman arviomuistion. Arviomuistiossa on käsitelty mm. omaisuudensuojaan ja suhteellisuuteen liittyviä

perusoikeuskysymyksiä sekä jäsenvaltioiden ja EU:n toimivaltasuhteita. Huawei yhtyy arviomuistiossa esitettyihin huomioihin.

Huawei Technologies Oy (Finland) Co., Ltd on toiminut Suomessa jo seitsemäntoista vuotta. Suurin osa henkilöstöstämme työskentelee tutkimuksen ja tuotekehityksen parissa Helsingissä ja Tampereella. Huawei on investoinut noin 400 miljoonaa euroa tutkimukseen ja tuotekehitykseen Suomessa. Yhtiöllä on vakiintunut markkina-asema Euroopassa yhtenä kolmesta keskeisestä 5G-verkkojen laitevalmistajasta.

Kunnioittavasti

Huawei Technologies Oy (Finland) Co., Ltd.

Tuomas Latola
lakiasianjohtaja

GERADIN
PARTNERS
COMPETITION, LITIGATION, REGULATION

4.3.2026

Arvio Euroopan komission ehdotuksesta EU:n uudistetuksi kyberturvallisuusasetukseksi (CSA2)

Sisällysluettelo

1 CSA2-ehdotuksen keskeinen tausta 3

2 Mitä CSA2 tarkoittaa Euroopan viestintäinfrastruktuurille? 5

3 CSA2-ehdotuksen taloudellinen ja tekninen arvio 11

3.1 Komission vaikutusarvion keskeiset ongelmat 11

3.2 CSA2:n tekninen ja sääntelyliitännäinen kyberturvallisuusarvio 18

4 CSA2-ehdotuksen EU-oikeudellinen arvio 20

4.1 SEUT 114 artiklan käyttöä koskevat rajoitukset 20

4.2 Toissijaisuus ja suhteellisuusperiaate 22

5 CSA2-ehdotuksen oikeudellinen arvio Suomen näkökulmasta 23

5.1 EU:n perusoikeuskirja 23

5.2 Suomen perustuslaki 25

5.2.1 Perusoikeudet Suomen perustuslaissa 25

5.2.1.1 Perustuslain 15 §: Omaisuudensuoja 26

5.2.1.2 Perustuslain 18 §: Oikeus harjoittaa elinkeinotoimintaa 30

5.2.1.3 Perustuslain 21 §: Hyvä hallinto ja oikeussuoja 31

5.2.2 Perusoikeuksien rajoitukset 32

5.3 Hallinto-oikeudelliset näkökohdat 34

5.4 Korvausjärjestelmä 35

6 Johtopäätökset 37

1 CSA2-ehdotuksen keskeinen tausta

1. Tämän arvion[1] tarkoituksena on tarkastella Euroopan komission (**komissio**) ehdotusta uudistetuksi EU:n kyberturvallisuusasetukseksi (**CSA2**) ja käsitellä ehdotukseen liittyviä keskeisiä kysymyksiä. Arviossa jäsennetään erityisesti ne teemat ja ongelmakohdat, joilla voi olla merkitystä jäsenvaltioiden arvioidessa ehdotuksen vaikutuksia ja muodostaessa kantojaan Euroopan unionissa (**EU** tai **unioni**).

2. Komission ehdottama CSA2 muuttaisi merkittävästi EU:n tieto- ja viestintätekniikan (**ICT**) toimitusketjujen sääntelyä. Ehdotuksen myötä jäsenvaltioiden arvioitavana ei siksi ole pelkästään sääntelyratkaisu, vaan käytännössä eurooppalaisten viestintäverkkojen rakenteellinen kestävyys ja toimintavarmuus sekä näihin kytkeytyvät unionin digitaalitalouden keskeiset toimintaedellytykset.

3. Komissio esitti 20.1.2026 uuden kyberturvallisuuspaketin[2] EU:n kyberturvallisuuden kestävyyden ja valmiuksien vahvistamiseksi. Komission ehdotuksella uudeksi kyberturvallisuusasetukseksi kumottaisiin ja korvattaisiin asetus (EU) 2019/881 eli nykyinen EU:n kyberturvallisuuslaki[3]. Uusi säädös, niin sanottu kyberturvallisuusasetus 2 eli CSA2, säätäisi tarkistetun toimivallan Euroopan unionin kyberturvallisuusvirastolle (**ENISA**)[4], uudistetun eurooppalaisen kyberturvallisuuden sertifiointikehyksen sekä uuden unionin tasoisen pakottavan mallin ICT-toimitusketjujen sääntelyyn.

4. Ehdotetulla CSA2-asetuksella otettaisiin käyttöön unionin keskitetty menettely, jonka nojalla komissio voisi nimetä kolmansia maita vakavia muita kuin teknisiä riskejä aiheuttaviksi, laatia luettelon korkean riskin ICT-laitetoimittajista sekä määrätä sitovia riskienhallintatoimenpiteitä. Käytännössä sääntelyn tarkoituksena olisi rajata tietyt kolmansien maiden laitetoimijat ulos EU:n viestintäverkoista sekä Euroopan muusta tieto- ja viestintäteknisestä infrastruktuurista.

5. CSA2-ehdotuksessa ei kuitenkaan osoiteta, että standardoituihin verkon osiin liittyisi nykyisellään sellaisia rajat ylittäviä sisämarkkinaongelmia, jotka edellyttäisivät unionitason keskitettyä ja kategorisiin riskiluokituksiin perustuvaa sääntelymallia. Ehdotuksessa ei yksilöidä konkreettisia markkinahäiriöitä, sääntelyn pirstoutumisesta aiheutuvia esteitä tai teknisiä yhteentoimivuusongelmia, joita nykyinen kansallinen tai unionin tasoinen kyberturvallisuuskehys ei jo kattaisi. Siksi on epäselvää, mihin sisämarkkinaoikeudelliseen

[1] Geradin Partners Asianajotoimisto Oy on laatinut tämän itsenäisen arvion Huawei Technologies Oy (Finland) Co Ltd:n toimeksiannosta.

[2] https://ec.europa.eu/commission/presscorner/detail/en/ip_26_105.

[3] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, ENISA:sta (Euroopan unionin kyberturvallisuusvirasto) ja tieto- ja viestintätekniikan kyberturvallisuuden sertifioinnista sekä asetuksen (EU) N:o 526/2013 (kyberturvallisuusasetus) kumoamisesta; https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[4] https://www.enisa.europa.eu/.

tarpeeseen esitetty uusi toimivaltamalli ja toimittajakohtaiset rajoitukset täsmällisesti vastaavat.

6. CSA2:n 98 artiklassa määriteltäisiin ns. luotettavaa ICT-toimitusketjua koskevan sääntelyn soveltamisala. Sääntely kohdistuisi muihin kuin teknisiin riskeihin EU:n NIS2 Direktiivissä (EU) 2022/2555 (**NIS2**)[5] tarkoitetuilla erittäin kriittisillä ja muilla kriittisillä toimialoilla. CSA2:n nojalla voitaisiin antaa sitovia riskienhallintaa koskevia säännöksiä, jotka kohdistuisivat NIS2:n liitteissä I ja II tarkoitettuihin toimijoihin.

7. CSA2:n 99 artiklassa säädettäisiin unionitason koordinoiduista ICT-toimitusketjujen turvallisuusriskien arvioinneista. Komissio tai vähintään kolme jäsenvaltiota voisivat pyytää NIS-yhteistyöryhmää[6] toteuttamaan arvioinnin. Arvioinnissa olisi kartoitettava keskeiset suojattavat ICT-kohteet, arvioitava niihin kohdistuvat uhkat ja haavoittuvuudet sekä analysoitava niistä aiheutuvat riskit. Arviointi olisi pääsääntöisesti saatettava päätökseen kuuden kuukauden kuluessa. Komission aloitteesta määräaikaa voitaisiin lyhentää. Artikla sisältäisi lisäksi kiireellisen menettelyn tilanteisiin, joissa komissiolla on riittävä peruste katsoa, että ICT-toimitusketjuun kohdistuu merkittävä kyberuhka ja että sisämarkkinoiden toiminta edellyttää välittömiä toimia. Tällöin komission olisi kuultava jäsenvaltioita mahdollisista riskinhallinnan toimenpiteistä ja toteutettava turvallisuusriskien arviointi nopeutetussa menettelyssä.

8. CSA2:n 100 artiklassa säädettäisiin menettelystä, jonka nojalla komissio voisi arvioida, aiheuttaako kolmas maa muita kuin teknisiä riskejä ICT-toimitusketjuille. Arviointi voisi perustua CSA2:n 99 artiklan mukaiseen riskinarviointiin, mutta myös muihin tietolähteisiin, kuten unionin tai jäsenvaltion lausumiin. Jos komissio katsoisi, että edellytykset täyttyvät, se voisi täytäntöönpanosäädöksellä nimetä kyseisen kolmannen maan kyberturvallisuutta koskevaa huolta aiheuttavaksi maaksi.

9. Nimeäminen merkitsisi käytännössä sitä, että kyseisessä kolmannessa maassa toimiviin tai sen määräysvallassa oleviin yrityksiin kohdistettaisiin oikeudellisia rajoituksia EU-alueella. Kun riskinarviointi olisi saatettu päätökseen, komissio voisi CSA2:n 101–103 artiklan nojalla ryhtyä jatkotoimiin. Se voisi antaa täytäntöönpanosäädöksiä, joilla yksilöitäisiin keskeiset tieto- ja viestintäteknologian resurssit sekä velvoitettaisiin NIS2:n mukaisilla toimialoilla toimivat yritykset toteuttamaan näihin resursseihin kohdistuvat riskienhallintatoimenpiteet.

10. CSA2:n 104 artiklan mukaan komissio antaisi täytäntöönpanosäädöksiä, joilla vahvistettaisiin luettelo ns. korkean riskin toimittajista, joihin rajoitukset kohdistuvat. Luettelon laatimista edeltäisi arviointi, jossa tarkasteltaisiin toimittajan sijoittautumista sekä omistus- ja määräysvaltasuhteita, mukaan lukien toimittajien yhteyksiä kolmansiin maihin.

[5] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, 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 (NIS 2 Direktiivi); https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022L2555.

[6] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.

Menettelyyn sisältyisi velvollisuus kuulla kyseisiä toimittajia sekä tarvittaessa toimivaltaisia viranomaisia.

11. Ehdotettu CSA2-malli loisi siten perustan unionitason rajoittaville toimenpiteille, jotka perustuisivat toimittajien kategoriseen riskiluokitukseen. Toimenpiteitä voitaisiin soveltaa riippumatta siitä, täyttävätkö tarkasteltavat ICT-laitteet ja komponentit niille asetetut tekniset kyberturvallisuusvaatimukset. Rajoituksia olisi mahdollista kohdistaa myös tilanteissa, joissa kyseisissä laitteissa tai komponenteissa ei olisi todettu teknisiä haavoittuvuuksia tai muita turvallisuuspuutteita.

12. CSA2:n 100 artiklassa tarkoitettu kolmannen maan nimeäminen ja 104 artiklan mukainen toimittajan sisällyttäminen korkean riskin toimittajien luetteloon sisältäisi välittömiä oikeusvaikutuksia. Komissio voisi täytäntöönpanosäädöksillä velvoittaa kriittisillä toimialoilla toimivat yritykset toteuttamaan riskienhallintatoimenpiteitä, mukaan lukien kieltää korkean riskin toimittajien laitteiden, ohjelmistojen tai komponenttien käytön, asentamisen tai liittämisen verkko- ja tietojärjestelmiin.

13. CSA2-ehdotuksessa täytäntöönpanovastuu osoitetaan jäsenvaltioille, joiden olisi nimettävä toimivaltaiset viranomaiset ja annettava niille riittävät valvonta- ja täytäntöönpanovaltuudet. Samalla perustettaisiin jäsenvaltioiden viranomaisten ja komission välinen yhteistyörakenne. Ehdotus rakentuu siten moniportaiselle mallille, jossa riskiluokitukset ja toimittajaluettelot vahvistettaisiin unionin tasolla, kun taas valvonta ja seuraamusten määrääminen kuuluisivat kansallisille viranomaisille. Työnjako herättää perusteltua kritiikkiä sääntelyn johdonmukaisuudesta, vastuun kohdentumisesta sekä tehokkaan oikeussuojan toteutumisesta käytännössä.

2 Mitä CSA2 tarkoittaa Euroopan viestintäinfrastruktuurille?

14. CSA2:lla olisi välittömiä ja laajoja vaikutuksia koko EU:n alueella. Unionin tasolla tehty toimittajien riskiluokitus voisi velvoittaa teleyritykset ja muut NIS2-sääntelyn piiriin kuuluvat toimijat korvaamaan osan verkkoinfrastruktuuristaan tiukassa määräajassa. Tämä puolestaan johtaisi olemassa olevien investointien nopeutettuihin poistoihin, rahoitusmenojen kasvuun, hankintajärjestelyjen uudelleenarviointiin sekä viivästyksiin verkkojen kehittämisessä – myös 5G-verkkojen laajentamisessa sekä tulevien 6G-verkkojen käyttöönotossa Euroopassa.

15. CSA2 ei siksi ole pelkkä sääntelytekninen tai kyberturvallisuuden menettelyitä yhtenäistävä uudistus, vaan korostetusti merkittävä rakenteellinen puuttuminen Euroopan digitaaliseen infrastruktuuriin. Tässä arviossa keskitytään CSA2-ehdotuksen vaikutuksiin viestintäinfrastruktuurille. Sääntely vaikuttaisi suoraan viestintäinfrastruktuurin markkinoiden rakenteeseen, investointien kohdentumiseen ja teknologian kehitykseen sekä muuttaisi pysyvästi Euroopan viestintäverkkojen rakennetta, kilpailuolosuhteita ja toimintavarmuutta koko unionissa.

16. Kuluneen vuosikymmenen kriisit, kuten pandemia, geopoliittiset jännitteet ja energiaturvallisuuteen liittyvät häiriöt ovat osoittaneet, että globaalit toimitusketjut ovat huomattavan monimutkaisia ja keskinäisriippuvaisia, ja niiden häiriöherkkyys voi realisoitua nopeasti myös Euroopan sisämarkkinoilla. CSA2 synnyttäisi teleyrityksille velvoitteita, joiden toteuttaminen riippuisi jäljelle jäävien ns. luotettujen ICT-toimittajien laitteiden saatavuudesta ja niiden tuotantokyvystä. Kategorisiin EU-tason riskiluokituksiin perustuva sääntely muuttaisi olennaisesti markkinoille pääsyn edellytyksiä ja voisi sulkea toimijoita pois keskeisiltä markkinasegmenteiltä ilman, että rajoitus perustuisi yksittäisen tuotteen tai järjestelmän tekniseen arviointiin.

17. Tämä vahvistaisi jäljelle jäävien ns. luotettujen toimittajien markkina-asemaa ja lisäisi riippuvuutta näistä toimittajista. Keskittyneellä markkinalla tämä edelleen kasvattaisi riskiä kustannusten noususta, toimitus- ja asennusruuhkista sekä verkkojen entistä epätasaisemmasta kehityksestä eri jäsenvaltioissa. Samalla sääntely siirtäisi investointiriskejä yksityisille toimijoille tilanteessa, jossa pakottavat strategiset linjaukset tehdään unionin tasolla.

18. Pidemmällä aikavälillä CSA2 vaikuttaisi myös EU:n innovaatioympäristöön negatiivisesti. Markkinoiden kaventuminen ja riskiluokitukset sekä niiden merkittävät taloudelliset seuraukset heikentäisivät kannustimia tuotekehitykseen ja rapauttaisivat eurooppalaisten toimijoiden globaalia kilpailukykyä. Vaikutukset eivät rajoittuisi yksittäisiin yrityksiin, vaan ne ulottuisivat digitaalisen infrastruktuurin kestävyyteen ja investointeihin koko unionissa.

19. CSA2 annettaisiin suoraan sovellettavana EU-asetuksena. Sääntelyllä täsmennettäisiin NIS2:n liitteissä I ja II tarkoitettujen toimijoiden riskienhallintavelvoitteita ICT-toimitusketjujen luotettavuutta ja ns. korkean riskin toimittajia koskevilta osin. NIS2:n liitteessä I luetellaan 11 kriittistä alaa, kuten energia (ml. sähkö, kaukolämpö ja -jäähdytys sekä kaasun jakelu), liikenne, pankkitoiminta ja rahoitusmarkkinoiden infrastruktuurit, terveydenhuolto, juoma- ja jätevesihuolto, digitaalinen infrastruktuuri ja tieto- ja viestintätekniset palvelut, keskus- ja aluehallinto sekä avaruusala. Liitteessä II luetellaan lisäksi muita kriittisiä aloja, kuten posti- ja kuriiripalvelut, jätehuolto, kemikaalien valmistus ja jakelu, elintarvikeketju, useat teollisuuden alat, digitaaliset palvelut ja tutkimustoiminta.

20. CSA2-sääntelyn soveltamisala olisi siten erittäin laaja. Myös silloin kun asiaa tarkastellaan erityisesti viestintäverkkojen näkökulmasta, on huomioitava, että verkot muodostavat perustan muun muassa EU:n energia-, liikenne-, pankki- ja terveyspalveluille sekä julkiselle hallinnolle. Toimittajien poissulkemista koskevat EU-tason toimenpiteet voisivat siten heijastua muun ohella kaikkien näiden alojen palvelujen toimivuuteen.

21. CSA2 laajentaisi merkittävästi myös EU:n 5G-kyberturvallisuuden työkalupakissa (5G Toolbox) omaksuttujen käsitteiden ja lähestymistapojen soveltamisalaa sekä muuttaisi ne oikeudellisesti velvoittaviksi.[7] CSA2 ei tästä huolimatta muodosta kyberturvallisuuden ja toimittajaturvallisuuden osalta kokonaisvaltaista sääntelykehystä. Se ei esimerkiksi noudata

[7] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

johdonmukaisesti periaatteita, jotka on omaksuttu muun muassa OECD:n suuntaviivoissa[8], unionin kyberturvallisuusyhteistyön rakenteissa sekä kansainvälisesti hyväksytyissä turvallisuuden hallintaa ja kyberturvallisuutta koskevissa standardeissa. Näissä instrumenteissa korostetaan yleisesti toimenpiteiden riskiperusteisuutta, teknologianeutraaliutta, avoimuutta ja suhteellisuutta sekä arviointia, joka perustuu todennettavissa oleviin turvallisuuskriteereihin.

