U 71/2020 vp

Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi kriittisten toimijoiden häiriönsietokyvystä

Perustuslain 96 §:n 2 momentin mukaisesti lähetetään eduskunnalle Euroopan komission ehdotus Euroopan parlamentin ja neuvoston direktiiviksi kriittisten toimijoiden häiriönsietokyvystä (COM (2020) 829 final).

Helsingissä 28 päivänä tammikuuta 2021

Sisäministeri Maria Ohisalo

Neuvotteleva virkamies Eero Kytömaa

SISÄMINISTERIÖ MUISTIO 21.1.2021 EU/2020/1795

EUROOPAN KOMISSION EHDOTUS EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI KRIITTISTEN TOIMIJOIDEN HÄIRIÖNSIETOKYVYSTÄ

1 Tausta

Komissio julkaisi 16.12.2020 ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi kriittisten toimijoiden häiriönsietokyvystä (COM (2020) 829 final). Ehdotus on osin uutta sääntelyä unionin tasolla. Direktiiviluonnoksen kantavina teemoina ovat ymmärrys uhka- ja häiriöspektrin laajuudesta ja sen tuottama tarve siirtyä fyysisistä suojaustoimista yhteiskunnan häiriöttömän toiminnan varmistamiseen, eli kriisinkestävyyteen. Tässä valtioneuvoston kirjelmässä viitataan direktiiviehdotukseen lyhenteellä CER-direktiivi (Critical Entities Resilience Directive).

Komission mukaan CER-direktiivin päätarkoituksena on sisämarkkinoiden toiminnan takaaminen kriittisten palvelujen osalta direktiivin soveltamisalalla. Ehdotuksen tarkoituksena on parantaa Euroopan unionin (EU) kannalta välttämättömien palvelujen häiriönsietokykyä sekä ylläpitää yhteiskunnan elintärkeitä ja taloudellisia toimintoja määrittäen tietyt kriittiset sektorit, jotka tarjoavat tällaisia palveluja.

EU on jo pitkään tunnistanut kriittisten infrastruktuurien suojaamisen merkityksen Euroopan toimintakyvylle. Esimerkiksi jo vuonna 2006 EU käynnisti eurooppalaisen toimintaohjelman kriittisten infrastruktuurien suojaamiseksi (EPCIP). Vuonna 2008 voimaan tuli neuvoston direktiivi Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä sekä niiden suojaamisen parantamistarpeen arvioimisesta (ECI direktiivi). Sitä sovelletaan vain tiettyihin energia- ja liikenneinfrastruktuureihin, joiden häiriötilanne vaikuttaa samanaikaisesti ja merkittävällä tavalla kahteen tai useampaan jäsenvaltioon. Johtuen direktiivin rajallisesta soveltamisalasta, ovat monet jäsenvaltiot toteuttaneet omia toimenpiteitään kriittisen infrastruktuurien suojaamisessa sen sijaan, että direktiivi olisi ohjannut suojaustoimenpiteiden kehittämistä.

Komission mukaan on ilmeistä, että elintärkeiden infrastruktuurien suojaamista koskevat nykyiset puitteet eivät ole yhteismitallisia, eivätkä riittäviä suojaamaan Euroopan kriittistä infrastruktuuria ja siihen kytkeytyviä palveluita. Ottaen huomioon infrastruktuurien ja palvelujen lisääntyvän keskinäisriippuvuuden ja merkittävyyden sisämarkkinoiden toimintakyvylle, päätti komissio uudistaa kriittisten infrastruktuurien suojaamista koskevan direktiivin.

Komissio korostaa, että toimintaympäristö, jossa kriittiset toimijat toimivat, on muuttunut merkittävästi. Ensinnäkin Euroopan kohtaamat riskit ja uhat ovat monimuotoisempia kuin vuonna 2008. Toiseksi kriittisten järjestelmien toimijat, kuten palveluoperaattorit kohtaavat haasteita uuden teknologian käytönoton myötä, jotka usein liittyvät järjestelmien haavoittuvuuksiin. Uusi teknologia myös avaa mahdollisuuksia valtiolähtöiselle vihamieliselle toiminnalle, joka pyrkii hyödyntämään verkottuneen infrastruktuurin haavoittuvuuksia. Kolmanneksi uusi teknologia lisää entisestään infrastruktuuri- ja palveluoperaattoreiden keskinäisriippuvuutta, mikä voi johtaa häiriötilanteiden nopeaan laajentumiseen yhdeltä sektorilta toiselle ja mahdollisesti aiheuttaa merkittäviä häiriötilanteita useissa jäsenvaltioissa tai unionin tasolla.

Komission mukaan kriittisten toimijoiden keskinäisriippuvuuteen liittyviä haasteita ei tähän mennessä ole riittävästi tunnistettu unionin lainsäädännössä. Tähän on komission mukaan useita syitä. Ensinnäkin infrastruktuuri -ja palveluoperaattorit eivät ole täysin tietoisia tai eivät ole riittävässä määrin varautuneet dynaamisen riskimaiseman vaikutuksiin omalla toimialallaan. Toiseksi kriisinsietokyvyn parantamiseen keskittyvät toimet eroavat merkittävästi jäsenvaltioiden ja toimialojen välillä. Kolmanneksi jäsenvaltioiden kesken ei ole riittävää yhteismitallista kriittisten toimijoiden arviointikehikkoa, joten valmiuksissa ja valvonnassa on merkittäviä poikkeamia jäsenvaltioiden kesken. Vaatimukset ja valtion tarjoama tuki toimijoille vaihtelee jäsenvaltioittain, mikä aiheuttaa esteitä rajat ylittävälle yhteistyölle. Näin ollen on mahdollista, että jopa yksittäisen infrastruktuuri- ja palveluoperaattorin riittämätön valmius häiriötilanteen hoitamiseksi voi aiheuttaa vakavan riskin sisämarkkinoiden toiminnalle.

Komissio toteaakin, että sisämarkkinoiden moitteettoman toiminnan vaarantamisen lisäksi rajat ylittävillä häiriöillä voi olla Euroopan tasolla merkittäviä kielteisiä vaikutuksia kansalaisille, yrityksille, hallituksille ja ympäristölle. Komissio korostaa, että yksittäisen sektorin häiriöt voivat vaikuttaa esimerkiksi eurooppalaisten kykyyn matkustaa ja työskennellä vapaasti sekä esimerkiksi pääsyyn välttämättömien julkisten palvelujen, kuten terveydenhuollon piiriin.

Komissio myös korostaa, että häiriötilanteet, kuten suuret sähkökatkokset ja vakavat liikenneonnettomuudet, voivat heikentää turvallisuuden tunnetta ja väestön luottamusta kriittisten infrastruktuuri- ja palvelujärjestelmien toimintakykyyn sekä viranomaisiin, jotka viime kädessä ovat vastuussa järjestelmien valvonnasta ja väestön toimintakyvyn turvaamisesta.

2 Tavoite ja pääasiallinen sisältö

CER-direktiiviehdotus on osa laajaa pakettia, johon kuuluu uusi kyberturvallisuusstrategia sekä verkko- ja tietoturvadirektiivin päivitys (ehdotus Euroopan parlamentin ja neuvoston direktiiviksi kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja direktiivin 2016/1148 kumoamisesta, NIS2). Ehdotus perustuu 24.7.2020 komission julkaisemaan uuteen turvallisuusunionistrategiaan vuosille 2020-2025, jossa peräänkuulutettiin kokonaisvaltaista nykyiset ja tulevaisuuden riskit sekä fyysisen ja digitaalisen infrastruktuurin keskinäisriippuvuudet huomioivaa lähestymistapaa. Nämä toimet tukevat myös EU:n terrorismin vastaisen ohjelman tavoitteita.

Direktiiviehdotuksen tarkoituksena on parantaa välttämättömien palvelujen tarjontaa sisämarkkinoilla keskittymällä toimiin, jotka sekä ylläpitävät että parantavat yhteiskuntien kannalta kriittisten toimijoiden häiriönsietokykyä. Toimet kattavat monia aloja, ja niillä pyritään puuttumaan nykyisiin ja tuleviin verkossa ja sen ulkopuolella esiintyviin riskeihin johdonmukaisella ja toisiaan täydentävällä tavalla.

Komission mukaan toimivat sisämarkkinat ovat riippuvaisia kriittisten toimijoiden tuottamista palveluista, joita tarvitaan yhteiskunnan ja taloudellisen toiminnan ylläpitämiseksi. Yhteiskunnan toimintakyvyn kannalta kriittisten toimijoiden on oltava kriisinkestäviä, toisin sanoen kyettävä vastustamaan, kestämään, sopeutumaan ja toipumaan niihin vaikuttavista häiriöistä, jotka voivat johtaa vakaviin, toimialojen välisiin tai jopa rajat ylittäviin häiriötilanteisiin.

Komission mukaan ehdotus on linjassa verkko- ja tietojärjestelmiä koskevan NIS 2 direktiiviehdotuksen kanssa, luoden johdonmukaisen ja läheisen synergian toimenpiteisiin, joilla tavoitellaan korkean yhteisen kyberturvallisuuden tason saavuttamista koko unionissa.

Lisäksi komissio korostaa, että CER-direktiiviehdotus heijastaa kansallista lähestymistapaa yhä useammassa jäsenmaassa, joiden valmiustoimissa korostetaan sektorien välistä ja rajat ylittävää

keskinäisriippuvuutta, ja joissa kriisinkestävyystoimet ovat vain yksi elementti riskien ehkäisyn ja vähentämisen, liiketoiminnan jatkuvuudenhallinnan ja elpymisen rinnalla.

Komissio korvaa CER-direktiivillä Euroopan kriittisen infrastruktuurin suojaamista koskevan ECI-direktiivin (2008/114EC), joka on komission mukaan vanhentunut, soveltamisalaltaan liian kapea eikä vastaa enää tämän päivän uhkia, joihin lukeutuvat luonnononnettomuuksien lisäksi muun muassa valtiollinen hybridivaikuttaminen, sisäpiiriuhat, terrorismi, pandemiat ja teollisuusonnettomuudet. CER-direktiivillä komissio tavoittelee koko uhkaspektrin kattamista ja digitaalisen ja fyysisen infrastruktuurin suojaamista yhtenä kokonaisuutena.

Direktiivillä tavoitellaan keinovalikoiman laajentamista pelkistä suojaustoimista elintärkeiden toimintojen jatkuvuudenhallintaa kehittäviin toimiin. Suojaustoimien ohella keskeisiksi toimiksi on nostettu mm. riskienhallinta ja toipumiskyky häiriöistä. Direktiiviluonnoksessa tunnistetaan fyysisen ja digitaalisen infrastruktuurin kytköksen lisäksi myös sekä sektorirajat ylittävät keskinäisriippuvuudet että jäsenvaltioiden rajat ylittävät keskinäisriippuvuudet.

Direktiiviehdotuksen soveltamisala koskee kymmentä sektoria, kattaen liikenteen, energian, pankit, finanssimarkkinat, terveyden, vesi- ja jätevesihuollon, digitaalisen infrastruktuurin, julkishallinnon ja avaruuden.

Ehdotuksessa sääntelyinstrumenttina säilyy direktiivi, mutta sen oikeusperustaksi komissio ehdottaa SEUT 114 artiklaa, joka koskee sisämarkkinoiden toteuttamiseen ja toimintaan liittyviä toimenpiteitä. Oikeusperustan muutoksen myötä siirrytään yksimielisestä päätöksenteosta määräenemmistöpäätöksentekoon. Sisällön osalta merkittävimmät muutokset koskevat soveltamisalaa, kriittisten toimijoiden identifiointia sekä jäsenmaille ja kriittisille toimijoille asetettavia velvoitteita.