22. CSA2 nojautuu voimakkaasti toimittajan sijoittautumiseen ja määräysvaltasuhteisiin perustuviin kategorisiin riskiluokituksiin. EU-sääntelyn painopiste siirtyisi siten korostetusti laitteiden ja järjestelmien teknisestä arvioinnista rakenteellisiin ja geopoliittisiin kriteereihin. Ratkaisu poikkeaa kansainvälisesti vakiintuneesta verkkoturvallisuuden hallinnan mallista, jossa keskeistä on uhkien, haavoittuvuuksien ja vaikutusten järjestelmällinen arviointi sekä oikeasuhtaisten – ei automaattisesti kategoristen – torjuntatoimien käyttö.

23. CSA2 keskittyy lisäksi valikoituihin kyberturvallisuuden ja toimittajaturvallisuuden osa-alueisiin, eikä se kata turvallisuuden hallintaa johdonmukaisena kokonaisuutena. Ehdotuksen painopiste on ENISA:n toimivallan tarkistamisessa, eurooppalaisen kyberturvallisuuden sertifiointikehyksen uudistamisessa sekä unionitason ICT-toimitusketjujen sääntelyssä. Toimittajaturvallisuudessa korostuvat muut kuin tekniset tekijät ja erityisesti kolmansiin maihin liittyvät riskit, kun taas ICT-järjestelmien koko elinkaaren kattava teknisen, organisatorisen ja operatiivisen turvallisuuden järjestelmällinen valvonta jää CSA2:ssa vähäiselle huomiolle. Tämä herättää perusteltua kritiikkiä siitä, onko CSA2:n tavoitteet määritelty riittävän täsmällisesti, ja voidaanko niitä edes saavuttaa komission esittämällä sääntelymallilla.

24. CSA2 seuraa komission tiedonantoja Euroopan unionin valmiusstrategiasta[9], Euroopan sisäisen turvallisuuden strategiasta[10] ja EU:n taloudellisen turvallisuuden vahvistamisesta[11]. Vaikka CSA2:ssa viitataan taloudellisen turvallisuuden strategiaan, ja kyberturvallisuus esitetään keskeisenä tekijänä taloudellisen turvallisuuden ja kilpailukyvyn kannalta, sääntelyn painopiste siirtyisi EU:n teknologiseen suvereniteettiin perustuvaan toimittajavalvontaan. Ehdotus liittyy unionin pyrkimykseen vahvistaa sen teknologista omavaraisuutta suhteessa strategisiin kolmansiin maihin. Taustana on myös Eurooppa-neuvoston korostama EU:n kilpailukyvyn, yhtenäisyyden ja sääntelyn johdonmukaisuuden vahvistaminen.

25. CSA2-ehdotuksen yhteydessä onkin syytä arvioida huolellisesti, parantavatko esitetyt toimenpiteet kyberturvallisuutta, vai palvelevatko ne lähtökohtaisesti ennemmin Euroopan geopoliittisia ja muita poliittisia tavoitteita. Kysymys on olennainen, koska sääntelyllä olisi erittäin merkittäviä vaikutuksia Euroopan viestintäverkoille. On myös huomattava, että unionilla on yksinomainen toimivalta esimerkiksi tulliliiton ja yhteisen kauppapolitiikan

[8] OECD (2015), Digitaalisen turvallisuuden riskienhallinta taloudellisen ja sosiaalisen vaurauden edistämiseksi: OECD:n suositus ja liiteasiakirja, OECD Publishing, Pariisi; https://doi.org/10.1787/9789264245471-en.
[9] JOIN/2025/130 final.
[10] COM (2025) 148 final.
[11] JOIN (2025) 977 final.

aloilla. SEUT[12] 114 artikla, johon CSA2:n oikeusperusta perustuu, ja jota käsitellään tarkemmin jäljempänä tässä arviossa, koskee sen sijaan sisämarkkinoita ja niihin liittyvää jaettua toimivaltaa. Jos sääntelyssä esitetyt toimenpiteet vastaavat käytännössä ennemmin esimerkiksi geopolitiikan ja turvallisuuspolitiikan välineitä, ratkaisu herättää perusteltua kritiikkiä CSA2:n oikeusperustasta.

26. Komissio esittää CSA2:ta samanaikaisesti digitaaliverkkoasetusta (**DNA**)[13] koskevan ehdotuksensa kanssa. Komission mukaan CSA2 tukee DNA:n tavoitteita vahvistaa digitaalista kilpailukykyä sekä edistää sääntelyn yhdenmukaistamista unionissa. Myös DNA-ehdotus on kuitenkin herättänyt teleoperaattoreiden ja niiden toimittajien keskuudessa huolta nykyisten investointien suojasta sekä taajuuspolitiikan ennakoitavuudesta ja oikeudellisesta epävarmuudesta.

27. Kun DNA:ta tarkastellaan yhdessä CSA2:n kanssa, on selvää, että sääntelyn kokonaisvaikutukset kasaantuvat. Erityisesti tilanteissa, joissa ICT-toimitusketjua koskevat rajoitukset kytkeytyvät taajuusoikeuksiin, verkkolupiin ja pitkäaikaisiin infrastruktuuri-investointeihin, DNA voimistaa CSA2:n vaikutuksia teleoperaattoreille ja niiden toimittajille.

28. Digitaalisen viestinnän markkinoilla sääntely- ja investointiympäristö on valmiiksi epätasainen eri puolilla unionia. 5G-verkkojen käyttöönottovaihe vaihtelee huomattavasti: osa jäsenvaltioista on vasta rakentamassa kattavia verkkoja, kun taas toiset, erityisesti Pohjoismaat, ovat jo tehneet merkittäviä investointeja ja suuntaavat kohti seuraavaa, 6G-teknologian investointisykliä. Unionitason yhtenäiset velvoitteet vaikuttaisivat eri tavoin markkinoihin, jotka ovat teknologisen kehityksen ja investointien osalta eri vaiheissa.

29. ICT-verkkolaitteiden markkinoilla rakenteellinen keskittyminen on viime vuosina yleisesti voimistunut, ja kilpailu on käytännössä supistunut muutaman globaalin toimijan varaan. Samankaltainen kehitys on nähtävissä myös muilla keskeisillä teknologiamarkkinoilla. Tällaisessa markkinarakenteessa riippuvuuksien vähentämiseen ja unionin teknologisen omavaraisuuden vahvistamiseen tähtäävien toimien olisi perustuttava realistiseen arvioon kilpailutilanteesta, investointisykleistä ja laitetarjonnan rakenteellisista rajoitteista.

30. CSA2-ehdotus näyttää kuitenkin kokonaisuutena arvioiden nojaavan pitkälti yksinkertaistettuihin oletuksiin. Se ei ota riittävästi huomioon nykyisiä eurooppalaisia markkinarakenteita, käynnissä olevia investointisyklejä ja EU-alueen tuotanto-, toimitus- ja investointikapasiteetin rajoitteita eikä digitaalisen viestinnän markkinoiden todennäköistä kehitystä keskipitkällä ja pitkällä aikavälillä. Heikko empiirinen perusta herättää perusteltua kritiikkiä siitä, vastaavatko esitetyt toimenpiteet tosiasiallisia markkinaolosuhteita ja verkkojen realistista teknologista kehitystä.

31. CSA2-ehdotus ei myöskään ota riittävästi huomioon digitaalisten viestintäverkkojen teknistä rakennetta. Jokainen matkaviestinverkko perustuu maailmanlaajuisesti sovellettaviin 3GPP-

[12] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A12016ME%2FTXT.
[13] COM (2026) 16 final.

standardeihin ja niissä määriteltyyn yhtenäiseen arkkitehtuuriin. Yksittäisen operaattorin verkko on osa tätä standardoitua kokonaisuutta ja liittyy muihin verkkoihin yhteisten, tarkasti määriteltyjen rajapintojen kautta.

32. Tämä tekninen perusrakenne on keskeinen myös sääntelyn arvioinnissa, koska se määrittää ne tekniset reunaehdot, joiden puitteissa sisämarkkinoiden yhtenäisyyttä voidaan edistää. Tämä arviointi puolestaan vaikuttaa suoraan siihen, kuinka tehokkaita ja oikeasuhtaisia CSA2-ehdotuksen mukaiset toimenpiteet voivat olla jäsenvaltioiden valtiosäännön ja unionin oikeuden näkökulmasta. Oikeudellista arviota käsitellään tarkemmin jäljempänä tässä arviossa.

33. 3GPP:n 5G-standardit määrittelevät 5G-verkon rakenteen, verkon eri osien väliset rajapinnat sekä kunkin osan tehtävät. Rajapinnat on yhdenmukaistettu, ja tukiasemien sekä muiden verkkokomponenttien toiminnot on määritelty 3GPP-standardeissa siten, että ne perustuvat samaan tekniseen kehykseen kaikissa unionin jäsenvaltioissa. Rajapintojen standardointi mahdollistaa eri toimittajien laitteiden yhteentoimivuuden, tukee monitoimittajamallia ja luo edellytykset laajojen markkinoiden mittakaavaeduille.

34. Jotta sääntely ei johtaisi tarpeettomiin negatiivisiin vaikutuksiin verkkojen toimintakyvyssä, rajoittavan sääntelyn tulisi kohdistua oikeasuhtaisesti niihin viestintäverkon osiin, joilla on **todellista ja merkittävää vaikutusta verkon toimintaan, turvallisuuteen ja jatkuvuuteen sekä viestinnän luottamuksellisuuden turvaamiseen**. Verkon kriittisiksi määriteltyjen osien laajentaminen CSA2-ehdotuksessa ilman selkeää ja riskiperusteista arviota johtaa tilanteeseen, jossa rajoitukset ulotetaan myös sellaisiin verkon osiin, joiden merkitys kokonaisuuden kannalta on rajallinen.

35. Suomessa viestintäverkon kriittisistä osista säädetään lain sähköisen viestinnän palveluista (917/2014 muutoksineen; **SVPL**)[14] 244 a §:ssä. Viestintäverkon kriittisenä osana pidetään lain mukaan verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä. Sääntely koskee yleisten viestintäverkkojen lisäksi myös yhteiskunnan elintärkeiden toimintojen, kuten ydinvoimaloiden, satamien ja lentokenttien yleiseen viestintäverkkoon liitettyjä erillisverkkoja. Liikenne- ja viestintävirasto (**Traficom**) antaa tarkempia määräyksiä viestintäverkkojen ja niiden kriittisten osien teknisestä määrittelystä.

36. CSA2:ssa ja NIS2:n kautta viestintäverkon kriittisten osien käsitettä laajennettaisiin siten, että kriittisiksi voitaisiin määritellä ydintoimintojen lisäksi myös muita verkon eri tasoilla sijaitsevia laitteita, ohjelmistoja ja toiminnallisia kokonaisuuksia. Tällainen ratkaisu voi ideologisella tasolla vaikuttaa kyberturvallisuutta vahvistavalta. Kriittisyyden määritelmän laajentaminen ilman huolellista arviota käytännön toteutettavuudesta ja eri verkkotasojen kustannus–hyötysuhteesta kuitenkin lisää merkittävästi muun ohella täytäntöönpanoon ja investointeihin liittyviä riskejä.

[14] https://www.finlex.fi/fi/lainsaadanto/2014/917.

37. Kriittisyyden käsitteen laajentaminen ja toimittajiin kohdistuvat rakenteelliset rajoitukset voivat johtaa kalliisiin ja monimutkaisiin muutoksiin Euroopan viestintäverkoissa. Tällöin resursseja joudutaan ohjaamaan rakenteellisiin muutoksiin sen sijaan, että ne kohdennettaisiin täsmällisiin teknisiin riskienhallintatoimiin. Tämä voi paradoksaalisesti heikentää kyberturvallisuutta, vaikka komission tavoitteena on nimenomaan sen vahvistaminen. Erittäin keskittyneillä 5G-verkkolaitteiden markkinoilla vaihtoehtoisia toimittajia on myös vain vähän. Tällaisessa markkinassa ICT-laitteiden nopea korvaaminen ei ole käytännössä mahdollista ilman merkittäviä teknisiä, tuotannollisia ja logistisia ongelmia.

38. Seurauksena voi olla verkon suorituskyvyn heikkeneminen, käyttöönottojen viivästyminen sekä integraatio-ongelmat, jotka huonontaisivat eurooppalaisten verkkojen toimintakykyä ja -varmuutta. Vaikutukset eivät rajoittuisi vain teleoperaattoreihin, vaan ne ulottuisivat koko EU:n digitaaliseen toimintaympäristöön, joka on riippuvainen suorituskykyisistä ja kohtuuhintaisista viestintäyhteyksistä.

39. Riskit ovat suuret myös sisämarkkinoiden tasolla. Jäsenvaltioiden erilaiset lähtökohdat yhdistettynä unionin tason pakottavaan sääntelyyn ja sen kansallisen tason täytäntöönpanoon voivat johtaa taloudellisiin vaikutuksiin, jotka kohdistuvat eri tavoin eri jäsenmaihin, ja siten eriarvoisiin kilpailuolosuhteisiin. Erityisesti ne operaattorit, jotka ovat jo ottaneet käyttöön tiettyjen mahdollisesti riskisiksi luokiteltavien toimittajien verkkoinfrastruktuuria, joutuisivat kantamaan suuremman kustannustaakan kuin ne, joiden verkot ovat vasta rakentamisvaiheessa. Erot voivat vääristää kilpailua, hidastaa Euroopan digitaalista kehitystä ja heikentää nimenomaan niitä kilpailukyky- ja kestävyystavoitteita, joita komissio pyrkii CSA2-ehdotuksella edistämään.

40. CSA2-ehdotuksen mukaan korkean riskin toimittajiksi luokiteltujen yritysten toimittamat ICT-laitteet olisi poistettava käytöstä enintään 36 kuukauden kuluessa komission päätöksestä. Siirtymäajan tarkempi soveltaminen määriteltäisiin täytäntöönpanosäädöksissä.

41. Jos laajamittaisia ICT-laitteiden pakkovaihtoja toteutetaan näin lyhyessä määräajassa, kielteiset vaikutukset EU-alueen viestintäverkkoihin ovat väistämättä erittäin merkittävät. Investoinnit ohjautuvat tällöin uusien laitteiden hankintaan sen sijaan, että niitä käytettäisiin verkkojen kehittämiseen. Tämä puolestaan hidastaa 5G-verkkojen laajentamista ja viivästyttää sekä jopa estää 6G-teknologian käyttöönottoa. Samalla koko EU:n digitaalinen toimintaympäristö altistuu suuremmille häiriöille ja kustannuspaineille, mikä heikentää unionin kilpailukykyä ja digitaalista kestävyyttä.

42. CSA2 merkitsisi Euroopan viestintäinfrastruktuurille laajaa ja oikeudellisesti sitovaa rakennemuutosta. Unionin tason toimittajaluokitukset ja niihin liittyvät verkkolaitteiden poistovelvoitteet vaikuttaisivat suoraan Euroopan viestintäverkkojen tekniseen kokoonpanoon, investointien ajoitukseen ja markkinarakenteeseen. Sääntely lisäisi kustannuksia, kasvattaisi riippuvuutta harvoista toimittajista ja kohdentaisi taloudellisia rasitteita erityisesti niille toimijoille, joiden verkot on jo rakennettu nykyisellä toimittajarakenteella. Laajamittaiset ja ajallisesti keskittyvät laitekorvaukset voisivat lisäksi

heikentää verkkojen toimintavarmuutta ja suorituskykyä, hidastaa kapasiteetin laajentamista sekä lisätä häiriö- ja integraatioriskejä.

43. Turvallisuushyötyjen ja sääntelystä aiheutuvien kustannusten sekä toimintakykyyn kohdistuvien vaikutusten välinen suhde jää CSA2-ehdotuksessa kuitenkin epäselväksi. Tämä korostaa sääntelyn huolellisen suhteellisuus- ja vaikutusarvioinnin tarvetta.

3 CSA2-ehdotuksen taloudellinen ja tekninen arvio

3.1 KOMISSION VAIKUTUSARVION KESKEISET ONGELMAT

44. Komissio on liittänyt CSA2-ehdotukseensa vaikutusarvion, jossa tarkastellaan muun ohella esityksen kustannus- ja investointivaikutuksia. Koska CSA2:lla olisi laajoja ja pitkäkestoisia vaikutuksia Euroopan viestintäverkkoihin, niitä koskeviin markkinarakenteisiin ja investointeihin, sääntelyn vaikutusarvion tulisi olla poikkeuksellisen huolellinen. Erityisesti silloin, kun sääntely voi johtaa merkittäviin kustannuksiin ja pysyviin muutoksiin kilpailuolosuhteissa, arvioinnin olisi perustuttava kattavaan ja realistiseen analyysiin. Puutteellinen tai yksipuolinen vaikutusarvio heikentää merkittävästi sääntelyn ennakoitavuutta ja vaikeuttaa sen oikeasuhtaisuuden arviointia.

45. Komission CSA2-vaikutusarvio on kokonaisuutena arvioituna selvästi riittämätön suhteessa ehdotuksen laajuuteen ja sen väistämättömiin taloudellisiin seurauksiin. Arvio ei sisällä riittävän perusteellista analyysia esimerkiksi siitä, miten ehdotettu sääntely vaikuttaisi EU:n tieto- ja viestintätekniikan markkinoiden kilpailurakenteeseen, investointien kohdentumiseen, kannustimiin innovaatioihin sekä mahdollisimman korkean innovaatioasteen ratkaisuiden hyödyntämiseen, toimittajien markkina-asemaan tai toimitusketjujen rakenteeseen ja toimintaan välittömällä ja pidemmällä aikavälillä.