Direktiiviehdotuksessa nykyinen jäsenvaltioiden asiantuntijoista muodostettu Critical Infrastructure Protection Point of Contact -ryhmä uudistetaan ja sen nimi muuttuu kriittisten toimijoiden häiriönsietokyvyn asiantuntijaryhmäksi (Critical Entities Resilience Group CERG). Ryhmän tehtävänä olisi avustaa komissiota direktiivin toimeenpanossa ja siihen sovellettaisiin komission horisontaalisten ryhmien toimintamallia (182/2011).

2.1 Vaikutukset jäsenmaille

Direktiiviehdotus edellyttää jäsenvaltioiden tunnistavan sektorikohtaiset elintärkeät toiminnot ja nimeävän niitä tarjoavat kriittiset toimijat yhteisten eurooppalaisten kriteerien ja kansallisen riskiarvion pohjalta.

Jäsenvaltioilta myös edellytetään kansallista strategiaa kriittisten toimijoiden häiriönsietokyvyn vahvistamiseksi. Strategiassa tulee muun muassa määritellä kansalliset tavoitteet ja prioriteetit huomioiden rajat ylittävät ja sektoreiden väliset riippuvuudet; toimeenpanoon osallistuvien roolit, tehtävät ja vastuut sekä koordinaatio CER- ja NIS-direktiivien alaisten vastuuviranomaisten välillä tiedonvaihdon ja valvonnan edistämiseksi.

Jäsenvaltioiden tunnistamilta kriittisiltä toimijoilta direktiivi edellyttää omien riskiarvioiden ja kriisinkestävyyssuunnitelmien laadintaa. Kriittisiä toimijoita koskettavat kriisinsietokykyvaatimukset liittyvät häiriöiden ehkäisyyn, infrastruktuurin fyysiseen suojaamiseen, riskin- ja kriisinhallintajärjestelyihin, jatkuvuudenhallintaan ja henkilöstön turvallisuusselvityksiin.

Direktiiviehdotuksessa erityistä valvontaa komissio esittää kohdennettavaksi strategisesti merkittäviin toimijoihin, joiden tuottamat palvelut koskettavat vähintään kolmasosaa jäsenmaista.

Komissio myös korostaa yhteistyötä kumppanimaiden kanssa, koska keskinäiset riippuvuudet eivät pääty EU:n ulkorajoille. Ehdotetussa direktiivissä säädetään mahdollisuudesta tällaiseen yhteistyöhön esimerkiksi EU:n alueella tehtävien riskianalyysien osalta.

2.2 Ehdotuksen johdonmukaisuus suhteessa unionin muuhun politiikkaan

Ehdotetulla direktiivillä on rajapintoja muiden alakohtaisten ja monialaisten Euroopan unionin tavoitteiden kanssa, joita on tehty muun muassa katastrofiriskien vähentämisestä ja ilmastonmuutokseen sopeutumisesta, pelastuspalvelusta, suorista ulkomaisista investoinneista, kyberturvallisuudesta ja rahoituspalveluja koskevasta säännöstöstä. Eurooppalainen yhteinen lainsäädäntökehys on komission mukaan perusteltu kriittisen infrastruktuurin toimijoiden välisten suhteiden ja keskinäisriippuvuuksien tunnistamiseksi, niiden rajat ylittävän luonteen vuoksi ja kriittisten palveluiden takaamiseksi.

Yleisellä ja koordinoidulla lähestymistavalla komissio pyrkii varmistamaan, että jäsenvaltioiden tunnistamat kriittiset toimijat pystyvät jatkamaan toimintaansa häiriötilanteessa. Koska kyseessä on horisontaalilainsäädäntö, mahdollinen sektorikohtainen lainsäädäntö pätee edelleen ja direktiiviehdotus täydentää sitä. Direktiiviehdotus esimerkiksi edellyttää kansallisten vaatimusten noudattamista (strategian ja riskiarvio laadinta), mutta mahdolliset päällekkäiset toimijakohtaiset vaatimukset tulevat sektorikohtaisesta sääntelystä. Komission mukaan lisääntyneet keskinäisriippuvuudet ja rajat ylittävät vaikutukset puoltavat lainsäädännön soveltamisalan laajentamista. Samalla komissio korostaa yhteensovittamisen tärkeyttä sektorikohtaisen lainsäädännön kanssa, jotta vältyttäisiin mahdollisilta päällekkäisyyksiltä.

Erityisesti ehdotuksessa on komission mukaan huomioitu synergiat samanaikaisesti esitellyn NIS 2 -direktiiviehdotuksen kanssa, jonka tavoitteena on vahvistaa sekä unionin että jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta asettamalla riskienhallintatoimia kyberturvallisuushäiriöiden varalta.

Lisäksi CER-ehdotuksessa on komission mukaan huomioitu rahoituspalveluja koskeva yhteisön sisämarkkinasäännöstö, joka asettaa kattavat vaatimukset rahoitusyhteisöille operatiivisten riskien hallitsemiseksi ja liiketoiminnan jatkumiseksi. Tämän vuoksi rahoituspalvelusektoriin sovellettaisiin vain direktiivin osan II vaatimuksia. Ehdotettu direktiivi ei myöskään rajoita kilpailusääntöjen soveltamista.

Palveluiden verkostot ovat tiukasti toisiinsa kietoutuneita ja yhdessä jäsenvaltiossa sijaitseva toimija voi tarjota palveluja useassa jäsenvaltiossa tai koko EU:ssa. Tästä seuraa, että tähän operaattoriin vaikuttavalla häiriöllä voi olla kauaskantoisia vaikutuksia muille aloille ja yli kansallisten rajojen. Mahdollinen yleiseurooppalainen häiriötilanne edellyttää toimia koko EU: n tasolla.

Direktiiviehdotuksella on myös liittymäpintoja unionin pelastuspalvelumekanismiin (EU/1313/2013/EU). Pelastuspalvelumekanismi pitää sisällään elementtejä, jotka ovat direktiiviehdotuksen kannalta relevantteja (riskiarviot, jäsenmaiden valmiudet riskienhallintaan), mutta direktiiviehdotuksen soveltamisalan ja pelastuspalvelumekanismipäätöksen soveltamisalan välillä on kuitenkin eroavuuksia. Direktiiviehdotuksessa todetaan, että unionin pelastuspalvelumekanismin osalta voidaan kehittää synergioita katastrofien ennaltaehkäisyyn ja hallintaan liittyen. Komission vaikutusarvion mukaan uuden direktiivin ehdotukset ovat yhteensopivia unionin pelastuspalvelumekanismin muutosta koskevan ehdotuksen kanssa.

Direktiiviehdotuksen 4. artiklan mukaisessa riskien arvioinnissa tulee ottaa huomioon muiden asiaankuuluvien unionin lainsäädännön säädösten mukaisesti suoritetut riskinarvioinnit, tiettyjen alojen välisestä riippuvuudesta johtuvat riskit ja käytettävissä olevat tiedot vaaratilanteista. Yhtenä huomioonotettavana EU-säädösten mukaisena riskiarviointina mainitaan unionin pelastuspalvelumekanismia koskevan päätöksen 6 artiklan mukainen velvoite, jonka mukaan jäsenmaiden on kehitettävä riskiarviointeja, riskienhallintasuunnittelua ja katastrofiriskien hallintaa kansallisella ja alueellisella tasolla. Parhaillaan EU:ssa käsittelyssä olevassa pelastuspalvelumekanismin uudistusta koskevassa päätösehdotuksessa ennaltaehkäisy- ja varautumistoimia pyritään vahvistamaan EU-tasolla määritettävillä katastrofivalmiutta ja -palautuvuutta koskevilla tavoitteilla.

3 Artiklakohtainen tarkastelu

Direktiivin kohde, soveltamisala ja määritelmät (artiklat 1–2)

Direktiivin 1 artiklassa määritetään direktiivin kohde ja soveltamisala, jonka puitteissa jäsenvaltioille asetetaan velvoite toteuttaa ja valvoa toimenpiteitä kriittisten toimijoiden häiriönsietokyvyn parantamiseksi. 1 artikla sisältää myös kuvaukset direktiivin suhteesta muuhun unionilainsäädäntöön ja menettelytavoista direktiivin puitteissa toteutettavasta luottamuksellisen tiedon vaihdosta.

Rajoittamatta SEUT 346 artiklan soveltamista, tulee luottamukselliset tiedot saattaa komission ja muiden asiaankuuluvien viranomaisten tietoon siinä tapauksessa, jos tiedonvaihto on tarpeen tämän direktiivin soveltamiseksi. Tiedonvaihdon järjestelyissä turvataan kriittisten toimijoiden tietoturvallisuus ja kaupalliset edut. 2 artiklassa on luettelo direktiivissä sovellettavista määritelmistä.

Kansalliset toimenpiteet kriittisten toimijoiden häiriönsietokyvyn parantamiseksi (artiklat 3–9)

3 artiklassa todetaan, että jäsenvaltioiden on laadittava kansallinen strategia kriittisten toimijoiden häiriönsietokyvyn vahvistamiseksi kolmen vuoden sisään direktiivin voimaanastumisesta. 3 artikla määrittelee yksityiskohtaisesti strategiassa huomioitavat asiat. Strategian tulee sisältää vähintään seuraavat osat: a) strategiset tavoitteet ja painopisteet järjestelmien kriisinsietokyvyn kehittämiseksi, ottaen huomioon rajat ylittävät ja monialaiset keskinäiset riippuvuudet; b) hallintokehys strategisten tavoitteiden ja painopisteiden saavuttamiseksi, mukaan lukien kuvaus eri viranomaisten rooleista ja vastuista; c) kuvaukset kriisinkestävyyden parantamistoimista mukaan lukien kansallinen riskinarviointi, toimintamalli kriittisten toimijoiden tunnistamiseksi ja niille suunnatut tukitoimenpiteet; d) toimintakehys toimivaltaisten viranomaisten välisen koordinaation tehostamiseksi.

4 artiklassa todetaan, että toimivaltaisten viranomaisten on laadittava luettelo olennaisista palveluista ja suoritettava säännöllisesti kaikkien asiaankuuluvien riskien arviointi, jotka voivat vaikuttaa näiden olennaisten palvelujen saatavuuteen ja kriittisten toimijoiden tunnistamiseen. Arvioinnissa on otettava huomioon muun muassa kansallisen riskinarvion esiin nostamat havainnot, erityisesti keskinäisriippuvuuksien näkökulmasta. Jäsenvaltioiden tulee varmistaa, että riskinarvioinnin olennaiset osat saatetaan sekä kriittisten kansallisten toimijoiden että komission tietoon.

5 artiklassa todetaan, että jäsenvaltioiden on tunnistettava täsmällisesti kriittiset toimijat direktiivin määrittämillä toimialoilla. Artikla määrittää identifiointiprosessissa huomioon otettavia seikkoja, kuten esimerkiksi sen, että jäsenvaltioiden on ylläpidettävä ajantasaista luetteloa kan-

sallisesti tunnistetuista, direktiivin mukaisista kriittisistä palveluista ja niihin liittyvistä toimijoista. Samoin jäsenvaltioita edellytetään informoimaan toimijoille asetetuista direktiivin edellyttämistä velvoitteista.

6 artikla asettaa jäsenvaltioille velvollisuuden ilmoittaa komissiolle merkittävästä kriittisen toimijan häiriötilanteesta. Samoin artikla valtuuttaa komission antamaan ohjeistuksia konsultoituaan direktiivissä perustettua jäsenvaltioiden edustajista muodostettua kriittisten toimijoiden häiriönsietokyvyn asiantuntijaryhmää.