46. Vaikutusarviossa esitetään keskeisenä kustannuseränä 5G-verkkolaitteiden korvaaminen ns. korkean riskin toimittajiin kohdistuvien rajoitusten vuoksi. Komission mukaan kustannukset nousisivat useisiin miljardeihin euroihin. Tarkastelu rajoittuu kuitenkin pääosin matkaviestinverkkoihin, eikä se sisällä kattavaa arviota toimittajamarkkinoiden rakennemuutoksesta, vaihtoehtoisten toimittajien todellisesta kapasiteetista tai kilpailun kehityksestä siirtymäajan jälkeen. Näin suppea tarkastelutapa ei anna riittävää perustaa arvioida ehdotuksen kokonaisvaikutuksia sisämarkkinoihin ja unionin digitaaliseen kilpailukykyyn.[15]

[15] Commission Staff Working Document, Impact Assessment Report, Accompanying the documents: Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) and Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the Proposal for the Cybersecurity Act 2, Council doc ST-5611/26 ADD 4 (**CSA2 vaikutusarviointi**), s. 85–86.

47. Vaikutusarviossa todetaan, että markkinoilla on useita 5G-laitteiden toimittajia, ja että kilpailu ja innovaatiot ”todennäköisesti säilyisivät”.[16] Tämä johtopäätös on mahdollinen vain, jos relevantti markkina määritellään riittävän laajasti ja siihen sisällytetään myös piirisarja- ja komponenttivalmistajat. 5G-radio- ja runkoverkkojen osalta tuotemarkkina on olennaisesti suppeampi, ja toimittajien määrä on jo valmiiksi erittäin rajallinen.

48. EU:ssa toimii käytännössä kolme yritystä, joilla on kyky toimittaa laajamittaisia 5G-verkkolaitteita: Huawei, Ericsson ja Nokia. ZTE:n markkinaosuus on vähäinen ja Samsungin toimitukset rajoittuvat yksittäisiin hankkeisiin. Jos yksi kolmesta päätoimittajasta suljettaisiin pois unionin alueella, markkinat kaventuisivat tosiasiallisesti kahden toimijan varaan. Muutos lisäisi jäljelle jäävien toimittajien neuvotteluvoimaa, heikentäisi kilpailua tarjouskilpailuissa ja merkittävästi kasvattaisi riippuvuutta näistä toimittajista. Näitä vaikutuksia ei arvioida määrällisesti, eikä niiden hintavaikutuksia tai vaikutuksia investointien tasoon analysoida komission vaikutusarviossa.

49. Taloudellisen kokonaisarvion tulisi perustua hyötyjen ja kustannusten tasapainoiseen ja todennettavaan punnintaan. CSA2:n oletetut hyödyt nojaavat kuitenkin väitteeseen, että kyberturvallisuustapahtumien vakavuus vähenisi, vaikka komissio ei esitä tätä tukevia varsinaisia perusteita. Samalla markkinoiden keskittymisen vaikutuksia käsitellään myönteisessä valossa, kun luotettaviksi katsottujen toimittajien kasvavia tuloja pidetään hyötynä, vaikka tosiasiallisesti kyse on markkinaosuuksien siirtymisestä toimijalta toiselle. Kilpailun väheneminen johtaa tyypillisesti myös aina hintatason nousuun ja investointikannustimien heikkenemiseen, jolloin kustannukset siirtyvät ensin operaattoreille ja lopulta käyttäjille.

50. Myös pakollisten laitteiden korvaamistoimien kustannuksia aliarvioidaan vaikutusarviossa. Arvio rajoittuu 5G-infrastruktuuriin eikä huomioi sitä, että laajamittainen ja samanaikainen laitekorvaaminen EU:n alueella rajallisen toimittajajoukon varassa aiheuttaa hyvin todennäköisesti hintapaineita, toimitusviiveitä ja tuotanto- sekä asennuskapasiteetin pullonkauloja. Tällaisessa tilanteessa toteutuneet kustannukset voivat nousta olennaisesti arvioitua suuremmiksi.

51. Kokonaisuutena vaikutusarvio ei anna luotettavaa perustaa komission johtopäätökselle, jonka mukaan ehdotuksen taloudelliset hyödyt ylittäisivät siitä aiheutuvat kustannukset. Komissio arvioi CSA2-ehdotuksen tuottavan 3,7–4,4 miljardin euron taloudelliset hyödyt viiden vuoden aikana. Arvio perustuu oletukseen, että toimenpiteet lyhentävät kyberturvallisuustapahtumien keskimääräistä palautumisaikaa 241 päivästä 200 päivään ja pienentävät siten yksittäisen tietoturvaloukkauksen kustannuksia noin 0,5 miljoonalla eurolla. Tämä arvioitu säästö kerrotaan oletetulla tapausmäärällä, minkä jälkeen tulosta oikaistaan alaspäin.[17] Valtaosa lasketusta kokonaishyödystä riippuu kuitenkin nimenomaan oletetusta palautumisajan lyhenemisestä, jonka toteutumiselle ei esitetä riittävää empiiristä

[16] CSA2 vaikutusarviointi, s. 93.

[17] CSA2 vaikutusarviointi, s. 69.

näyttöä. Näin ollen keskeinen osa ehdotuksen taloudellisesta hyödystä perustuu oletukseen eikä tosiasiassa osoitettuun vaikutukseen.

52. Televerkkojen kyberturvallisuutta koskeva riskikuva edellyttää myös suhteellisuusarviointia. Esimerkiksi radioverkkoihin ei ole kohdistunut merkittäviä kyberturvallisuustapahtumia, jotka osoittaisivat järjestelmätason haavoittuvuuksia. Ukrainan sota on konkreettisesti osoittanut televerkkojen resilienssin myös poikkeuksellisissa ja äärimmäisen kuormittavissa olosuhteissa.[18] Tämä herättää perustellun kysymyksen siitä, missä määrin CSA2:ssa ehdotetut lisätoimenpiteet tosiasiallisesti parantaisivat kyberturvallisuuden tasoa tilanteessa, jossa televerkkojen suojaus- ja resilienssikyvykkyydet ovat jo osoittautuneet korkeatasoisiksi.

53. Myös vaikutusarviossa esitetty riskilähestymistapa on teknisesti ongelmallinen. Riskin oletettu väheneminen perustuu mallinnettuun arvioon kyberturvallisuustapahtumien palautumisajan lyhenemisestä eikä tekniseen näyttöön siitä, että ehdotetut toimenpiteet todennettavasti parantaisivat tietoturvan tasoa.

54. ENISA Threat Landscape 2025[19] vahvistaa aiemmat havainnot siitä, että verkko-operaattorin tietoturvan tasoon vaikuttavat ensisijaisesti hyvä kyberhygienia, ajantasaiset protokollat, päätelaitteiden suojaus sekä henkilöstön tietoturvaosaaminen ja -käytännöt. Myös verkon arkkitehtuurin eriyttäminen, erityisesti ydinverkon ja muiden verkko-osien selkeä segmentointi, on keskeinen turvallisuustekijä. Verkkoviestinnän luottamuksellisuus perustuu pääosin sovellustason salaukseen ja muihin päästä päähän -ratkaisuihin, eikä näiden turvallisuus riipu yksittäisestä laitetoimittajasta. Matkaviestinverkot perustuvat kerrokselliseen suojausmalliin, jossa verkon eri osat on erotettu toisistaan ja niiden välistä liikennettä valvotaan. Tukiasemat ja ydinverkko toimivat erillisillä turvallisuusalueilla, ja viestinnän luottamuksellisuus turvataan pääosin sovellustason salauksella.

55. Potentiaalisen hyökkääjän näkökulmasta radioverkkokerroksen merkitys on yleensä rajallinen, sillä ydinverkko ja esimerkiksi teleyrityksen henkilöstö ovat usein houkuttelevampia kohteita. On myös erittäin olennaista todeta, ettei EU:ssa ole esitetty näyttöä siitä, että tietyn toimittajan verkkolaitteet olisivat olleet tietoturvaloukkausten lähde niiden teknisten ominaisuuksien vuoksi.

[18] Ukrainan telekommunikaatioinfrastruktuuri on ollut sodan aikana toistuvien ohjus- ja drooni-iskujen, kyberhyökkäysten sekä laajojen sähkökatkosten kohteena, mutta verkot ovat tästä huolimatta säilyttäneet toimintakykynsä ja palautuneet vaurioista nopeasti, mikä osoittaa merkittävää teknistä ja operatiivista resilienssiä. Verkkojen ylläpito ja korjaaminen on edellyttänyt tiivistä yhteistyötä operaattoreiden ja laitevalmistajien välillä. Huawei on ollut historiallisesti yksi keskeisistä laite- ja teknologiatoimittajista Ukrainan suurille teleoperaattoreille, kuten Kyivstarille ja Vodafone Ukrainelle, ja yhtiön paikallinen organisaatio on jatkanut toimintaansa myös sodan aikana osallistuen verkkojen ylläpitoon, modernisointiin ja tekniseen tukeen. Huaweilla on Ukrainassa merkittävä rooli osana laajempaa teleinfrastruktuurin jatkuvuuden turvaamista poikkeusoloissa.

[19] Euroopan unionin kyberturvallisuusviraston ENISA:n uhkatilannekuva vuodelle 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

56. Vaikutusarviossa esitetty arvio keskimääräisistä kustannuksista perustuu yllä todetusta huolimatta aineistoon, jossa ei erotella, johtuuko kyberturvallisuuspoikkeama teknisestä haavoittuvuudesta, inhimillisestä virheestä, puutteellisesta prosessista vai muusta syystä. Komission hyötylaskelma nojaa oletukseen, että palautumisaika lyhenee, mutta siinä ei osoiteta, että juuri CSA2:n toimenpiteet vaikuttaisivat niihin tekijöihin, joista suurin osa tietoturvavahingoista käytännössä syntyy. Kun sääntely kohdistuu ennen kaikkea toimittajiin ja rakenteellisiin riskeihin, on epäselvää, missä määrin se tosiasiassa vähentäisi teknisistä ja operatiivisista puutteista johtuvia haittoja.

57. Samalla laitetoimittajien määrän väheneminen väistämättä lisää riippuvuutta harvoista ns. jäljelle jäävistä toimittajista. Kun vaihtoehtoja on vähemmän, yhden toimittajan virhe, haavoittuvuus tai toimitusongelma vaikuttaa laajemmin koko Euroopan viestintäverkkoihin. Vaikutusarviossa ei arvioida tätä riskiä perusteellisesti, vaikka markkinoiden keskittyminen voi pitkällä aikavälillä todennäköisesti lisätä teknisiä ja toiminnallisia riskejä.

58. Oletus kyberhaittojen merkittävästä vähenemisestä on vaikutusarviossa siten kokonaisuutena arvioiden heikosti perusteltu. Hyötylaskelma rakentuu oletuksille, joiden toteutumisesta ei esitetä näyttöä. Kokonaisarvioon jää siten huomattavaa epävarmuutta.

59. Vaikutusarvion tulisi lisäksi huomioida, että CSA2:n täytäntöönpano tosiasiassa kaventaisi Euroopan 5G-infrastruktuurimarkkinoita. 5G-verkkojen toimittaminen edellyttää merkittäviä pääomainvestointeja, immateriaalioikeuksia ja pitkäaikaisia sopimussuhteita, minkä vuoksi uusien toimijoiden markkinoille tulo on käytännössä vaikeaa. Jos markkinarakenne supistuisi kolmesta päätoimittajasta kahteen, markkinoiden keskittyminen kasvaisi selvästi ja samalla kilpailupaine heikkenisi.

60. Taloustieteellisen tutkimuksen perusteella kilpailun väheneminen ja markkinoiden keskittyminen heikentävät investointi- ja innovaatiokannustimia. Kun kilpailupaine vähenee, yrityksillä on vähemmän tarvetta parantaa tehokkuuttaan tai kehittää uusia tuotteita ja teknologioita. Samalla niiden mahdollisuudet nostaa hintoja ja siirtää kustannuksia asiakkaille kasvavat.

61. Laitteiden hinnannousu puolestaan kasvattaa suoraan operaattoreiden investointikustannuksia. Pääomavaltaisella toimialalla jo suhteellisen pieni kustannusten nousu voi johtaa investointien lykkäämiseen, verkkojen laajentamisen hidastumiseen ja seuraavan sukupolven teknologioiden käyttöönoton viivästymiseen. Pitkällä aikavälillä tämä merkitsee heikompaa kilpailukykyä ja korkeampia kustannuksia koko Euroopan tieto- ja viestintätekniikan toimintaympäristössä.

62. Näin ollen komission väite, jonka mukaan markkinoiden keskittymisen lisääntyminen olisi taloudellinen etu, ei perustu kestävään taloudelliseen analyysiin. Kyse on pikemminkin tulonjaon muutoksesta ja kilpailun heikkenemisestä, jonka kustannukset jakautuisivat laajasti koko EU:n talouteen.

63. CSA2:n toimittajarajoitukset voisivat käytännössä johtaa niin sanottuihin rip-and-replace-toimiin, minkä vuoksi vaikutusarviossa olisi arvioitava tätä näkökulmaa huomattavan

perusteellisesti. Rip-and-replace tarkoittaa jo asennettujen verkkolaitteiden pakollista poistamista ja korvaamista ennen niiden taloudellisen käyttöiän päättymistä. Se ei siten merkitse pelkästään uusia hankintakustannuksia, vaan myös olemassa olevien laitteiden jäännösarvon menettämistä, purku- ja asennustöiden kustannuksia, verkon uudelleenjärjestelyä sekä siirtymävaiheen häiriöriskejä.

64. Komissio arvioi EU:n 5G-verkkoihin kohdistuvien rip-and-replace-toimien kustannuksiksi noin 9,6 miljardia euroa.[20] Arvio rajautuu kuitenkin 5G-infrastruktuuriin eikä se kata muita tieto- ja viestintätekniikan osa-alueita, jotka voivat tulla sääntelyn soveltamisalaan. Kyse on ensinnäkin siten vain osittaisesta kustannusarviosta. Lisäksi on huomattava, että esimerkiksi Huawein arvioiden mukaan kustannukset olisivat huomattavasti korkeammat, mikäli sääntely koskisi esimerkiksi radioverkkoa. Tältä osin 9,6 miljardin euron arvio ei anna miltään osin realistista kokonaiskuvaa ehdotuksen mahdollisista taloudellisista vaikutuksista.

65. Komission laskelma perustuu arvioon siitä, kuinka suuri osa nykyisestä laitekannasta olisi oletetuilta korkean riskin toimittajilta sekä oletukseen korvaavien laitteiden ja asennustöiden keskimääräisistä kustannuksista. Menetelmä on sinänsä kirjanpidollisesti johdonmukainen, mutta se tarkastelee tilannetta staattisena eikä huomioi markkinoiden reagointia, kuten hintojen nousua, toimitusviiveitä tai kapasiteettirajoitteita. Komissio ei myöskään avaa arvion lähtöoletuksia riittävästi.

66. Euroopan tilintarkastustuomioistuimen vuoden 2022 erityiskertomuksen mukaan 5G-verkon käyttöönoton kokonaiskustannusten EU:ssa vuoteen 2025 mennessä on arvioitu olevan 281–391 miljardia euroa ja kustannusten jakautuvan suunnilleen puoliksi uuden 5G-infrastruktuurin rakentamiseen ja kiinteän infrastruktuurin päivittämiseen. Samassa yhteydessä erityiskertomuksessa on viitattu arvioihin, joiden mukaan 5G-verkon käyttöönoton kokonaiskustannukset kaikissa jäsenvaltioissa voivat nousta jopa 400 miljardiin euroon.[21] Nämä luvut asettavat komission 9,6 miljardin euron rip-and-replace-arvion mittakaavaan ja herättävät kysymyksen siitä, mihin komission kustannuslaskelma perustuu, sekä miksi se ei huomioi laajempaa investointiympäristöä ja markkinavaikutuksia.

67. Komission kustannuslaskelmien arviointi on lisäksi vaikeaa siksi, että vaikutusarviossa ei täsmennetä, mitä mobiiliverkkojen laite- ja verkkoelementtejä (esimerkiksi RAN-laitteita, ydinverkon komponentteja tai siirtoverkkoja) oletetaan vaihdettavan, eikä avata yksityiskohtaisesti, mihin markkina-, kustannus- tai laitekantadataan arviot perustuvat. Ilman läpinäkyvää kuvausta lähtöoletuksista ja käytetystä aineistosta on käytännössä mahdotonta arvioida, heijastavatko laskelmat tosiasiallista laitekannan rakennetta ja markkinatilannetta vai perustuvatko ne yleisluonteisiin oletuksiin.

[20] CSA2 vaikutusarviointi, s. 59.

[21] https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf; Commission estimate based on data by EIB, Analysis, GSMA and company announcements, and ETNO – European Telecommunications, Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All, March 2021.

68. Laajamittainen ja samanaikainen rip-and-replace useissa jäsenvaltioissa merkitsisi joka tapauksessa huomattavaa verkkolaitteiden kysynnän kasvua lyhyessä ajassa. Kun CSA2:ssa säädetty siirtymäaika olisi vain 36 kuukautta ja vaihdettavien laitteiden osuus Euroopan viestintäverkoissa voisi olla merkittävä, hankinnat painottuisivat väistämättä samalle ajanjaksolle. Koska toimittajia on vähän ja niiden tuotanto- sekä asennuskapasiteetti on rajallinen, ovat hintojen nousu, toimitusviiveet ja kapasiteettipuutteet erittäin todennäköisiä.

69. Huawein arvion mukaan tällainen 36 kuukauden siirtymäaika ei olisi teknisesti ja operatiivisesti realistinen ottaen huomioon verkkojen laajuuden, toimitusketjujen kapasiteetin sekä sen, että samanaikaisesti useissa jäsenvaltioissa toteutettavat laitekorvaukset kuormittaisivat rajallista tuotanto- ja asennuskapasiteettia merkittävästi.

70. Koska laitetarjontaa ei voida lyhyellä aikavälillä merkittävästi lisätä ja kilpailu on jo valmiiksi vähäistä, laitteiden hinnat voivat myös nousta siirtymäkauden aikana. Tätä hintavaikutusta ei ole otettu huomioon komission kustannusarviossa. Lisäksi asennusresurssien rajallisuus ja eri toimittajien laitteiden tekniset erot voivat kasvattaa kokonaiskustannuksia. Toimitusrajoitteet voivat edelleen johtaa tilanteisiin, joissa laitteita poistetaan käytöstä ennen kuin korvaavat ratkaisut ovat täysimääräisesti saatavilla. Tällöin verkon kapasiteettia saatetaan joutua supistamaan, mikä heikentää palvelun toimintakykyä ja -varmuutta.