7 artiklassa säädetään, että jäsenvaltioiden olisi yksilöitävä ne pankki- ja rahoitusalan toimijat ja markkina- ja digitaalinen infrastruktuuri, jotka kansallisen arvion mukaisesti lukeutuvat kriittisiksi. Näitä tahoja pitää myös informoida siitä, että heidät on tunnistettu kansallisesti kriittisiksi toimijoiksi. Edellä mainituilla toimialoilla ensisijaisena ohjaavana normistona häiriönsietokyvyn kehittämistoimissa on sektorikohtainen sääntely.

8 artiklassa säädetään, että jäsenvaltioiden nimetyillä, toimivaltaisilla viranomaisilla ja kansallisella yhteyspisteellä tulee olla riittävät resurssit direktiivin mukaisen arviointi-, valvonta- ja raportointitoiminnan järjestämiseksi sekä rajat ylittävän yhteistyön organisoimiseksi, mukaan lukien NIS 2 -direktiiviehdotuksen puitteissa toteutettava yhteistyö. Kansallisen yhteyspisteen on raportoitava komissiolle toimistaan säännöllisesti.

Artikla 9 koskee kansallisia toimenpiteitä, joilla tuetaan direktiivin mukaisesti tunnistettuja kriittisiä toimijoita muun muassa kehittämällä tiedonvaihtoa viranomaisten ja toimijoiden kesken.

Kriittisten toimijoiden häiriönsietokyvyn kehittämistoimet (artiklat 10–13)

Kriittisten toimijoiden on säännöllisesti arvioitava tunnistetut ja merkittävät riskit toimialallaan huomioiden kansallinen riskiarvio ja muut asiaankuuluvat tietolähteet. 11 artiklassa säädetään toimijoiden toteuttamista teknisistä ja organisatorisista toimenpiteistä kriisinkestävyyden parantamiseksi, sisältäen raportointivelvoitteet ja komissiolle myönnettävän oikeuden antaa täytäntöönpanosäädöksiä. 11(4) artiklan nojalla komissiolle myös annettaisiin oikeus käyttää delegoituja asetuksia ko. artiklan ensimmäisen paragrafin muuttamiseksi tai täydentämiseksi.

12 artiklassa säädetään kriittisten toimijoiden oikeudesta pyytää turvallisuusselvityksiä henkilöstöstään, jotka työskentelevät sensitiivisissä tehtävissä tai joita harkitaan rekrytoitavaksi näihin tehtäviin. Direktiivin 12 artikla laajentaisi jäsenvaltioiden velvoitteita luovuttaa rikosrekisteritietoja neuvoston puitepäätöksen 2009/315/YOS mukaisessa ECRIS-yhteistyössä (eurooppalainen rikosrekisteritietojärjestelmä) sekä tehdä kolmannen maan kansalaisia koskevia hakuja asetuksen 2019/816 mukaiseen ECRIS-TCN-järjestelmään (niiden jäsenvaltioiden tunnistamista koskeva keskitetty järjestelmä, joilla on kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden tuomioita koskevia tietoja).

13 artikla koskee jäsenvaltioiden järjestelyä, jolla varmistetaan, että kriittiset toimijat ilmoittavat viipymättä toimivaltaiselle viranomaiselle merkittävistä häiriötilanteista tai tilanteista, jotka saattavat eskaloitua merkittäväksi häiriötilanteeksi. Artikla myös määrittelee keskitetyn yhteyspisteen tiedonvälitystoiminnasta muille jäsenvaltioille.

14–15 artikloissa säädetään erityisen merkittävien eurooppalaisten kriittisten toimijoiden tunnistamisesta ja niiden suojaukseen liittyvistä toimenpiteistä. Artiklat koskevat toimijoita, jotka on tunnistettu kriittisiksi vähintään yhdessä kolmasosassa Euroopan unionin jäsenvaltioista. Jä-

senvaltio, jonka alueelta kyseisen tahon toimintaa johdetaan, on vastuussa tarvittavien ilmoitusten tekemisestä sekä toimijalle että komissiolle. 15 artiklassa kuvataan erityisen kriittisiin toimijoihin sovellettavat valvontajärjestelyt ja muut toimenpiteet, jotka noudattavat pääpiirteittäin artikloissa 5–6 kuvattuja menettelyjä sillä lisäyksellä, että myös komissiolle tulisi oikeus perehtyä erityisen merkittävän toimijan häiriönsietokyvyn kehittämistoimiin.

Yhteistyö ja raportointi (artiklat 16–17)

16 artiklassa kuvataan kriittisten toimijoiden häiriönsietokyvyn asiantuntijaryhmän (CERG) rooli ja tehtävät. Ryhmä perustetaan jäsenvaltioiden ja komission nimeämistä edustajista kuuden kuukauden sisään direktiivin voimaantulosta. Komissio toimii ryhmän puheenjohtajana. Ryhmän tehtävänä on tukea ja mahdollistaa strategisen tason yhteistyö ja tiedonvaihto. Artiklan mukaan komissio voi antaa täytäntöönpanosäädöksiä, jotka komitea käsittelee tarkastelumenettelyn mukaisesti.

17 artiklassa säädetään komission tukitoimenpiteistä sekä jäsenvaltioille että kriittisille toimijoille, joiden tavoitteena on varmistaa, että kriittiset toimijat ja jäsenvaltiot noudattavat direktiivin mukaisia velvoitteitaan, ottaen huomioon rajat ylittävät ja monialaiset häiriötilanteet.

Valvonta ja täytäntöönpano (artiklat 18–19)

Direktiiviehdotuksen 18 artiklassa todetaan jäsenvaltioiden vastuut ja tehtävä varmistaa direktiivin kansallinen täytäntöönpano, mukaan lukien yhteistyö NIS 2 direktiiviehdotuksen mukaisilla toimialoilla.

Direktiiviehdotuksen 19 artikla edellyttää, että jäsenvaltiot toteuttavat tarvittavat järjestelyt seuraamusten määrittämiseksi niille jäsenvaltioiden tunnistamille kriittisille toimijoille, jotka eivät ole noudattaneet direktiivissä määrättyjä toimenpiteitä. Jäsenvaltioiden tehtävänä on varmistaa artiklan 19 mukaisilla toimenpiteillä, että kriittiset toimijat saadaan noudattamaan direktiivin määräämiä toimenpiteitä.