71. Kansainväliset reaalimaailman kokemukset osoittavatkin, että rip-and-replace-ohjelmat aiheuttavat merkittäviä käytännön ongelmia. Yhdistynyt kuningaskunta ja Yhdysvallat ovat toteuttaneet laitteiden poistamis- ja korvaamisohjelmia, ja molemmissa maissa seurauksina on ollut kustannusten kasvu, viivästykset ja markkinahäiriöt.

72. Yhdistyneen kuningaskunnan hallitus päätti heinäkuussa 2020 sulkea Huawein pois 5G-verkoista ja velvoitti operaattorit poistamaan toimittajan laitteet käytöstä vuoteen 2027 mennessä.[22] Siirtymäajaksi muodostui näin noin seitsemän vuotta. Jo varhaisissa arvioissa päätöksen katsottiin aiheuttavan noin kahden miljardin punnan lisäkustannukset ja viivästyttävän 5G-verkkojen valtakunnallista käyttöönottoa useilla vuosilla.[23]

73. Yhdistyneen kuningaskunnan osalta on olennaista huomata, että ohjelma toteutettiin vaiheittain. Ensin asetettiin ns. korkean riskin toimittajille 30 prosentin markkinaosuuskatto verkon muissa kuin ydinosissa, minkä jälkeen linjausta kiristettiin täydeksi kielloksi. Lisäksi päätökset tehtiin ajankohtana, jolloin 5G-verkkojen rakentaminen oli käynnissä ja osa aiemmasta infrastruktuurista oli luonnollisen investointisyklin taitekohdassa. Verkkoja modernisoitiin joka tapauksessa siirryttäessä 4G-arkkitehtuurista 5G-aikaan, jolloin laitteistojen uusiminen tapahtui osittain käyttöikänsä päähän tulleen infrastruktuurin korvaamisen yhteydessä. Jatkaminen samalla toimittajalla osana normaalia modernisointisykliä olisi ollut kustannustehokkaampaa kuin laajamittainen ja ennenaikainen täysi laitevaihto.

[22] https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027.

[23] https://www.nbcnews.com/news/world/after-months-u-s-pressure-u-k-bans-china-s-n1233752.

74. Tilanne Euroopan unionissa on nyt olennaisesti erilainen. 5G-verkkojen rakentaminen on monissa jäsenvaltioissa loppusuoralla, ja verkoilla on jäljellä useita käyttövuosia ennen kuin seuraavan sukupolven 6G-verkkojen kaupallinen käyttöönotto arviolta vuosina 2030–2032 käynnistyy. Samanaikaisesti 5G-verkkojen käyttöönoton kokonaiskustannusten on arvioitu EU:ssa olevan vuoteen 2025 mennessä 281–391 miljardia euroa[24], jakautuen noin puoliksi uuden 5G-infrastruktuurin rakentamiseen ja kiinteän infrastruktuurin päivittämiseen, ja investointien pääosan rahoittavat mobiiliverkko-operaattorit itse. Tässä vaiheessa toteutettava laajamittainen rip-and-replace merkitsisi siten ennenaikaista investointien alasajoa, eikä se ajoittuisi luonnolliseen teknologiasyklin murroskohtaan.

75. Ohjelman käytännön toteutus on osoittautunut selvästi ennakoitua vaativammaksi. Laitteiden korvaaminen on ollut teknisesti monimutkainen ja operatiivisesti raskas prosessi, joka on sitonut huomattavasti henkilöstö- ja asennusresursseja. Yhdistyneen kuningaskunnan kokemus osoittaa, että laajamittainen toimittajan poissulkeminen ei ole pelkkä tekninen vaihto, vaan se vaikuttaa koko verkon kehittämiseen ja investointien ajoitukseen. Vaikka siirtymäaika oli Yhdistyneessä kuningaskunnassa seitsemän vuotta – eli selvästi pidempi kuin CSA2:ssa esitetty 36 kuukauden määräaika – toteutuksessa on ilmennyt merkittäviä aikatauluviiveitä, integraatiohaasteita ja resurssipulaa.[25]

76. Yhdysvalloissa Huawei- ja ZTE-laitteiden poistaminen toteutettiin liittovaltion sääntely- ja rahoitusohjelman avulla. Ohjelman tavoitteena oli tukea erityisesti pieniä ja maaseutualueilla toimivia teleyrityksiä, jotka olivat ottaneet käyttöön kyseisten toimittajien laitteita niiden edullisuuden ja hyvän saatavuuden vuoksi. Kongressi myönsi ohjelmaan aluksi noin 1,9 miljardin dollarin määrärahan. Toteutuksen aikana kävi kuitenkin ilmi, ettei rahoitus riittänyt kattamaan todellisia kustannuksia. Merkittävä osa operaattoreista ilmoitti tarvitsevansa lisärahoitusta korvaustoimien loppuunsaattamiseen.[26] Lisäksi työvoimapula ja toimitusketjujen rajoitteet hidastivat ohjelmaa, ja määräaikoja jouduttiin pidentämään.[27]

77. Yhdysvaltain viestintäviranomaisen (**FCC**) mukaan hyväksyttyjen hakemusten perusteella ohjelman kokonaiskustannukset ovat nousseet noin 5,9 miljardiin dollariin, mikä ylittää alkuperäisen rahoituksen moninkertaisesti. Tämä osoittaa, että alkuperäinen kustannusarvio aliarvioi merkittävästi laitekorvausten todellisen laajuuden ja markkinavaikutukset.[28]

---

[24] https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_EN.pdf; Commission estimate based on data by EIB, Analysis, GSMA and company announcements, and ETNO – European Telecommunications, Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All, March 2021.

[25] https://www.ft.com/content/54d46cf2-5e24-49d4-9939-63a564c27ca6; https://www.datacenterdynamics.com/en/news/vodafones-uk-rip-and-replace-of-huawei-kit-going-to-plan-but-5g-rollout-has-slowed-down/; https://www.lightreading.com/5g/huawei-swap-out-in-uk-has-become-a-costly-and-tortuous-slog.

[26] https://www.reuters.com/business/media-telecom/many-us-telecom-firms-need-more-funding-replace-huawei-zte-equipment-fcc-says-2024-05-02/.

[27] https://www.phonearena.com/news/FCC-says-that-40-of-rural-carriers-need-more-money-to-remove-Huawei-ZTE-gear-from-their-networks_id160385.

[28] https://www.sdxcentral.com/analysis/fcc-fully-funds-china-focused-rip-and-replace/.

78. Yhdysvaltojen kokemus osaltaan vahvistaa, että edes julkisesti rahoitettu ja keskitetysti hallinnoitu ohjelma ei poista pakolliseen verkkolaitteiden korvaamiseen liittyviä ongelmia. Pääomavaltaisilla ja keskittyneillä verkkolaitemarkkinoilla poistovelvoitteet aiheuttavat helposti rahoitusvajetta, aikataulupaineita ja toteutusriskejä, vaikka taustalla olisi kansallinen koordinointi ja taloudellinen tuki.

79. Kansainvälisten kokemusten perusteella ei ole perusteltua olettaa, että CSA2:n mukainen unionin laajuinen rip-and-replace-ohjelma välttyisi vastaavilta tai vakavammilta ongelmilta. CSA2:n soveltamisala olisi laajempi kuin Yhdistyneen kuningaskunnan ja Yhdysvaltojen ohjelmissa, ja se ulottuisi useille NIS2:n soveltamisalaan kuuluville toimialoille. Samalla siirtymäaika olisi huomattavan lyhyt, eikä ehdotus sisällä esimerkiksi Yhdysvaltojen mallin kaltaista rahoitusmekanismia. EU:n mallissa kustannukset kohdistuisivat ensisijaisesti operaattoreihin ja heijastuisivat siten edelleen käyttäjiin sekä julkisiin toimijoihin.

80. Lisäksi on ristiriitaista, että komission vaikutusarviossa esitetään mobiiliverkkoihin kohdistuville toimenpiteille satojen miljoonien eurojen kustannuslaskelmia, samalla kun poliittisessa viestinnässä korostetaan, ettei asiasta ole tehty lopullisia päätöksiä ja että jatkotoimia arvioidaan myöhemmin. Tämä herättää perustellun kysymyksen siitä, missä määrin kustannusarviot nojaavat jo ennalta oletettuun sääntelyratkaisuun sekä siitä, kuinka läpinäkyvästi niiden taustalla olevat oletukset, rajaukset ja käytetty aineisto on esitetty.

3.2 CSA2:N TEKNINEN JA SÄÄNTELYLIITÄNNÄINEN KYBERTURVALLISUUSARVIO

81. CSA2:n teknisessä ja sääntelyliitännäisessä kyberturvallisuusarviossa voidaan tunnistaa kolme keskeistä ongelmaa. Ensinnäkin sääntelyn painopiste kohdistuisi ei-teknisiin, rakenteellisiin riskeihin, vaikka tehokas kyberturvallisuus edellyttää teknisten ja ei-teknisten riskien kokonaisvaltaista ja tasapainoista arviointia. Toiseksi toimittajaturvallisuutta koskeva sääntely typistyisi käytännössä korkean riskin toimittajien luokitteluun. Kategorinen lähestymistapa kaventaisi jäsenvaltioiden harkintavaltaa ja rajoittaisi mahdollisuuksia soveltaa tapauskohtaista, riskiperusteista ja suhteellista arviointia, joka ottaa huomioon yksittäisten verkkojen tekniset ratkaisut ja kansalliset erityispiirteet. Kolmanneksi sääntelytoimenpiteiden tulisi perustua ajantasaiseen ja objektiiviseen riskinarviointiin sekä riskien vakavuuden ja kustannusten huolelliseen punnintaan. CSA2:ssa kriittisyyden käsitettä kuitenkin laajennettaisiin edellä tässä arviossa todetusti ilman riittävää erottelua verkon eri osien ja niiden todellisen riskitason välillä.

82. Kansainvälisesti hyväksytyt standardit, kuten ISO-, IEC- ja ETSI-viitekehykset sekä 3GPP:n tekniset standardit, perustuvat järjestelmälliseen riskien tunnistamiseen, arviointiin, hallintaan ja jatkuvaan seurantaan. Myös OECD korostaa, että digitaalinen turvallisuus on monitasoinen kokonaisuus, jossa tekninen haavoittuvuuksien analyysi on olennainen osa riskienhallintaa. Toimittajariskiä ei käsitellä erillisenä tai kategorisena luokitteluna, vaan osana verkon arkkitehtuuriin ja teknisiin toteutuksiin kytkeytyvää kokonaisarviota.

83. CSA2 poikkeaa tästä lähestymistavasta. Ero korostuu myös suhteessa EU:n 5G-työkalupakkiin, jossa toimittajariski käsitellään osana laajempaa, riskiperusteista

kokonaisarviointia. Työkalupakki ei sisällä unionin tasolla sitovia kieltoja, vaan jättää riskinarvioinnin ja toimenpiteiden valinnan jäsenvaltioille yhteisesti sovitussa ja koordinoidussa kehyksessä. CSA2 sen sijaan siirtäisi keskeisen arviointitoimivallan unionin tasolle ja mahdollistaisi kategoriset rajoitukset ilman vastaavaa tapauskohtaista harkintaa, mikä heikentää EU-sääntelyn joustavuutta ja aitoa riskiperusteisuutta.

84. Edellä tässä arviossa jo kuvatun mukaisesti Suomen sääntely tarjoaa esimerkin toimivasti eriytetystä ja riskiperusteisesta mallista. Kansallisen lainsäädännön mukaan verkkolaitetta ei saa käyttää julkisen viestintäverkon kriittisissä osissa, jos on vakavia perusteita epäillä, että sen käyttö vaarantaisi kansallista turvallisuutta tai maanpuolustusta esimerkiksi mahdollistamalla ulkomaisen tiedustelun tai muun yhteiskunnan elintärkeitä toimintoja vahingoittavan toiminnan. Kriittisyys määrittyy siten verkon ohjaus- ja hallintatoimintojen merkityksen perusteella eikä yleisen toimittajaluokituksen nojalla. Arviointi tehdään tapauskohtaisesti.

85. Suomessa omaksutun kaltaisessa mallissa verkkolaitteen poissulkeminen edellyttää objektiivista ja perusteltua arviota laitteen tai toimittajan aiheuttamasta konkreettisesta riskistä. Kaikkia verkon osia ei lähtökohtaisesti pidetä kriittisinä, vaan kriittisyys arvioidaan niiden teknisen tehtävän ja riskiprofiilin perusteella. Kolmansien maiden poliittiset tai lainsäädännölliset olosuhteet voivat olla yksi arviointiin vaikuttava tekijä, mutta ne eivät yksin ratkaise verkon turvallisuustasoa.

86. CSA2 muuttaisi tätä toimivaa peruslogiikkaa. Komissio voisi nimetä kolmansia maita ja sisällyttää toimittajia korkean riskin luetteloon unionin tasolla sitovin oikeusvaikutuksin. Rakenteellinen luokittelu muodostuisi ensisijaiseksi lähtökohdaksi, ja toimenpiteiden suhteellisuutta arvioitaisiin pääosin poikkeusmenettelyn kautta. Tämä merkitsisi toimivallan siirtämistä jäsenvaltioilta komissiolle. Ratkaisu poikkeaisi myös NIS2:n riskienhallintamallista, jossa toimenpiteet suhteutetaan toimijan riskiprofiiliin.

87. CSA2:n mukainen kategorinen luokittelumalli ei perustu riittävän selkeästi ajantasaiseen ja objektiiviseen riskinarviointiin, jossa toimenpiteet suhteutetaan riskien vakavuuteen ja todennäköisyyteen. Kriittisyyden käsitteen laajentaminen sekä unionin tason toimittajaluettelot voivat johtaa yleisluonteisiin rajoituksiin ilman, että verkon eri osien todellista teknistä riskiprofiilia arvioidaan eriytetysti. Tällöin vaarana on, että toimenpiteet eivät kohdistu niihin riskitekijöihin, joista suurimmat kyberturvallisuusuhat tosiasiassa syntyvät. Samalla kustannusten ja saavutettavan turvallisuushyödyn välinen suhde jää epäselväksi, mikä heikentää sääntelyn suhteellisuutta ja aiheuttaa perustuslaillisia ongelmia. Näitä käsitellään tarkemmin jäljempänä tässä arviossa.

88. CSA2:n tekninen ja sääntelyliitännäinen kyberturvallisuusarvio siten osoittaa, että ehdotus poikkeaa EU:ssa vakiintuneista riskiperusteisista periaatteista. Sääntely painottuu rakenteellisiin ja toimittajakohtaisiin luokitteluihin sekä toimittajan kotimaan lainsäädännön analyysiin, kun taas verkkoarkkitehtuuriin sidottu tekninen riskinarviointi ja toimenpiteiden suhteellisuus jäävät toissijaisiksi.

89. Unionin tason sitovat ja kategoriset toimittajaluokittelut kaventavat jäsenvaltioiden mahdollisuuksia soveltaa tapauskohtaista ja teknisesti eriytettyä arviointia. Kokonaisuutena tarkasteltuna CSA2:n malli heikentää riskiperusteisen kyberturvallisuuden systematiikkaa ja kuitenkin jättää samalla avoimeksi, parantaako se käytännössä verkkojen turvallisuutta suhteessa aiheutuviin merkittäviin rakenteellisiin ja taloudellisiin vaikutuksiin.

4 CSA2-ehdotuksen EU-oikeudellinen arvio

4.1 SEUT 114 ARTIKLAN KÄYTTÖÄ KOSKEVAT RAJOITUKSET

90. CSA2:n oikeusperustaksi esitetään SEUT[29] 114 artikla, joka koskee sisämarkkinoiden toteuttamista ja toimintaa.[30] Unionin tuomioistuimen oikeuskäytännön mukaan 114 artikla ei ole yleinen sääntelyvaltuus, vaan sen käyttö edellyttää todellista sisämarkkinatavoitetta ja tarvetta harmonisoida unionin sisämarkkinoita.[31] CSA2-ehdotuksessa ei yksilöidä konkreettisia sisämarkkinaesteitä, jotka johtuisivat nykyisistä kansallisista sääntelyratkaisuista.

91. CSA2-ehdotuksen IV-luvussa perustetaan keskitetty unionin tason mekanismi, jolla komissio voi nimetä kolmansia maita ja luetteloida ns. korkean riskin toimittajia sitovin oikeusvaikutuksin. Tämä poikkeaa perinteisestä yhdenmukaistamisesta, jossa sääntelykehys lähennetään, mutta riskien arviointi ja täytäntöönpano jäävät kansallisille viranomaisille koordinoidussa järjestelmässä. CSA2:ssa geopoliittisen tai muun kuin teknisen riskin ratkaiseva arviointi siirtyisi komissiolle.

92. Perustelut 114 artiklan soveltamiselle nojaavat lisäksi yksinkertaistettuun käsitykseen 5G- ja tulevista 6G-verkoista. Edellä jo tässä arviossa todetun mukaisesti matkaviestinverkot perustuvat 3GPP-standardeihin, jotka takaavat korkean yhteentoimivuuden. Televerkoissa käytettävä teknologia perustuu 3GPP-standardeille. Esimerkiksi tukiaseman toiminnallisuudet ja avoimet rajapinnat (NG, Xn, F1, E1, Uu) on määritelty täsmällisesti standardissa TS 38.300. Tämän vuoksi eri valmistajien käytännön tukiasematoteutukset (gNB-toteutukset) ovat keskenään samankaltaisia.[32]

93. Teleoperaattorit rakentavat tyypillisesti verkkonsa useiden eri laitetoimittajien ratkaisuilla. Standardisointi mahdollistaa sen, että laitevalmistaja A:n päätelaite toimii saumattomasti verkossa, jossa tukiaseman on toimittanut B, siirtoverkon C ja runkoverkossa D ja E. Eurooppalaiset teleoperaattorit ovat tyypillisesti vallinneet useamman kuin yhden toimittajan

[29] https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A12016ME%2FTXT.

[30] Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security, and repealing Regulation (EU) 2019/881 (Cybersecurity Act 2, CSA2) 2026/0011 (COD); https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act, s. 5.

[31] Ks. esim. Unionin tuomioistuimen ratkaisu asiassa C-376/98 *Germany v Parliament and Council (Tobacco Advertising I),* kohta 84.

[32] Ks. Juha Korhonen 2025.

radioverkkoon. Standardisoinnin vuoksi jopa yksittäinen tukiasema saattaa koostua useamman kuin yhden laitetoimittajan ratkaisuista ja osa tukiaseman komponenteista voidaan esimerkiksi toteuttaa virtualisoituna pilvilaskentaa hyödyntäen.

94. Verkkojen keskeiset rajapinnat ja toiminnot on siten standardoitu, ja laite- ja ohjelmistomarkkinat toimivat unionissa ilman rakenteellisia esteitä. Tukiasemat ovat luonteeltaan paikallisia, ja verkkojen ydin ja hallinta ovat kansallisten operaattoreiden vastuulla. Tukiaseman vaikutusalue on paikallinen. Tukiasemat eivät pääsääntöisesti ole suoraan yhteydessä toisiinsa, vaan kaikki liikenne ja käyttäjien autentikointi kulkevat runkoverkkojen kautta.

95. CSA2-ehdotuksessa ei osoiteta, että standardoituihin verkon osiin liittyisi sisämarkkinaongelmia.

96. Eurooppalaiset teleoperaattorit ovat vuosikymmeniä koordinoineet radiotaajuuksien käyttöä raja-alueilla. Haasteet tässä liittyvät pääosin hallinnollisiin kysymyksiin. Mahdolliset erilaiset rajoitukset laitevalmistajakysymyksissä eivät aiheuta ylitsepääsemätöntä käytännön vaikeutta rajat ylittävää radioverkkoa suunnittelevalle teleoperaattorille. Raja-alueille voidaan valita sellaisen laitetoimittajan tukiasemia, joihin ei kohdistu rajoituksia millään puolella rajaa. Vaihtelevilla kansallisilla lähestymistavoilla ei voi siten olla sisämarkkinoita pirstaloivaa vaikutusta, jos tukiaseman tai muun alueellisen verkkolaitteen vaikutusalue ei ulotu rajan yli.

97. Kansalliset erot laitetoimittajien riskien arvioinnissa eivät aiheuta esteitä myöskään teleoperaattorien palveluiden vapaalle liikkuvuudelle. Komission CSA2-esityksessä tai muutoinkaan ei ole näyttöä siitä, että vaihtelevat kansalliset lähestymistavat pirstaloisivat sisämarkkinoita tai vääristäisivät teleyritysten kilpailua. Kansalliset erot laitetoimittajien riskiarvioinneissa ja jäsenvaltioiden toimenpiteissä eivät myöskään ole aiheuttaneet esteitä telealan konsolidaatiolle. Komission lähestymistapa ei siten ole uskottava etenkään liityntä- ja siirtoverkkojen osalta.

98. Myös runkoverkot ovat lähtökohtaisesti kansallisia kokonaisuuksia. Mahdolliset sisämarkkinaesteet liittyvät tässä yhteydessä pikemminkin jäsenvaltioiden toisistaan poikkeaviin vaatimuksiin esimerkiksi tietosuojasta tai viranomaisten tiedonsaanti- ja avustamisvelvoitteista, jotka voivat edellyttää kansallisesti eriytettyä runkoverkkoratkaisua. Ne eivät johdu laitetoimittajien valinnoista.

99. Jos EU:n tavoitteena olisi luoda rajat ylittävä eurooppalainen ydinverkko, kyse olisi olennaisesti erilaisesta ja huomattavasti CSA2:ta laajemmasta hankkeesta, joka edellyttäisi eurooppalaisen taajuuspolitiikan ja verkkoarkkitehtuurin perusteellista uudelleenjärjestelyä. Mikäli komission tavoitteena on edistää monikansallisten operaattorien mahdollisuuksia toteuttaa rajat ylittäviä core-verkkoja tai esimerkiksi OSS/BSS-järjestelmien kehittämistä, voisi SEUT 114 mukainen harmonisointi olla asiallisesti ja siten myös oikeudellisesti perusteltua.

100. CSA2 ei kuitenkaan rakenna tällaista mallia, eikä nykyinen järjestelmä teknisen yhteentoimivuuden vuoksi lähtökohtaisesti estä sisämarkkinoiden toimintaa. Jos kansallisten verkkojen rinnalle haluttaisiin luoda eurooppalainen runkoverkko ja yleiseurooppalaiset operaattorit, voisi tämän sääntelyn perustana olla SEUT 114 artikla. Sen sijaan nyt ehdotettu malli kohdistuisi suoraan kansalliseen viestintäinfrastruktuuriin ja sen tekniseen kokoonpanoon ilman, että kyse olisi rajat ylittävän verkkoarkkitehtuurin rakentamisesta tai sisämarkkinoiden toiminnan esteiden poistamisesta.

101. Kansallinen verkkoinfrastruktuuri on kiinteä osa jäsenvaltioiden kriittistä infrastruktuuria ja kokonaisturvallisuutta, ja siihen liittyvät riskinarvioinnit sekä verkon rakenteelliset ratkaisut tulisi lähtökohtaisesti jättää kansallisen päätöksenteon ja vastuun piiriin. Unionitason harmonisoinnin tulisi rajoittua aineellisten vaatimusten ja yhteisten kriteerien määrittelyyn, ei yksittäisten jäsenvaltioiden verkkojen teknisen kokoonpanon tosiasialliseen ohjaamiseen.

102. SEUT 114 artikla on asianmukainen oikeusperusta siltä osin kuin kysymys on ENISA:a koskevasta sääntelystä sekä eurooppalaisesta kyberturvallisuussertifioinnista.

103. Tämän vuoksi keskeinen kysymys CSA2-ehdituksessa on se, palveleeko ehdotuksen IV-luku tosiasiallisesti sisämarkkinoiden yhdentymistä vai ensisijaisesti taloudellisen turvallisuuden ja geopoliittisten riskien hallintaa. Jos SEUT 114 artiklaa käytetään oikeusperustana unionin tason kolmansien maiden nimeämiseen ja yritysten luettelointiin geopoliittisin perustein, sen soveltamisala lähenee yleistä turvallisuuspoliittista toimivaltaa.

104. Lisäksi kyberturvallisuuden sekä turvallisuuspoliittiset tavoitteet Euroopan unionin teknologisesta suvereniteetista ovat saavutettavissa olennaisesti vähemmän perusoikeuksia rajoittavilla toimenpiteillä kuin mitä CSA2 esittää. Toimittajien riskien arviointiin olisi riskiperusteisen ajattelutavan mukaisesti perusteltua soveltaa eri tasoisia vaatimuksia verkkojen eri osissa, kuten tässä arviossa on perusteltu edellä.

105. CSA2 herättää näin ollen perustellun EU- ja valtiosääntöoikeudellisen kritiikin siitä, pysyykö se SEUT 114 artiklan asettamissa rajoissa. Vaikka osa ehdotuksesta liittyy yhdenmukaistamiseen, IV-luvun mekanismi keskittää geopoliittisen riskinarvioinnin ja toimittajien poissulkemisen unionin tasolle tavalla, joka ylittää tavanomaisen lainsäädännön lähentämisen ja venyttää 114 artiklan toiminnallista soveltamisalaa.

106. Tältä osin Suomen edustajien olisi perusteltua edellyttää CSA2-ehdotuksen oikeusperustan asianmukaisuuden perusteellista arviointia osana neuvostossa tehtävää valmistelua.

4.2 TOISSIJAISUUS JA SUHTEELLISUUSPERIAATE

107. CSA2:n on myös noudatettava SEUT 5 artiklan 3 ja 4 kohdassa vahvistettuja toissijaisuus- ja suhteellisuusperiaatteita. Nämä periaatteet rajoittavat jaetun toimivallan käyttöä ja edellyttävät riippumatonta perustuslaillista tarkastelua. Unionin tulee osoittaa, että tavoitteita ei voida saavuttaa riittävästi jäsenvaltioiden tasolla, ja että ne voidaan paremmin saavuttaa unionin tasolla.

108. Suhteellisuusperiaatteen kannalta arviointi kohdistuu toimenpiteen soveltuvuuteen, tarpeellisuuteen ja siitä aiheutuviin rasitteisiin. Vaikka unionin tason mekanismi voi lisätä yhdenmukaisuutta, CSA2-ehdotuksessa ei osoiteta, että päätösten keskittäminen parantaisi sisämarkkinoiden toimintaa enemmän kuin harmonisoidut aineelliset kriteerit ja kansallinen täytäntöönpano. Yhteys keskitetyn toimittajien nimeämisen ja markkinoiden yhdentymisen välillä jää siten heikosti perustelluksi.

109. Suhteellisuuden osalta CSA2 valitsee vahvasti puutuvan mallin, jossa unionin tasolla tehtävillä nimeämis- ja luettelointipäätöksillä on välittömiä ja sitovia poissulkevia vaikutuksia kaikissa jäsenvaltioissa. Ehdotuksessa ei osoiteta, miksi vähemmän rajoittavat vaihtoehdot eivät riittäisi.

110. Toimenpiteiden rasitteet voivat olla merkittäviä. Toimittajaluettelointi voi johtaa keskeisten ICT-resurssien menettämiseen, hankintarajoituksiin, nopeutettuun laitteiston poistamiseen ja huomattaviin kustannuksiin. CSA2:ssa ei kuitenkaan esitetä konkreettista punnintaa näiden seurausten ja mahdollisten sisämarkkinahyötyjen välillä.

111. Suhteellisuus edellyttää myös tehokkaita prosessuaalisia oikeuksia yksityisille asianosaisille. Unionin laajuisilla poissulkemispäätöksillä voi olla huomattavia taloudellisia vaikutuksia, joten puolustautumisoikeuksien ja tehokkaan oikeussuojan on oltava aidosti toimivia. Komission harkintavalta on CSA2-ehdotuksesa kuitenkin laajasti muotoiltu, eikä ehdotuksessa yksityiskohtaisesti rajata sen käyttöä.

112. Kokonaisuutena CSA2 herättää siksi merkittävää kritiikkiä toissijaisuus- ja suhteellisuusperiaatteiden noudattamisesta. Kolmansien maiden nimeämisen ja toimittajien luetteloinnin keskittäminen unionin tasolle merkitsee komission toimivallan huomattavaa laajentamista. Ilman täsmällistä näyttöä toimenpiteen välttämättömyydestä ja oikeasuhtaisuudesta ehdotus on vaarassa ylittää jaetun toimivallan perustuslailliset rajat.

5 CSA2-ehdotuksen oikeudellinen arvio Suomen näkökulmasta

5.1 EU:N PERUSOIKEUSKIRJA

113. Euroopan unionin perusoikeuskirja (2012/C 326/02)[33] (**perusoikeuskirja**) koskee EU:n toimielimiä unionin lainsäädännön hyväksymisessä ja jäsenvaltioita unionin lainsäädännön täytäntöönpanossa. Komissio olisi siten CSA2:n nojalla täytäntöönpanosäädöksiä antaessaan velvollinen noudattamaan perusoikeuskirjaa. Myös jäsenvaltioiden viranomaiset, jotka soveltaisivat CSA2:ta, toimisivat perusoikeuskirjan sääntelyn piirissä.

114. CSA2:n mukaiset toimenpiteet voisivat aiheuttaa yksityisille yrityksille merkittäviä oikeudellisia vaikutuksia. Tämän vuoksi ehdotuksen arvioinnissa keskeisiä ovat erityisesti perusoikeuskirjan 16, 17 ja 41 artikla sekä 52 artiklan 1 kohta.

[33] https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:12012P/TXT.

115. Perusoikeuskirjan 16 artikla turvaa elinkeinovapauden unionin ja kansallisen lainsäädännön mukaisesti. CSA2 mahdollistaisi kolmansien maiden nimeämisen ja ns. korkean riskin toimittajien luetteloinnin täytäntöönpanosäädöksillä, millä olisi tosiasiallisesti markkinoilta sulkeva vaikutus. Puuttuminen elinkeinovapauteen olisi siten huomattava.

116. Perusoikeuskirjan 17 artikla suojaa omaisuutta ja immateriaalioikeuksia. Korkean riskin toimittajien nimeämiseen liittyvät rajoitukset voisivat johtaa sopimussuhteiden päättymiseen, laitteiden pakolliseen poistamiseen ja investointien arvon alenemiseen. Ehdotetut siirtymäajat merkitsisivät lisäksi omaisuuserien ennenaikaista käytöstä poistoa.

117. Perusoikeuskirjan 41 artikla turvaa oikeuden hyvään hallintoon, mukaan lukien oikeuden tulla kuulluksi, oikeuden tutustua asiakirjoihin sekä asettaa viranomaisille velvollisuuden perustella päätöksensä. Nämä vaatimukset koskevat suoraan CSA2:n 100 artiklan mukaista kolmansien maiden nimeämistä ja 104 artiklan mukaista korkean riskin toimittajien luettelointia silloin, kun niillä on rajoittavia vaikutuksia yksittäisiin yrityksiin. Lisäksi perusoikeuskirjan 47 artikla edellyttää tehokasta oikeussuojaa.

118. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan oikeuksien rajoitusten on perustuttava lakiin, kunnioitettava oikeuksien ydinsisältöä ja oltava tarpeellisia ja oikeasuhteisia hyväksyttävän yleisen edun tavoitteen kannalta. CSA2:n tavoitteet, kuten kyberturvallisuus ja kriittisen infrastruktuurin suoja, ovat itsessään sinänsä lähtökohtaisesti hyväksyttäviä. Keskeinen arviointikysymys liittyy siten ehdotuksen suhteellisuuteen ja prosessuaalisten oikeuksien riittävyyteen.

119. CSA2-ehdotuksen puuttuminen erityisesti perusoikeuskirjan 16 artiklaan kohdistuen on laaja, koska ns. korkean riskin toimittajan luokittelu voi käytännössä merkitä unioninlaajuista markkinoilta sulkemista. CSA2-ehdotuksessa ei osoiteta riittävän selvästi, miksi näin ankara väline olisi välttämätön suhteessa vähemmän rajoittaviin keinoihin.

120. Suhteellisuus liittyy myös prosessuaaliseen oikeudenmukaisuuteen. Komission nimeämis- ja luettelointivaltuuksien on täytettävä perusoikeuskirjan 41 ja 47 artiklan vaatimukset. Vaikka CSA2 sisältää kuulemismenettelyjä, ehdotus ei täsmennä riittävästi, mitä tietoja toimittajalle on vähintään annettava, jotta oikeus tulla kuulluksi toteutuu tehokkaasti. Jos päätökset esimerkiksi perustuvat salassa pidettäviin tietoihin, yksityinen yritys voi joutua puolustautumaan ilman pääsyä keskeisiin asiakirjoihin. Ilman selkeitä sääntöjä asiakirjojen saatavuudesta ja päätösten perusteluista on olemassa riski, että kuuleminen jää muodolliseksi eikä todellisuudessa täytä 41 artiklan vaatimuksia.

121. Erityisen ongelmallinen on säännös, jonka mukaan yksityisen asianosaisen tietojen toimittamatta jättäminen sille asetetussa määräajassa voi johtaa siihen, että komissio päättelee toimittajan olevan sijoittautunut nimettyyn kolmanteen maahan tai olevan sen määräysvallassa. Tämä merkitsee todistustaakan siirtymistä yksityiselle asianosaiselle tavalla, jolla voi olla huomattavia oikeudellisia ja taloudellisia seurauksia. Tietojen puuttuminen ei myöskään välttämättä johdu yhteistyöhaluttomuudesta, vaan se voi olla seurausta esimerkiksi kolmannen maan lainsäädännöllisistä rajoitteista, salassapitovelvoitteista tai muista oikeudellisista esteistä.

122. Yksityiselle asianosaiselle epäedullisen ratkaisun tekeminen tällaisessa tilanteessa voi merkittävästi heikentää perusoikeuskirjan 41 artiklassa turvattua oikeutta hyvään hallintoon sekä 47 artiklassa turvattua oikeutta tehokkaaseen oikeussuojaan ja oikeudenmukaiseen oikeudenkäyntiin.[34] EU:ssa ei tulisi edistää tällaisia ratkaisuja.

5.2 SUOMEN PERUSTUSLAKI

5.2.1 Perusoikeudet Suomen perustuslaissa

123. Unionin oikeuden ensisijaisuusperiaatteen mukaan EU-oikeus on etusijalla suhteessa kansalliseen oikeuteen, mukaan lukien Suomen perustuslakiin (731/1999 muutoksineen)[35]. Jos CSA2-ehdotus hyväksyttäisiin, se olisi suoraan sovellettavaa oikeutta kaikissa EU:n jäsenvaltioissa.

124. Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan unionin lainsäädäntö on ensisijaista suhteessa kansallisiin säännöksiin oikeuskäytännössä määriteltyjen edellytysten mukaisesti.[36] Suomalaisessa lainsäädännössä ei tule pyrkiä EU-oikeuden kanssa ristiriidassa oleviin ratkaisuihin.[37] Euroopan unionin sääntelyn jättämän liikkumavaran puitteissa kansallisen lainsäätäjän on otettava huomioon perus- ja ihmisoikeuksista seuraavat vaatimukset.[38]

125. Perustuslain 22 §:n mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Sama velvoite sisältyy myös jokaiseen perusoikeuteen ja niiden taustalla oleviin kansainvälisiin ihmisoikeusvelvoitteisiin. Turvaamisvelvoite koskee myös tilanteita, joissa kansalliset viranomaiset soveltavat ja panevat täytäntöön suoraan sovellettavaa unionin oikeutta. Samoin lainsoveltajan on tulkittava myös unionin oikeutta perusoikeuksien vaatimukset huomioon ottavalla tavalla.