Loppusäännökset (artiklat 20–26)

Direktiiviehdotuksen 20 artiklassa todetaan, että komissiota avustaa asetuksen (EU) 182/2011 mukainen komitea. 21 artikla antaa komissiolle oikeuden antaa delegoituja säädöksiä artiklassa säädetyin edellytyksin. 22 artiklassa säädetään, että komissio toimittaa kertomuksen Euroopan parlamentille, Euroopan parlamentti ja neuvosto arvioivat, missä määrin jäsenvaltiot ovat toteuttaneet tarvittavat toimenpiteet direktiivin noudattamiseksi.

23 artiklassa todetaan, että ECI-direktiivi 2008/114 / EY kumotaan CER-direktiiviehdotuksen voimaantulopäivästä.

24 artiklassa todetaan, että jäsenvaltioiden on annettava ja julkaistava ehdotuksen määrittämässä määräajassa tarvittavat lait, asetukset ja hallinnolliset määräykset,

ja ilmoitettava siitä komissiolle.

25 artiklassa todetaan, että CER-direktiivi tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu Euroopan unionin virallisessa lehdessä.

Direktiivin 26 artiklassa todetaan, että direktiivi on osoitettu kaikille jäsenvaltioille.

4 Ehdotuksen oikeusperusta, toissijaisuus- ja suhteellisuusperiaate sekä suhde perustuslakiin

CER-direktiiviehdotuksen oikeusperustana on SEUT 114 artikla, joka koskee sisämarkkinoiden toteuttamiseen ja toimintaan liittyviä toimenpiteitä. SEUT 114 artiklan tavoitteena on lähentää jäsenvaltioiden lainsäädäntöjä, kun niissä on eroja, jotka ovat omiaan rajoittamaan sisämarkkinoiden perusvapauksia ja joilla näin ollen voi olla suora vaikutus sisämarkkinoiden toimintaan.

Ehdotus käsitellään Euroopan parlamentin ja neuvoston yhteispäätösmenettelyssä tavanomaista lainsäätämisjärjestystä noudattaen. Neuvosto päättää ehdotuksen hyväksymisestä määräenemmistöllä. Säädöspohjan muutos ECI-direktiivin SEUT 352 artiklan (ent. SEY 308 artikla) SEUT 114 artiklaksi on komission mukaan perusteltua direktiivin tavoitteen, soveltamisalan ja sisällön muuttuessa. Lisäksi ehdotus on pyritty yhdenmukaistamaan verkko- ja tietojärjestelmiä koskevan direktiiviehdotuksen (NIS2) kanssa.

Komissio pitää direktiiviehdotusta suhteellisuus- ja toissijaisuusperiaatteiden mukaisina. Komissio katsoo perustelluksi sen, että jäsenvaltiot ottavat keskenään samansuuntaisen lähestymistavan sisämarkkinoiden palveluiden kriisinkestävyyden parantamiseksi ja niitä koskevaan toiminnan sääntelyyn sekä valvontaan. Kyseinen toiminta on myös luonteeltaan usein jäsenvaltioiden rajat ylittävää, mikä osaltaan jo nyt luo haasteita sisämarkkinoiden yleisen järjestyksen ja taloudellisen toiminnan tehokkaalle ja ennakoivalle turvaamiselle.

Suhteellisuusperiaatteen osalta komissio kiinnittää huomiota siihen, että joissakin tapauksissa direktiivin noudattaminen voi vaatia huomattavia investointeja. Tällaisissa tapauksissa nämä investoinnit ovat kuitenkin komission mukaan perusteltuja, koska ne edistävät sekä operatiivisen tason että järjestelmätason kriisinkestävyyden parantamista. Lisäksi direktiivistä valtioille, unionille ja sen kansalaisille mahdollisesti aiheutuvan ylimääräisen lisärasituksen komissio katsoo olevan perusteltu ja kohtuullinen, kun sen suhteuttaa niihin potentiaalisesti merkittäviin kustannuksiin, jotka aiheutuvat laajoista häiriöistä, jotka vaarantavat kriittisiin yhteiskunnallisiin toimintoihin liittyvät palvelut ja yksittäisten jäsenvaltioiden operaattoreiden taloudellisen toimintakyvyn.

Direktiiviehdotuksen 12 artiklassa tarkoitettuihin työntekijöiden taustaselvityksiin (turvallisuusselvityksiin/ luotettavuuden selvittämiseen) liittyisi henkilötietojen käsittelyä, jossa olisi noudatettava henkilötietojen suojaa koskevia säännöksiä. Henkilötietojen suojaa koskeviin vaatimuksiin sisältyvät muun muassa käsiteltävien tietojen minimointiperiaate ja oikeasuhteisuuden vaatimus. Komissio ei ole arvioinut ehdotettujen erityissäännösten perusoikeusvaikutuksia kattavammin. Ehdotuksen mukaan työntekijöiden taustan selvittämisessä olisi erityisesti hyödynnettävä myös muilta jäsenvaltioilta saatavia rikosrekisteritietoja ECRIS-järjestelmän kautta.