---

[34] CSA2:n mekanismit ja todistustaakkaa koskevat säännöt ovat samankaltaisia kuin EU:n kaupan suojatoimivälineissä yleisesti käytetyt ja hyväksytyt menettelyt, mukaan lukien perusasetukset (EU) 2016/1036 ja 2016/1037. Kokemus on osoittanut, että komission arvioinnin riitauttamiseksi vaadittavan todistustaakan täyttäminen on erittäin vaikeaa. EU:n kaupan suojatoimivälineissä vaikutuksia kuitenkin lievennetään merkittävästi erilaisilla yrityskohtaisilla sitoumuspäätöksillä, joissa yritys voi sitoutua riittäviin korjaaviin toimenpiteisiin ja näitä toimenpiteitä noudattaessaan jatkaa toimintaansa sisämarkkinoilla. CSA2 ei sisällä vastaavia mekanismeja, mikä tekee ehdotetun asetuksen seurauksista huomattavasti ankarampia ja suhteettomampia. CSA2:n 105 artiklassa säädetään poikkeusjärjestelmästä, joka jakaa tiettyjä rakenteellisia piirteitä asetusten (EU) 2016/1036 ja 2016/1037 mukaisten sitoumusten kanssa, mutta muodostaa lopulta erillisen sääntelymekanismin. Artiklan 105 mukaiset poikkeukset toimivat harkinnanvaraisina poikkeuksina turvallisuusperusteisista kielloista, ja ne myönnetään vain, jos hakija osoittaa tehokkaan riskien lieventämisen sekä sen, ettei kyseessä ole kolmannen maan sopimaton vaikutus. Sen sijaan asetusten (EU) 2016/1036 ja 2016/1037 mukaiset sitoumukset toimivat tullien vaihtoehtoisena täytäntöönpanokeinona, ja ne hyväksytään, jos yritys poistaa polkumyynnin tai tuen sekä siitä aiheutuneen vahingon.

[35] https://www.finlex.fi/fi/lainsaadanto/1999/731.

[36] PeVL 18/2024 vp, kappale 32; PeVL 14/2018 vp, s. 13; PeVL 20/2017 vp, s. 6.

[37] PeVL18/2024 vp, kappale 32; PeVL 15/2018 vp, s. 49; PeVL 14/2018 vp, s. 13; PeVL 26/2017 vp, s. 42.

[38] PeVL 6/2026 vp, kappale 3; PeVL 33/2025 vp, kappale 4; PeVL 8/2021 vp, s. 2; PeVL 9/2019 vp, s. 2, PeVL 1/2018 vp, s. 3.

126. Jäsenvaltioiden viranomaiset, jotka panevat CSA2:n sääntelyä täytäntöön, käyttävät julkista valtaa. Niiden on tällöin noudatettava perustuslain vaatimuksia laillisuudesta, suhteellisuudesta ja oikeussuojasta. Perustuslain 21 § turvaa oikeuden hyvään hallintoon ja hyvän hallinnon takeiden toteutumiseen, kuten oikeuteen saada perusteltu päätös ja muutoksenhakuun. Viranomaisten on samoin sovellettava perustuslain mukaisia perusoikeuksia ja niiden soveltamista ja rajoittamista koskevia yleisiä periaatteita unionin oikeuden jättämän kansallisen liikkumavaran puitteissa.

127. Vakiintuneen valtiosääntökäytännön mukaan Suomen hallituksen ministerit ja muut edustajat ottavat osallistuessaan unionin säädösehdotusten valmisteluun ja neuvottelemiseen Euroopan unionin neuvostossa ja sen valmisteluelimissä huomioon perustuslain vaatimukset.

128. Perustuslakivaliokunta on korostanut, että Suomen perustuslaissa turvatut perusoikeudet ovat merkityksellisiä myös EU-sääntelyä valmisteltaessa. Valiokunta on pitänyt selvänä, että Suomen perustuslain tulee ohjata valtioneuvoston kannanmuodostusta EU-lainsäädännön valmistelussa.[39] Suomen edustajien tulee siten pyrkiä edistämään ratkaisuja, joilla varmistetaan, että unionin sääntely on yhteensopivaa perustuslain kanssa ja että perusoikeuksien turvaaminen toteutuu myös unionin tasolla hyväksyttävässä sääntelyssä.[40]

129. Euroopan unionin säädöksen oikeusperustan asianmukaisuus on EU-oikeudellinen kysymys, jonka ratkaisee viime kädessä EU-tuomioistuin. Perustuslakivaliokunta on kuitenkin pitänyt tärkeänä, että unionilainsäädäntöä kehitetään ensisijaisesti perussopimusten puitteissa. Perustuslakivaliokunta on näistä syistä edellyttänyt, että valtioneuvosto ja Suomen edustajat neuvoston valmisteluelimissä ja neuvostossa varmistuvat oikeusperustan asianmukaisuudesta silloin, kun se herättää kritiikkiä.[41]

130. CSA2-ehdotukselle on siksi perusteltua tehdä huolellinen oikeusperustan asianmukaisuuden varmistaminen.[42]

5.2.1.1 Perustuslain 15 §: Omaisuudensuoja

131. Perustuslain 15 §:n mukaan jokaisen omaisuus on turvattu. Vastaavasti EU:n perusoikeuskirjan 17 artikla suojaa omistusoikeutta. Ehdotetun CSA2:n mukaiset ns.

[39] PeVL 6/2023 vp, kappale 10; PeVL 16/2022 vp, kappale 6; PeVL 20/2021 vp, kappale 11; PeVL 15/2017 vp, s. 4; PeVL 9/2017 vp, s. 5—6 ja niissä viitatut lausunnot.
[40] Ks. tästä omaisuuden suojan turvaamisen näkökulmasta esimerkiksi PeVL 67/2022 vp ja PeVL 62/2022 vp.
[41] PeVL 6/2023 vp, kappale 5–8; PeVL 47/2022 vp, kappale 15; PeVL 61/2016 vp.
[42] Myös suomalainen ICT-alan edunvalvoja FiCom ry on 17.2.2026 antamassaan lausunnossa valtioneuvoston U-kirjelmäluonnokseen CSA2-asetuksesta ja NIS2-muutosridektiivistä todennut, että ”sääntelyn tulee olla riskiperusteista, ennakoitavaa ja oikeasuhtaista, ja sen on tuettava viestintäpalveluiden jatkuvuutta sekä oltava sopusoinnussa perusoikeusjärjestelmän ja jäsenvaltioiden toimivallan kanssa”. FiCom ry esittää lausunnossaan useita täydennyksiä valtioneuvoston U-kirjelmäluonnokseen liittyen ICT-toimitusketjujen riskienhallintaa, rajoituksia ja teknistä toteutettavuutta koskeviin periaatteetteisiin, komission toimivaltuuksien tarkentamiseen, tietojen luottamuksellisuuden varmistamiseen sekä sääntelystä aiheutuvien kustannusten ja hallinnollisen taakan arviointiin; https://ficom.fi/ajankohtaista/lausunnot/ficomin-kommentit-valtioneuvoston-u%E2%80%91kirjelmaluonnokseen-csa2%E2%80%91asetuksesta-ja-nis2%E2%80%91muutosdirektiivista/.

korkean riskin toimittajien nimeäminen ja siitä johtuvat rajoittavat toimenpiteet vaikuttavat omaisuudensuojaan poikkeuksellisen merkittävästi.

132. Suomen perustuslain näkökulmasta CSA2:n säännökset herättävät kysymyksen siitä, tarkoittaako ns. korkean riskin toimittajien laitteiden poistaminen asiallisesti Suomen perustuslain näkökulmasta pakkolunastukseen vaikutuksiltaan rinnastuvaa käyttörajoitusta, jolloin perustuslain 15 §:n 2 momentin ja sen soveltamista koskevan perustuslakivaliokunnan vakiintuneen tulkintakäytännön mukaan rajoituksen hyväksyttävyyden edellytyksenä on täysi korvaus.[43] Vaikka omaisuutta ei siirrettäisi julkiselle vallalle, omaisuudensuoja tulee valtiosääntöoikeudellisesti arvioitavaksi myös silloin, kun sääntely rajoittaa merkittävästi omaisuuden käyttöä tai aiheuttaa merkittäviä taloudellisia rasitteita yksityisille toimijoille. Arvioinnissa keskeistä on, ovatko rajoitukset lailla säädettyjä, täsmällisiä, hyväksyttävään tarkoitukseen perustuvia ja painavan yhteiskunnallisen tarpeen välttämättä vaatimia sekä oikeasuhtaisia suhteessa tavoiteltuun päämäärään.[44]

133. Suomen perustuslain 15 §:n 1 momentin mukaan jokaisen omaisuus on turvattu, ja 2 momentin mukaan omaisuuden pakkolunastuksesta on säädettävä lailla ja siitä on suoritettava täysi korvaus. Perustuslaillisesti erotetaan siten tavanomaiset omaisuuden käyttöä koskevat rajoitukset ja pakkolunastukseen rinnastuvat toimenpiteet. Jälkimmäisissä täyden korvauksen vaatimus muodostaa perustuslaillisen vähimmäistason. Erottelussa olennaista on, estyykö omaisuudenhaltijan mahdollisuus käyttää omaisuutta pääasialliseen käyttötarkoitukseensa.[45]

134. Perustuslakivaliokunta on vakiintuneesti tulkinnut perustuslain 15 §:ää siten, että kaikki omaisuudensuojaan kohdistuvat puuttumiset on arvioitava perusoikeuksien rajoitusedellytysten yleisten vaatimusten mukaisesti. Tämä merkitsee sitä, että myös omaisuuden käyttöä koskevien rajoitusten tulee perustua lakiin, olla täsmällisiä ja tarkkarajaisia, hyväksyttävään tarkoitukseen perustuvia sekä oikeasuhtaisia.

135. Näin ollen omaisuudensuojaan kohdistuvan rajoituksen on täytettävä perusoikeuksien yleiset rajoitusedellytykset. Rajoituksen tulee siten (i) perustua eduskunnan säätämään lakiin; (ii) tavoitella hyväksyttävää ja riittävän painavaa yhteiskunnallista päämäärää; (iii) olla suhteellisuusvaatimuksen mukainen; (iv) olla puuttumatta oikeuden ydinsisältöön; (v) turvata riittävät oikeussuojakeinot; ja (vi) olla Suomen kansainvälisten ihmisoikeusvelvoitteiden mukainen.[46]

136. Jos jokin näistä kumulatiivisista vaatimuksista ei täyty, rajoitus on perustuslain kannalta ongelmallinen. Esityksen jatkokäsittelyssä Suomen edustajien tulisikin pyrkiä perustuslaillisten ongelmien poistamiseen tai vähintään niiden merkittävään lieventämiseen.

[43] PeVL 8/2017 vp; PeVL 32/2010 vp; PeVL 38/1998 vp.
[44] PeVL 6/2026 vp, kappale 7 ja siinä viitatut lausunnot.
[45] PeVL 6/2026 vp, kappale 7; PeVL 35/2020 vp.
[46] PeVL 25/1994 vp, s. 4–5.

CSA2-esityksen osalta erityisesti suhteellisuusperiaate eli rajoitusten oikeasuhtaisuus on keskeisessä asemassa omaisuudensuojaa koskevassa arvioinnissa.

137. Omaisuudensuojaa rajoittavan toimenpiteen tulee säilyttää oikeudenmukainen tasapaino tavoitellun yleisen edun ja yksityiselle aiheutuvan haitan välillä siten, ettei yksittäiselle toimijalle kohdistu kohtuutonta tai epäsuhteista rasitetta suhteessa sääntelyn päämäärään.[47] Jos tämä tasapaino ei toteudu, rajoitus voidaan katsoa perustuslain vastaiseksi tai tosiasialliseksi pakkolunastukseksi, joka edellä todetusti edellyttää täyttä korvausta.[48]

138. Omaisuuteen kohdistuvien rajoitusten hyväksyttävyys on perustuslakivaliokunnan käytännössä ollut vahvempi silloin, kun rajoitus palvelee toisen perusoikeuden tai erittäin painavan yleisen edun turvaamista, kuten ympäristönsuojelua. Ympäristönsuojelun osalta arvioitavana on ollut kysymys omaisuudensuojan tasapainottamisesta perustuslain 20 §:ssä säädetyn ympäristöperusoikeuden kanssa. Esimerkiksi kivihiilen käytön kieltäminen suurissa voimalaitoksissa on katsottu perustuslakivaliokunnan käytännössä perustuslain mukaiseksi. Arvioinnissa merkitystä on annettu erityisesti riittävän pitkälle siirtymäajalle, joka on mahdollistanut omaisuuden käytön jatkamisen sen taloudellisen elinkaaren ajan, sekä ympäristönsuojelun huomattavalle painoarvolle kilpailevien oikeuksien ja etujen punninnassa ilmastonmuutoksen torjunnan yhteydessä.[49]

139. Perustuslaillisen omaisuudensuojan näkökulmasta velvollisuus poistaa omaisuus kesken sen taloudellista käyttöaikaa rinnastuu perustuslakivaliokunnan käytännössä pakkolunastukseen, jollei kysymyksessä ole vähäinen omaisuusmassa, ja jollei toimijalla ole jo ennakkoon ollut syytä olettaa, että lainsäädännöstä voi johtua rajoituksia omaisuuden käytölle. Taloudellista elinkaarta arvioidaan perustuslain soveltamiskäytännössä omaisuuden tosiasiallisen käyttökelpoisuuden perusteella. Ratkaisevaa ei ole investointimenojen kirjanpidollinen käsittely tai poistojen muodollinen aikataulu, vaan se, onko omaisuus edelleen teknisesti ja taloudellisesti käyttökelpoinen sekä tosiasiallisesti hyödynnettävissä sen tarkoitettuun käyttöön.

140. Ratkaisevaa siten on, miten rajoitus vaikuttaa omaisuuden käyttöön ja arvoon. Vaikka kansallinen turvallisuus on sinänsä painava ja hyväksyttävä peruste omaisuuden käyttöä koskeville rajoituksille, perustuslakikäytännössä on katsottu, että myös tällaisissa tilanteissa voidaan edellyttää korvausta, jos rajoituksen vaikutukset ovat poikkeuksellisen ankarat tai rinnastuvat pakkolunastukseen.[50]

141. Suomen perustuslakia on tulkittava Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa. Euroopan ihmisoikeussopimuksen omaisuudensuojaa koskeva tulkintakäytäntö sisältää vaatimuksen oikeudenmukaisesta tasapainosta sekä tietyissä tilanteissa myös asianmukaisesta korvauksesta. Unionin oikeudessa Euroopan ihmisoikeussopimuksen periaatteet muodostavat osan unionin oikeuden yleisiä periaatteita. Suomen

[47] PeVL 55/2018 vp; PeVL 10/2010 vp; PeVL 6/2010 vp.
[48] PeVL 55/2018 vp; PeVL 10/2010 vp; PeVL 6/2010 vp.
[49] PeVL 55/2018 vp.
[50] PeVL 37/2022 vp, 8 ja 32 kohta; PeVL 16/2022 vp; PeVL 57/2018 vp.

perustuslakivaliokunnan vakiintuneen kannan mukaan unionin sääntelyn on turvattava perusoikeuksien osalta vähintään vastaava suojan taso kuin mitä perustuslaki ja ihmisoikeussopimus edellyttävät.

142. CSA2:n tapauksessa on siksi esitettävä painavaa kritiikkiä siitä, onko ehdotus Euroopan ihmisoikeussopimuksen vaatimusten mukainen.

143. CSA2:n ongelmat Suomen perustuslain 15 §:n kannalta ovat tiivistetysti ainakin seuraavat:

1. *Vakava taloudellinen puuttuminen ilman korvausta:*

   Jos suomalaiset operaattorit joutuisivat EU:n tason luettelointipäätösten seurauksena korvaamaan osia infrastruktuuristaan tai päättämään olemassa olevia toimittajasuhteita, niille voi aiheutua huomattavia ja yksittäisille toimijoille keskittyviä kustannuksia. Sääntely ilman olennaisia lievennyksiä näyttäisi tosiasiallisesti merkitsevän pakkolunastukseen rinnastuvaa puuttumista omaisuudensuojaan ilman asianmukaista korvausjärjestelmää, mikä olisi Suomen perustuslain perusteella perustuslain vastaista.

2. *Liian heikko ennustettavuus ja oikeusvarmuus:*

   Korkean riskin toimittajan määritelmä perustuisi osin omistus- ja määräysvaltasuhteita koskeviin kriteereihin, joiden soveltaminen voi olla ennakolta vaikeasti arvioitavissa erityisesti monimutkaisissa konsernirakenteissa ja rajat ylittävissä omistusjärjestelyissä. Tämä voisi heikentää sääntelyn ennakoitavuutta ja oikeusvarmuutta sekä vaikeuttaa pitkäjänteistä omaisuuden käyttöä ja investointien suunnittelua.

3. *Lyhyet poistamisaikataulut*

   Mobiiliverkkojen enintään 36 kuukauden pituinen vaiheittainen poistovelvoite on verkkoarkkitehtuurin laajuus ja tekninen monimutkaisuus huomioon ottaen poikkeuksellisen lyhyt. Näin tiukka määräaika vahvistaa arviota siitä, että omaisuudensuojaan kohdistuva puuttuminen muodostuu vaikutuksiltaan suhteettomaksi verrattuna toimenpiteellä saavutettavissa olevaan hyötyyn.

144. Perustuslain 15 §:n omaisuudensuojaa koskevat vaatimukset sitovat Suomen hallitusta ja sen edustajia heidän osallistuessaan Euroopan unionin neuvostossa ja sen valmistelevissa elimissä käytäviin neuvotteluihin EU:n säädösehdotuksista.

145. Perustuslakivaliokunta on korostanut, että Suomen edustajien on tuotava unionin lainsäädäntöneuvotteluissa esiin omaisuudensuojaan liittyvät perustuslailliset huolenaiheet

ja tarvittaessa vastustettava säädösehdotusta, mikäli se on ristiriidassa perustuslain turvaaman omaisuudensuojan tai muiden perusoikeuksien kanssa.[51]

146. Perustuslakivaliokunta on lisäksi katsonut, että jäsenvaltion budjettisuvereniteettia on suojeltava tehokkaasti myös tilanteissa, joissa unionin säädös velvoittaisi toteuttamaan merkittäviä kustannuksia aiheuttavia toimenpiteitä ilman, että niille osoitetaan rahoitusta unionin talousarviosta.[52]

5.2.1.2 Perustuslain 18 §: Oikeus harjoittaa elinkeinotoimintaa

147. Suomen perustuslain 18 § turvaa jokaiselle oikeuden hankkia toimeentulonsa valitsemallaan työllä, ammatilla tai elinkeinolla lain mukaisesti. Vaikka säännös liitetään usein luonnollisiin henkilöihin, sen on katsottu ulottuvan myös yritystoimintaan siltä osin kuin se heijastaa perustuslaillista sitoutumista elinkeinovapauteen, taloudelliseen toimintavapauteen ja oikeusvarmuuteen kaupallisessa toiminnassa.