Ehdotetut turvallisuusselvityksiä koskevat säännökset ovat merkityksellisiä perustuslain 10 §:n kannalta. Sen 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa rajoittaa tämän säännöksen lisäksi myös se, että henkilötietojen suoja sisältyy osittain samassa momentissa turvatun yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa (ks. esim. PeVL 13/2016 vp, s. 3—4). Perustuslakivaliokunta on painottanut arkaluonteisten tietojen käsittelyn aiheuttamia uhkia. Valiokunnan mielestä arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille (PeVL 14/2018 vp, s. 5, PeVL 13/2016 vp, s. 4, PeVL 14/2009 vp, s. 3/I). Myös EU:n yleisen tietosuoja-asetuksen

johdantokappaleessa 51 painotetaan, että asetuksen 9 artiklassa tarkoitettuja erityisiä henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, koska niiden käsittelyn asiayhteys voisi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille. Valiokunta on tämän johdosta kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on syytä rajata täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään (PeVL 14/2018 vp, s. 5, PeVL 3/2017 vp, s. 5). Komission ehdotuksesta ei käy ilmi, voisiko ehdotetussa 12 artiklassa tarkoitettu henkilötietojen käsittely kattaa erityisiin henkilötietoryhmiin kuuluvia tietoja. Ehdotuksessa tarkoitetut rikosrekisteritiedot ovat kuitenkin valtiosääntöoikeudellisesti arkaluonteisia tietoja. Näitä tietoja olisi myös ehdotuksen mukaan vaihdettava jäsenvaltioiden kesken työntekijöiden taustan selvittämistä varten. Ehdotuksesta on myös vaikea arvioida tarkalleen, mitä henkilöryhmiä selvitykset tulisivat kattamaan. Ehdotuksella olisi kuitenkin arviolta enemmän perusoikeuksien suojaan, erityisesti yksityiselämän suojaan ulottuvia vaikutuksia kuin ehdotuksesta käy ilmi. Lisäksi säädösehdotuksen jatkokäsittelyn yhteydessä olisi syytä arvioida mahdollisia vaikutuksia perustuslain 18 §:n mukaiseen elinkeinovapauteen.

Komission ehdotusta voidaan pitää toissijaisuus- ja suhteellisuusperiaatteen mukaisina. Vaikka esitetyt perustelut eivät ole kovin yksityiskohtaisia, ei niitä voida pitää asian arvioimisen kannalta riittämättöminä. Valtioneuvosto ei katso ehdotuksen olevan ristiriidassa Suomen perustuslain tai Suomea velvoittavien perus- ja ihmisoikeussopimusten kanssa.

Valtioneuvosto suhtautuu komission ehdotukseen direktiivin oikeusperustaksi alustavasti myönteisesti, mutta arvioi asiaa vielä valmistelun edetessä. Direktiiviehdotuksen voidaan katsoa liittyvän jäsenvaltioiden lainsäädännön yhteensovittamiseen ja sisämarkkinoiden kehittämiseen, sekä kriittisten infrastruktuuritoimijoiden suojaamiseen ja niiden kriisinkestävyyden parantamiseen. Lisäksi direktiiviehdotuksella varmistetaan, että jäsenvaltiot soveltavat yhtenäistä tapaa yhteiskuntien kannalta kriittisten toimijoiden tunnistamisessa sekä huomioidaan kansalliset erityispiirteet, kuten jäsenvaltiokohtaiset riskitasot.

5 Vaikutukset

5.1 Vaikutukset lainsäädäntöön

Direktiivi saatetaan voimaan EU:n jäsenmaissa kansallisella lainsäädännöllä. CER-direktiiviehdotuksesta seuraa uusia toiminnan järjestämistä koskevia vaatimuksia, kuten kriittisten toimijoiden tunnistamiseen ja valvontaan liittyviä viranomaistehtäviä. Tällä hetkellä Suomessa ei kansallista kriittistä infrastruktuuria, kriittisiä sektoreita tai toimijoita ole määritelty lainsäädännön tasolla.

Direktiivin täytäntöönpano edellyttää tarkempaa kansallista lainsäädäntövaikutuksien sekä eri toimialojen viranomaisille ja yksityisille yrityksille aiheutuvien velvoitteiden arviointia. Kansallisten varautumisjärjestelyjen tarkastelu ja kehittäminen ovat ajankohtaisia myös koronakriisin tuottamien vaikutusten johdosta.

CER-direktiiviehdotuksen soveltamisala koskee kymmentä sektoria, kattaen liikenteen, energian, pankit, finanssimarkkinat, terveyden, vesi- ja jätevesihuollon, digitaalisen infrastruktuurin, julkishallinnon ja avaruuden. Se asettuu yhteiskunnan turvallisuusstrategian ja sitä palvelevan kokonaisturvallisuusmallin nimeämien yhteiskunnan elintärkeiden toimintojen ja huoltovarmuuden turvaamiseksi tunnistettujen sektorien sekä huoltovarmuuspoolien toimialojen väliin. Niiden joukossa on lisäksi yksi sektori, avaruus, joka ei sisälly tällä hetkellä tunnistettuihin toimintoihin tai sektoreihin.

Huoltovarmuudelle käsitteenä, sellaisena kuin se Suomessa ymmärretään, ei tällä hetkellä ole EU:ssa vastinparia. Suomessa huoltovarmuudella tarkoitetaan sitä, että poikkeusolojen ja niihin verrattavissa olevien vakavien häiriöiden varalta turvataan väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömät taloudelliset toiminnot ja niihin liittyvät tekniset järjestelmät (laki huoltovarmuuden turvaamisesta 1390/1992). Valtioneuvosto asettaa huoltovarmuuden yleiset tavoitteet. Huoltovarmuuden järjestämisen näkökulmasta on tärkeää yhteen sovittaa direktiivi ja huoltovarmuutta koskeva kansallinen säädöspohja.

Huoltovarmuus pohjautuu toimiviin kansainvälisiin markkinoihin, kuten EU:n sisämarkkinoihin, kilpailukykyiseen talouteen sekä monipuoliseen teolliseen ja muuhun tuotannolliseen pohjaan.

Huoltovarmuuskeskuksen tehtävänä on maan huoltovarmuuden ylläpitäminen ja kehittäminen. Suomen huoltovarmuusjärjestelmän perustana on huoltovarmuusorganisaatio. Se on verkosto, joka ylläpitää ja kehittää Suomessa huoltovarmuutta julkinen-yksityinen -kumppanuusperiaatteella. Yhteistyö on yksityisen sektorin toimijoille lähtökohtaisesti vapaaehtoista. Vapaaehtoisen kumppanuuden lisäksi huoltovarmuutta turvataan eräillä toimialoilla myös velvoittavilla säädöksillä.