148. CSA2:lla luotaisiin sääntelymekanismi, jonka nojalla komissio voisi unionin tason täytäntöönpanosäädöksillä nimetä kolmansia maita ja laatia luettelon ns. korkean riskin toimittajista. Päätökset voisivat käytännössä johtaa siihen, että tietyt toimittajat suljetaan markkinoilta unionin alueella.

149. CSA2:n valtiosääntöoikeudelliset ongelmakohdat ovat tältä osin tiivistetysti ainakin seuraavat:

1. *De facto -markkinoilta sulkeminen:*

   Jos korkean riskin toimittajien luetteloon ottaminen johtaa toimittajan sulkemiseen julkisista hankinnoista, rajoittaa rahoituksen saamisen edellytyksiä tai tiettyjen ICT-tuotteiden toimittamista, kyse on lähtökohtaisesti merkittävästä puuttumisesta perusoikeutena suojattuun elinkeinovapauteen.

2. *Liian laaja kattavuus suppeilla arviointikriteereillä:*

   CSA2 ulottaa korkean riskin toimittajan määritelmän kaikkiin yksityisiin asianosaisiin, jotka ovat riskialttiiksi lainsäädännöltään ja siihen liittyviltä käytännöiltään nimettyjen kolmansien maiden yritysten ja kansalaisten määräysvallassa. Poliittis-oikeudellisen yleisen tason riskimäärittely kattaisi siten yrityksiä, joiden tekninen, operatiivinen ja kyberturvallisuuden kokonaisuuden hallinnan kannalta määritelty riskiprofiili ei olisi tavanomaista riskitasoa korkeampi. Tällainen kriteeristö herättää perusteltua kritiikkiä sääntelyn kohdentumisen täsmällisyydestä ja riskiperusteisuudesta sekä erityisesti sen oikeasuhtaisuudesta.

[51] Ks. perustuslakivaliokunnan lausunnot PeVL 62/2022 vp ja PeVL 30/2022 vp EU:n säädösehdotuksista. Molemmissa tapauksissa EU:n säädösehdotusta muutettiin merkittävästi neuvoston valmisteluvaiheessa.
[52] PeVL 62/2022 vp, joka koskee ehdotusta EU:n asetukseksi luonnon ennallistamisesta.

3. *CSA2 100 artiklan tarkoittaman korkean riskin toimittajan määrittelyn kriteerien perustuminen mahdollisesti muuhun kuin näyttöön:*

   CSA2 sallii nimeämisen käynnistämisen ”muiden lähteiden” perusteella, mukaan lukien unionin tai jäsenvaltioiden julkisten lausuntojen pohjalta. Tämä lisää riskiä siitä, että päätökset eivät ole johdonmukaisesti tietoon ja näyttöön perustuvia, vaan ne voivat viime kädessä perustua poliittiseen harkintaan. Samoin kuin omaisuudensuojan osalta, kaikkien elinkeinon harjoittamisen vapauden rajoitusten on perustuttava laissa tarkkarajaisesti ja täsmällisesti määriteltyihin säännöksiin. Niiden on oltava välttämättömiä yleisen edun mukaisen ja painavan yhteiskunnallisen tavoitteen saavuttamiseksi, eivätkä ne saa koskea oikeuden ydinsisältöä. Niiden on ennen kaikkea oltava kokonaisuutena arvioiden oikeasuhtaisia. Arvioinnissa on punnittava yhtäältä tavoiteltuja yhteiskunnallisia päämääriä ja toisaalta elinkeinotoimintaan kohdistuvan rajoituksen laajuutta ja ankaruutta.

5.2.1.3 Perustuslain 21 §: Hyvä hallinto ja oikeussuoja

150. Suomen perustuslain 21 § takaa jokaiselle oikeuden saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä toimivaltaisessa tuomioistuimessa tai viranomaisessa sekä saada oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman elimen tarkasteltavaksi. Perustuslaki sisältää lisäksi säännökset julkisuudesta, oikeudesta tulla kuulluksi ja saada perusteltu päätös, muutoksenhakuoikeudesta ja muista hyvän hallinnon takeista.

151. Perustuslain 21 § säätää siten oikeuden hyvään hallintoon ja oikeussuojaan sekä edellyttää, että oikeussuoja ja hyvän hallinnon takeet on suojattava tarkemmin lailla.

152. Perustuslain 21 § liittyy suoraan CSA2-asetuksen täytäntöönpanoon Suomessa. Ehdotetun asetuksen täytäntöönpano jäsenvaltiossa edellyttäisi välttämättä Suomen viranomaisten hallinnollista päätöksentekoa, hallinnollisia sanktioita sekä myös lainkäyttöpäätöksiä.

153. CSA2:n aiheuttamat perustuslailliset ongelmakohdat hyvän hallinnon näkökulmasta sisältävät tiivistetysti ainakin seuraavat:

   1. *Asiakirjajulkisuus:*

      Korkean riskin toimittajien luettelointi perustuisi todennäköisesti ainakin osittain salaisiin turvallisuusasiakirjoihin. Ilman riittävää tietojen julkistamista sekä asianosaisjulkisuutta oikeus tulla kuulluksi voi muuttua pelkäksi muodollisuudeksi, mikä on suorassa ristiriidassa perustuslain 21 §:n vaatimusten kanssa.

   2. *Selvitysvelvollisuuden ja näyttötaakan siirtyminen:*

      CSA2 antaa komissiolle mahdollisuuden päätellä omistuksen ja määräysvallan yhteyksiä, jos tutkinnan kohteena oleva toimittaja ei toimita tietoja määräajassa. Suomen perustuslain kannalta tämä on ongelmallista, ellei asianomaiselle osapuolelle ole annettu todellista mahdollisuutta vastata tietopyyntöön. Perustuslain hyvän

hallinnon vaatimukset asettavat rajoitukset sille, kuinka laajasti selvittämisvelvollisuus ja todistustaakka voidaan siirtää viranomaiselta asianosaiselle.

3. *Moniportainen vastuu:*

EU:n tason täytäntöönpanosäädöksissä voitaisiin määrittää toimittajan asema, kun taas Suomen viranomaiset soveltaisivat rajoittavia seuraamuksia. Tämä luo riskin siitä, että kansalliset viranomaiset pitävät EU:n luokitusta tosiasiallisesti sitovana eivätkä arvioi sitä itsenäisesti, mikä voi heikentää käytännön oikeussuojaa.

5.2.2 Perusoikeuksien rajoitukset

154. Perusoikeuksia voidaan Suomen perustuslain ja sen vakiintuneeseen tulkintakäytäntöön perustuvien perusoikeuksien yleisten rajoitusperusteiden mukaan rajoittaa vain, jos rajoitus (i) perustuu lakiin; (ii) on täsmällinen ja tarkkarajainen siten, että rajoituksen olennainen sisältö ilmenee laista; (iii) palvelee hyväksyttävää tarkoitusta; (iv) ei ulotu perusoikeuden ydinsisältöön; (v) on painavan yhteiskunnallisen tarpeen saavuttamiseksi välttämätön ja oikeasuhtainen; (vi) sisältää riittävät oikeusturvajärjestelyt; ja (vii) ei ole ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa.[53]

155. Nämä vaatimukset perustuvat erityisesti perustuslain 2 §:ssä säädettyyn oikeusvaltioperiaatteeseen sekä julkiselle vallalle kuuluvaan velvollisuuteen turvata perusoikeuksien toteutuminen, josta säädetään nimenomaisesti perustuslain 22 §:ssä. Perustuslain vakiintuneen tulkintakäytännön mukaan perustuslain 2 §:n 3 momentin oikeusvaltioperiaatteeseen sisältyy vaatimus lain täsmällisyydestä ja tarkkarajaisuudesta, ja erityisesti perusoikeuksia koskevan lainsäädännön on oltava riittävän selkeää.[54]

156. Kyberturvallisuus ja kriittisen infrastruktuurin suoja ovat sinänsä lähtökohtaisesti hyväksyttäviä ja perustuslain tarkoittamalla tavalla painavia tavoitteita. Kansallinen ja yleinen turvallisuus voivat oikeuttaa tiettyjä perusoikeuksien rajoituksia. Arvioinnin keskeiset kysymykset koskevat siten rajoitusten täsmällisyyttä ja tarkkarajaisuutta, ennakoitavuutta ja oikeasuhtaisuutta sekä sitä, muodostuvatko omaisuuden käyttörajoitukset niin mittaviksi, että ne vaikutuksiltaan rinnastuvat pakkolunastukseen, samoin kuin oikeusturvajärjestelyiden riittävyyttä.

157. Perusoikeuksien rajoittamista täsmällisellä ja tarkkarajaisella lain säännöksellä koskevan edellytyksen osalta CSA2 tulisi Suomessa sovellettavaksi EU-asetuksena ja olisi siten muodollisesti lakitasoinen säädös. Perusoikeusrajoitusten edellytysten on kuitenkin ilmettävä EU-sääntelystä riittävän täsmällisesti ja tarkkarajaisesti. CSA2:ssa keskeiset rajoittavat vaikutukset konkretisoituisivat vasta myöhemmissä täytäntöönpanosäädöksissä ja kansallisissa toimenpiteissä. Rajoituksen ratkaiseva sisältö, kuten soveltamisala, kohde ja

[53] PeVL 25/1994 vp, s. 4–5, ennustettavuuden ja ymmärrettävyyden vaatimuksesta.

[54] PeVL 32/2020 vp, s. 2 sekä PeVL 10/2016 vp, s. 2 sekä PeVL 45/2016 vp, s. 3, PeVL 41/2006 vp, s. 4/II.

kiellon laajuus, ei näin ollen ilmene suoraan asetustasolta, mikä on ongelmallista omaisuudensuojaan ja elinkeinovapauteen kohdistuvien rajoitusten näkökulmasta.

158. Lakiperusteisuuden ja ennakoitavuuden kannalta perustuslain vaatimus edellyttää, että rajoitukset ovat tarkkarajaisia ja estävät mielivaltaisen puuttumisen. CSA2:n mekanismi kolmannen maan nimeämiseksi mahdollistaa päätöksenteon myös ”muiden lähteiden”, kuten unionin tai jäsenvaltion julkisten lausumien, perusteella. Tällainen avoin viittaus ei muodosta selkeää, objektiivisesti todennettavaa kriteeristöä. Lisäksi korkean riskin toimittajan määritelmä perustuisi laajasti omistus- ja määräysvaltasuhteisiin. Kriteerien soveltaminen monimutkaisissa konsernirakenteissa olisi tulkinnanvaraista. Sääntely ei siten anna markkinatoimijoille riittävän varmaa perustaa ennakoida, milloin heitä voitaisiin pitää korkean riskin toimittajina.

159. Suhteellisuusvaatimuksen mukaan rajoituksen on oltava välttämätön tavoitteen saavuttamiseksi, eikä se saa ylittää sitä, mikä on tarpeen. CSA2 mahdollistaa markkinoilta sulkemisen ja ICT-komponenttien pakollisen poistamisen, mukaan lukien matkaviestinverkkoja koskevan velvoitteen, jonka mukaan siirtymäaika ei saisi ylittää 36 kuukautta. Ehdotuksessa ei osoiteta riittävästi, miksi vähemmän rajoittavat keinot, kuten tekniset ja organisatoriset toimenpiteet, kohdennettu valvonta, segmentointi tai yksilöllinen riskinarviointi, olisivat riittämättömiä. Suomen perustuslaillisessa arvioinnissa näin laaja ja ankara rajoitus ilman selkeää näyttöä välttämättömyydestä on selkeästi ongelmallinen.

160. Menettelyllisten takeiden osalta perustuslain 21 § edellyttää oikeutta tulla kuulluksi, saada perusteltu päätös ja hakea muutosta. CSA2:n nimeämis- ja luettelointimenettelyt voivat johtaa tosiasialliseen markkinoilta sulkemiseen, mutta menettelylliset takeet eivät vaikuta olevan oikeassa suhteessa toimenpiteiden vakavuuteen. Päätökset voivat perustua luottamukselliseen aineistoon, jota ei voida täysimääräisesti julkistaa, mikä rajoittaa puolustautumismahdollisuuksia käytännössä. Lisäksi komissiolla on mahdollisuus tehdä epäedullisia päätelmiä, jos toimittaja ei toimita pyydettyjä tietoja määräajassa. Perustuslain 21 §:n näkökulmasta tällainen mekanismi voi muodostua tosiasialliseksi seuraamukseksi ilman mahdollisuutta kiistää väitteiden perusteet.

161. Sääntelyn seuraukset eivät myöskään rajoittuisi pelkästään laitetoimittajaan. Myös laitteen omistaja tai käyttäjä voisi joutua poistamaan tai korvaamaan jo hankittuja laitteita toimittajaan kohdistuvien toimenpiteiden vuoksi. Asiakkaisiin kohdistuva kielto käyttää omaisuutta on erityisen ankara toimenpide, etenkin kun asiakkailla ei ole määräysvaltaa toimittajan toimintaan. Tämä korostaa sääntelyyn liittyviä suhteellisuus- ja oikeudenmukaisuusongelmia.

162. CSA2:n rakenne, jossa unionitason täytäntöönpanosäädökset yhdistyvät kansalliseen täytäntöönpanoon, voi lisäksi heikentää oikeussuojan käytännön tehokkuutta. Jos ratkaiseva luokittelu tehdään unionitasolla mutta konkreettiset vaikutukset toteutuvat kansallisesti, oikeussuojan tehokkuus riippuu siitä, missä määrin tuomioistuimet voivat tutkia unionitason päätösten perusteet ja onko väliaikaista oikeussuojaa tosiasiallisesti saatavilla.

163. CSA2 ei tältä osin anna selkeää varmuutta tehokkaan oikeussuojan toteutumisesta.

5.3 HALLINTO-OIKEUDELLISET NÄKÖKOHDAT

164. Perusoikeuskysymysten lisäksi CSA2 voi aiheuttaa jännitteitä Suomen hallinto-oikeuden keskeisten periaatteiden kanssa, erityisesti oikeusvarmuuden, suhteellisuuden, yhdenvertaisuuden ja avoimuuden näkökulmasta. Jännitteet liittyvät EU-tason nimeämis- ja luettelointipäätöksiin, laajaan harkintavaltaan muiden kuin teknisten toimitusketjuriskien määrittelyssä sekä kansallisen täytäntöönpanon kautta toteutettaviin, mahdollisesti ankariin seurauksiin johtaviin toimenpiteisiin.

165. Oikeusvarmuus ja oikeutettujen odotusten suoja ovat suomalaisen hallinto-oikeuden keskeisiä periaatteita. Yksityisten toimijoiden on voitava ennakoida oikeudelliset seuraukset. Tämä korostuu erityisesti pääomaintensiivisissä ja pitkäaikaisissa infrastruktuuri-investoinneissa. CSA2:n mukaan komissio voisi tunnistaa keskeiset ICT-resurssit ja asettaa kieltoja sekä poistamisvaatimuksia täytäntöönpanosäädöksillä, joita tarkistetaan vähintään 36 kuukauden välein. Tällainen järjestelmä altistaa investoinnit myöhemmille unionitason päätöksille ja heikentää ennakoitavuutta, mikä on omiaan kaventamaan oikeutettujen odotusten suojaa.

166. Suhteellisuus on toinen hallinto-oikeuden keskeinen periaate. Viranomaistoimenpiteiden on oltava tarkoituksenmukaisia, välttämättömiä ja oikeasuhtaisia suhteessa tavoiteltuun päämäärään. CSA2 mahdollistaa kiellot käyttää, asentaa tai integroida ns. korkean riskin toimittajien ICT-komponentteja. Jos kansalliset viranomaiset soveltavat näitä rajoituksia kaavamaisesti erityisesti jo käyttöön otettuihin laitteisiin, tapauskohtainen suhteellisuusarviointi voi tosiasiallisesti jäädä syrjään. Tämä korostuu matkaviestinverkkojen osalta, joissa pakollinen siirtymäaika ei saisi ylittää 36 kuukautta. Lyhyt määräaika voi käytännössä tehdä velvoitteiden täyttämisestä teknisesti mahdotonta tai kohtuuttoman raskasta, ja siten muuttaa jopa sinänsä hyväksyttävän tavoitteen suhteettomaksi toimenpiteeksi.

167. Yhdenvertaisuusperiaate edellyttää, että vertailukelpoisia tapauksia kohdellaan samalla tavoin eikä mielivaltaista erottelua tehdä. CSA2:n korkean riskin toimittajakriteerit perustuvat osin sijoittautumiseen ja määräysvaltasuhteisiin nimettyihin kolmansiin maihin. Tämä voi johtaa erilaiseen kohteluun yritysrakenteen tai kansallisuusyhteyksien perusteella, vaikka tekninen riskiprofiili olisi tosiasiallisesti samankaltainen.

168. Suomen hallinto-oikeudessa korostuvat avoimuus, läpinäkyvyys ja päätösten huolellinen perusteleminen. Mikäli CSA2:n mukaiset EU-tason päätökset perustuvat luottamuksellisiin turvallisuusarviointeihin, kansalliset viranomaiset voivat joutua panemaan ne täytäntöön ilman, että niiden taustalla olevia perusteita voidaan esittää asianosaisille. Tällöin syntyy selkeä riski siitä, että kansalliset ratkaisut rakentuvat pelkästään viittaukselle EU-luokitukseen ilman itsenäistä, konkreettista ja läpinäkyvää perustelua.

5.4 KORVAUSJÄRJESTELMÄ

169. CSA2 ei sisällä korvausmekanismia niille operaattoreille tai muille toimijoille, joille aiheutuu kustannuksia komission määräämistä ICT-toimitusketjua koskevista rajoittavista toimenpiteistä. Samanaikaisesti CSA2:n 110 artiklassa kuitenkin säädetään velvoitteesta poistaa asteittain 104 artiklassa tarkoitettujen korkean riskin toimittajien ICT-komponentit.

170. Kuten edellä tässä arviossa on todettu, CSA2-ehdotuksen vaikutukset voivat tästä huolimatta olla taloudellisesti erittäin huomattavia. Komission vaikutusarviossa esitetään määrällisiä kustannusarvioita, joiden mukaan tiettyjen korkean riskin laitteiden poistaminen voisi aiheuttaa matkapuhelinoperaattoreille 3,4–4,3 miljardin euron vuotuiset kustannukset viiden vuoden ajan. Samalla investoinnit niin sanottuihin luotettaviin toimittajiin voisivat kasvaa jopa 2 miljardiin euroon vuodessa. Ehdotuksessa viitataan lisäksi ENISA:n maksujärjestelmiin liittyvään kolmen ensimmäisen vuoden siirtymäkauteen, jonka aikana kustannuksia katettaisiin unionin talousarviosta ja myöhemmin maksuilla. Tämä järjestely ei kuitenkaan muodosta yleistä ja oikeudellisesti turvattua korvausoikeutta niille toimijoille, jotka joutuvat poistamaan tai korvaamaan jo hankittuja laitteita.

171. CSA2:ssa todetaan, että komission on siirtymäaikoja määritellessään otettava huomioon taloudelliset vaikutukset. Kyse on täytäntöönpanon ajoituksesta, ei subjektiivisesta oikeudesta korvaukseen. Tämä tarkoittaa käytännössä sitä, että vaikka komissio voi ottaa yrityksille aiheutuvat kustannukset huomioon siirtymäaikoja määritellessään, yrityksille ei synny oikeutta saada korvausta aiheutuneista kustannuksista.

172. Suomen kansallisessa sääntelyssä ratkaisu on toisenlainen. Sähköisen viestinnän palveluista annetun lain 244 a §:n 1 momentin mukaan viestintäverkkolaitteen käyttö voidaan kieltää, jos on vakavia perusteita epäillä sen vaarantavan kansallista turvallisuutta tai puolustusta. Pykälän 3 momentissa säädetään mahdollisuudesta määrätä laite poistettavaksi. Näihin toimenpiteisiin liittyy nimenomainen korvaussäännös SVPL:n 301 a §:ssä, jonka mukaan viestintäverkon omistajalla tai muulla haltijalla on oikeus saada valtion varoista täysi korvaus laitteista, joiden käyttö on kielletty 244 a §:n 1 momentin nojalla tai jotka on määrätty poistettaviksi 244 a §:n 3 momentin nojalla.

173. SVPL:n 301 a § ei kuitenkaan sovellu tilanteisiin, joissa laitteiden poistaminen perustuisi unionin oikeuteen tai komission CSA2:n nojalla antamiin täytäntöönpanosäädöksiin. Jos laitteiden käytöstä poistaminen tapahtuisi CSA2:n perusteella, kansallista täyden korvauksen mekanismia ei voitaisi soveltaa.

174. Teoriassa vahinkoa kärsinyt toimija voisi hakea korvausta unionilta SEUT 340 artiklan 2 kohdan nojalla unionin sopimuksenulkoisen vastuun perusteella. Lisäksi jäsenvaltio voisi tietyin edellytyksin olla vastuussa EU-oikeuden rikkomisesta. Molemmat keinot edellyttäisivät kuitenkin riittävän vakavaa oikeudenrikkomista sekä välitöntä syy-yhteyttä vahinkoon. Jos CSA2:n mukainen toimenpide olisi sinänsä lainmukainen, pelkkä merkittävä taloudellinen menetys ei lähtökohtaisesti oikeuttaisi yksityistä asianosaista korvaukseen.

175. Edellä tässä arviossa on todettu, että Suomen perustuslain 15 § turvaa omaisuuden suojan ja edellyttää pakkolunastustilanteissa täyttä korvausta. CSA2-tyyppiset käyttökiellot ja poistovelvoitteet sekä niiden vaikutukset hyvin todennäköisesti rinnastuisivat tosiasiallisesti pakkolunastukseen. Ne merkitsisivät omaisuuden käytön olennaista ja pysyvää rajoittamista ja johtaisivat investointien arvon merkittävään alenemiseen tai menettämiseen. Tällaisessa tilanteessa perustuslain 15 §:llä olisi merkitystä vähintäänkin rajoituksen suhteellisuuden arvioinnissa. Jos toimenpiteen vaikutukset rinnastuisivat tosiasiallisesti pakkolunastukseen, säännös voisi tulla sovellettavaksi myös täyden korvauksen vaatimuksen perusteella.

176. Kolmansien maiden toimittajat voisivat vedota myös sovellettaviin kahdenvälisiin investointisopimuksiin ja saattaa asian sijoittajan ja valtion väliseen kansainväliseen riidanratkaisumenettelyyn. Tämä ratkaisu voisi tulla kyseeseen, jos jäsenvaltion toteuttamien rajoittavien toimenpiteiden katsottaisiin rikkovan investointisopimuksessa turvattuja velvoitteita, kuten oikeudenmukaisen ja tasapuolisen kohtelun vaatimusta tai pakkolunastusta koskevaa kieltoa.

177. Kokonaisuutena arvioituna CSA2:n sääntelyrakenne merkitsee korvausjärjestelmän osalta sitä, että unionitasolla tehtävät nimeämis- ja poistamispäätökset voivat aiheuttaa yksittäisille toimijoille huomattavia ja kohdennettuja taloudellisia menetyksiä ilman unionitason korvausmekanismia ja ilman, että Suomen SVPL:n 301 a §:n mukainen kansallinen täyden korvauksen järjestelmä on sovellettavissa.

178. Jos käyttökiellot ja poistovelvoitteet rinnastuvat vaikutuksiltaan perustuslain 15 §:ssä tarkoitettuun pakkolunastukseen – mikä on tässä omaisuuden käyttörajoituksen laajuuden ja syvyyden johdosta perusteltu tulkinta – pitäisi perustuslain mukaan omaisuuden omistajalle maksaa täysi korvaus edellytyksenä käyttörajoitukselle. Kun käyttörajoituksesta säädettäisiin unionin säädöksessä, joka saa etusijaa Suomen oikeuteen nähden, syntyy epäselvä tilanne korvausvelvollisuuden osalta. Jos Suomen valtio täytäntöönpanovaltaa käyttäessään myötävaikuttaa perustuslain 15 §:n vastaiseen omaisuudensuojan pakkolunastusta vastaavaan käytön estämiseen, voi Suomen valtiolle syntyä velvollisuus suorittaa täysi korvaus.

179. EU:n säädöksen valmisteluvaiheessa valtioneuvostolla on velvollisuus pyrkiä huolehtimaan siitä, että unionin säädökseen tulisi Suomen perustuslain ja EU:n perusoikeuskirjan sekä Euroopan ihmisoikeussopimuksen 1 lisäpöytäkirjan vaatimukset täyttävä korvausjärjestelmä. Lisäksi jäsenvaltio voi joutua vahingonkorvausvastuuseen, jos täytäntöönpano ei täytä perusoikeuksien rajoitusedellytyksiä tai jos kansallinen viranomainen ylittää sille osoitetun harkintavallan. Kolmansien maiden toimittajat voivat myös vaatia valtiolta korvauksia investointisopimusten nojalla.

180. CSA2:n toimeenpanoon voi siksi liittyä merkittävä ja monikanavainen valtiontaloudellinen vastuuriski, vaikka sääntelyn keskeinen sisältö määräytyy unionitasolla.

6 Johtopäätökset

181. CSA2 ei olisi luonteeltaan vain ENISA:n toimivallan ja sertifiointikehyksen tekninen päivitys, vaan se loisi unionitasoisen pakottavan mekanismin, jolla komissio voisi sulkea toimittajia pois EU:n viestintäverkoista ja muusta NIS2:n soveltamisalaan kuuluvasta digitaalisesta infrastruktuurista. Sääntelyn käytännön vaikutus kohdistuisi siten muun ohella suoraan Euroopan viestintäinfrastruktuurin tekniseen kokoonpanoon, investointisykleihin ja markkinarakenteeseen.

182. CSA2-ehdotuksessa ei osoiteta, että standardoituihin verkon osiin liittyisi nykyisellään sellaisia konkreettisia ja rajat ylittäviä sisämarkkinaongelmia, jotka edellyttäisivät unionitasoista keskitettyä, toimittajakohtaisiin riskiluokituksiin perustuvaa puuttumismekanismia. Ehdotuksessa ei yksilöidä markkinoiden toimintahäiriöitä, sääntelyn pirstoutumisesta aiheutuvia esteitä tai teknisiä yhteentoimivuusongelmia, joita ei voitaisi ratkaista vähemmän keskitetysti yhdenmukaistamalla aineellisia kriteerejä ja vahvistamalla jäsenvaltioiden koordinaatiota. Näin ollen komissiolta jää osoittamatta, että markkinoilta sulkevia oikeusvaikutuksia tuottava sääntelymalli olisi välttämätön sisämarkkinoiden toiminnan turvaamiseksi.

183. CSA2:n konkreettinen seuraus Euroopan viestintäinfrastruktuurille olisi laajamittainen rip-and-replace-riskitilanne: unionitasoinen riskiluokitus ja toimittajien luettelointi voisivat velvoittaa teleoperaattorit ja muut toimijat korvaamaan jo käyttöönotettua laitekantaa määräajassa, joka matkaviestinverkkojen osalta voisi olla enintään 36 kuukautta. Tämä johtaisi ennenaikaisiin poistoihin ja investointitappioihin, kasvattaisi rahoitus- ja hankintariskejä sekä sitoisi pääomaa verkkojen kehittämisen sijasta laitteiden pakkovaihtoon.

184. Seurauksena olisi väistämättä paitsi viive Euroopan 5G-verkkojen laajentamisessa ja 6G-investointien käynnistymisessä, myös merkittävä verkkojen integraatio- ja häiriöriskien kasvu. Vastaavasti hyöty kyberturvallisuuden osalta jää rajalliseksi. EU:n 5G-verkkolaitemarkkina on jo lähtökohtaisesti erittäin keskittynyt. Jos yksi kolmesta keskeisestä ja innovointikykyisestä ICT-laitetoimittajasta suljettaisiin pois unionin markkinoilta, markkina kaventuisi käytännössä kahden toimijan varaan.

185. EU-oikeudellisesti CSA2-ehdotuksen ensimmäinen keskeisistä ongelmista liittyy sen oikeusperustaan. CSA2:n IV-luvun mekanismi keskittäisi kolmansia maita koskevan nimeämisen ja toimittajien luetteloinnin komissiolle ja tuottaisi välittömiä, markkinoilta sulkevia oikeusvaikutuksia. Järjestelmä perustettaisiin SEUT 114 artiklaan, vaikka ehdotuksessa ei yksilöidä konkreettisia sisämarkkinaesteitä, joita ei voitaisi ratkaista yhdenmukaistamalla aineellisia kriteerejä ja jättämällä riskinarviointi koordinoidusti jäsenvaltioille. Tämä luo perustellun riskin siitä, että sääntely venyttää SEUT 114 artiklan soveltamisalaa sisämarkkinoiden harmonisoinnin ulkopuolelle.

186. Viestintäverkoissa on kyse globaalisti standardoidusta, yhteentoimivasta ja ristiinkäytettävästä teknologiasta, jonka tekniset rajapinnat ja turvallisuusvaatimukset perustuvat kansainvälisiin standardeihin. Mobiiliverkkojen laitteet, kuten tukiasemat, ovat

fyysisiä infrastruktuurikomponentteja, jotka sijaitsevat jäsenvaltion alueella ja palvelevat ensisijaisesti kansallista verkkoa. Niillä ei siksi lähtökohtaisesti ole sellaisia välittömiä rajat ylittäviä vaikutuksia, jotka itsessään muodostaisivat sisämarkkinaesteen. Tästä näkökulmasta unionitason kategorinen toimittajaluokitus, joka puuttuu kansallisten verkkojen tekniseen kokoonpanoon, edellyttäisi erityisen painavaa ja täsmällisesti osoitettua sisämarkkinaperustetta.

187. CSA2-ehdotuksen oikeudellisesti suurin ongelma liittyy perusoikeusrajoitusten oikeasuhtaisuuteen. EU-oikeuden toissijaisuus- ja suhteellisuusperiaatteiden kannalta ehdotuksen perusratkaisu olisi poikkeuksellisen ankara. Unionitasoinen kategorinen riskiluokitus mahdollistaisi kiellot ja poistovelvoitteet riippumatta yksittäisten tuotteiden teknisestä riskiprofiilista, eikä ehdotuksessa osoiteta riittävästi, miksi vähemmän rajoittavat keinot – kuten tekniset ja organisatoriset lieventämistoimet, segmentointi, kohdennettu valvonta tai tapauskohtainen riskinarviointi – eivät riittäisi. Lisäksi sääntely ulottuisi laajalle kriittisyyden käsitteen laajentamisen kautta, vaikka verkkoarkkitehtuurin kannalta kaikkien osien riskiprofiili ei ole sama. Tämä heikentää sekä sääntelyn suhteellisuutta että sen sisäistä johdonmukaisuutta.

188. EU:n perusoikeuskirjan näkökulmasta CSA2:n keskeiset ongelmat liittyvät elinkeinovapauden (16 artikla) ja omaisuudensuojan (17 artikla) merkittävään rajoittamiseen sekä hyvän hallinnon ja tehokkaan oikeussuojan vaatimuksiin (41 ja 47 artiklat). Ehdotuksen menettelysäännökset voisivat käytännössä rajoittaa yksityisen asianosaisen mahdollisuutta puolustautua tehokkaasti. Jos EU-tason päätös perustuisi sellaiseen luottamukselliseen aineistoon, jota asianosainen ei saisi riittävästi tietoonsa, tämän olisi vaikea arvioida ja kiistää häneen kohdistettuja väitteitä. Samoin mahdollisuus tehdä toimittajalle epäedullisia johtopäätöksiä pelkästään sillä perusteella, että tämä ei toimittaisi pyydettyjä tietoja määräajassa, voisi käytännössä heikentää puolustautumisoikeutta. Menettelyllisten oikeuksien tulisi olla täsmällisesti säädettyjä ja tosiasiallisesti tehokkaita.

189. Suomen perustuslain kannalta CSA2:n ongelmakohdat tiivistyisivät kolmeen kokonaisuuteen. Omaisuudensuojan (perustuslain 15 §) näkökulmasta käyttökiellot ja poistovelvoitteet rinnastuvat vaikutuksiltaan pakkolunastukseen erityisesti silloin, kun laitteisto jouduttaisiin poistamaan kesken sen taloudellisen käyttöiän ja kustannukset kohdistuisivat keskittyneesti yksittäisiin toimijoihin. Elinkeinovapauden (perustuslain 18 §) näkökulmasta korkean riskin luetteloon päätyminen merkitsisi tosiasiallista markkinoilta sulkemista, jonka hyväksyttävyys edellyttäisi täsmällistä, ennakoitavaa ja välttämättömyydeltään perusteltua sääntelyä. Hyvän hallinnon ja oikeussuojan (perustuslain 21 §) näkökulmasta moniportainen malli – unionitasoinen luokitus ja kansallinen täytäntöönpano – sisältäisi konkreettisen riskin siitä, että kansallinen päätöksenteko jäisi käytännössä EU-luokitukseen nojaavaksi täytäntöönpanoksi ilman itsenäistä harkintaa ja perusteluja.

190. Korvausjärjestelmän osalta CSA2 loisi rakenteen, jossa unionitasolla tehtäisiin markkinoilta sulkevia riskiluokituksia, mutta unionitasoista korvausmekanismia ei säädettäisi. Samalla Suomen SVPL 301 a §:n mukainen täyden korvauksen järjestelmä ei soveltuisi unionin

oikeuteen perustuvaan poistovelvoitteeseen. Valtiontaloudellinen vastuuriski kasvaisi myös kansallisella tasolla.

191. Näissä olosuhteissa Suomen edustajilta edellytetään CSA2:n käsittelyssä EU:ssa selkeää ja johdonmukaista neuvottelulinjaa, jonka tavoitteena olisi poistaa tai vähintään olennaisesti lieventää tässä arviossa yksilöidyt EU-oikeudelliset ja valtiosääntöiset ongelmakohdat.

192. Tämä merkitsisi vähintään seuraavia vaatimuksia: (i) CSA2-ehdotuksen IV-luvun mekanismin oikeusperustan asianmukaisuuden perusteellinen arviointi ja tarvittaessa sääntelyrakenteen muuttaminen; (ii) kriittisten ICT-resurssien täsmällinen ja teknisesti perusteltu rajaus siten, että velvoitteet kohdistuisivat vain aidosti verkon ohjaus- ja hallintatoimintoihin; (iii) välttämättömyys- ja suhteellisuusnäytön vahvistaminen sekä vähemmän rajoittavien vaihtoehtojen ensisijaisuus; (iv) siirtymäaikojen asettaminen teknisesti ja markkinarakenteellisesti realistiselle tasolle; (v) menettelytakeiden merkittävä vahvistaminen; sekä (vi) oikeudellisesti turvatun korvausmekanismin sisällyttäminen sääntelyyn tai muu ratkaisu, joka estäisi poikkeuksellisen suurten ja keskittyneiden kustannusten siirtymisen jäsenvaltioille ja yksityisille toimijoille ilman kompensaatiota.

193. Kokonaisuutena arvioiden CSA2 voitaisiin hyväksyä Suomen näkökulmasta vain, jos sitä muutettaisiin olennaisesti siten, että se olisi aidosti riskiperusteinen, teknisesti rajattu, perusoikeuksien ja oikeussuojan kannalta kestävä sekä taloudellisten vaikutusten osalta suhteellinen.

194. Muutoin sääntely luo merkittäviä riskejä Euroopan viestintäinfrastruktuurin kehitykselle, EU:n 6G-kyvykkyydelle sekä unionin ja Suomen perustuslailliselle järjestykselle.