Huomattavaa on myös, että direktiivi voimaantultuaan nostaisi yleistä kriisinkestävyyden tasoa Euroopan unionin jäsenmaissa, mukaan lukien sellaisissa, joissa on Suomen huoltovarmuuden kannalta merkittäviä toimintoja ja riippuvaisuuksia.

Direktiiviluonnoksen esittämien jäsenvaltioille asetettujen velvoitteiden täyttämisen arvioidaan edellyttävän toimivaltaisten viranomaisten täsmällistä määrittämistä ja uudenlaisten kyvykkyyksien kehittämistä.

Direktiiviehdotuksen valvontatehtävä, joka koskee kriittisten toimijoiden riskiarvioita ja kriittisten järjestelmien kriisinkestävyyden ohjaamista ja arviointia tulee edellyttämään osaamista mm. riskienhallinnan, toiminnanohjauksen, laadunhallinnan aloilla. Vaatimuksia voi kohdistua myös tietoturvallisuuteen ja tietosuojaan liittyvään osaamiseen.

Direktiivin mukaisten kriittisten järjestelmien tunnistaminen muistuttaa huoltovarmuudelle kriittisten toimijoiden määrittelyä. Koska direktiiviehdotuksen sektorit kuitenkin eroavat merkittävästi voimassa olevista huoltovarmuudelle kriittisistä sektoreista, on näiden kahden käsitteen suhde tärkeää määritellä.

Direktiivi tuo velvoitteita kansallisesti tunnistetuille kriittisille järjestelmille ja niiden operaattoreille. Tätä kokonaisuutta on uudelleenarvioitava direktiivin toimeenpanon yhteydessä. On myös mahdollista, että direktiiviehdotuksesta ja NIS2-direktiiviehdotukseen sisältyvistä laajennuksista syntyy sellaisia resurssi- ja muita vaikutuksia myös viranomaisille, joita olisi syytä arvioida kokonaisuutena.

Direktiiviluonnoksen asettamat velvoitteet vaativat tiivistä yhteistyötä viranomaisten kesken, raportointia jäsenvaltioiden sisällä, jäsenvaltioiden välillä ja jäsenvaltioiden sekä komission välillä. Koska raportoitava tieto koskee yhteiskunnan turvallisuutta ja toimintavarmuutta, on niiden suojaaminen ensisijaisen tärkeää niin jäsenvaltioissa kuin komissiossakin. Direktiivin velvoitteita koskevista tiedoista koostuvan aineiston arkaluontoisuuden tasoa on tässä vaiheessa vaikeaa määritellä, mutta sen käsittelyn voidaan arvioida jo tässä vaiheessa edellyttävän erityisiä toimia, joista komission tulisi antaa lisätietoa.

Direktiiviehdotuksen 12 artiklalla olisi ehdotetussa muodossa suoria vaikutuksia Suomen lainsäädäntöön. Näitä kohdistuisi ainakin turvallisuusselvityslakiin (726/2014) ja henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettuun lakiin (1054/2018). Direktiiviluonnoksen 12 artiklan velvoitteet ovat toteutettavissa turvallisuusselvityslain mukaisesti lukuun ottamatta EU-rikosrekisteritietoja (Art 12(2)(b)). Turvallisuusselvityslain rakenteesta johtuen näiden tietojen sisällyttäminen on mahdollista vain perusmuotoisissa turvallisuusselvityksissä, mutta luultavasti selvitysten piiriin tulisi myös henkilöitä, jotka lain systematiikan mukaan kuuluvat suppean turvallisuusselvityksen piiriin. Rikosrekisteritietojen laajentaminen on vaikeaa ilman, että ne laajenevat samalla kaikkien suppeiden turvallisuusselvitysten osalta.

Ehdotuksella voi olla vaikutuksia myös muuhun työntekijöiden taustan tai luotettavuuden selvittämistä koskevaan sääntelyyn, johon Suomessa kuuluu turvallisuusselvityslain lisäksi ainakin rikosrekisteriä koskeva sääntely. Lisäksi säädösehdotuksen jatkokäsittelyn yhteydessä olisi arvioitava sen suhdetta valmiuslakiin (1552/2011).

5.2 Vaikutukset talouteen

Ehdotetulla direktiivillä on vaikutuksia Euroopan unionin talousarvioon. Komissio arvioi ehdotuksen täytäntöönpanon tukemiseksi tarvittavien kustannusten olevan 42,973 miljoonaa euroa kaudella 2021—2027. Kustannuksista n. 37,8 miljoonaa euroa on tarkoitus kattaa sisäisen turvallisuuden rahastosta monivuotisen rahoituskehyksen otsakkeessa 5 (palautumiskyky, turvallisuus ja puolustus). Komissio arvioi hallintomenojen olevan n. 5,2 miljoonaa euroa ja nämä katetaan monivuotisen rahoituskehyksen otsakkeesta 7 (EU:n yleinen hallinto). Kaiken kaikkiaan kustannukset koostuvat seuraavasti: Komission tukitoimet, hankkeet ja tutkimukset sekä komission järjestämät neuvontamatkat, kriittisten toimijoiden häiriönsietokyvyn asiantuntijaryhmän komiteamenettely, komitean säännölliset kokoukset ja muut kokoukset.

Komission mukaan ehdotuksen taloudelliset vaikutukset EU-budjettiin voidaan kokonaisuudessaan rahoittaa uudelleenkohdennuksin monivuotisen rahoituskehyksen asianomaisen otsakkeen sisällä. Komission esityksen perusteluissa (Legislative Financial Statement) on esitetty rahoituksen tarkempi jakautuminen talousarvion otsakkeittain ja vuosittain.

Sisäisen turvallisuuden rahasto jakaantuu komission hallinnoimaan ns. temaattiseen välineeseen ja jäsenvaltioiden toimeenpanemiin kansallisiin ohjelmiin. Komissio aikoo hyödyntää direktiivin toimeenpanossa molempia välineitä. Kansallisiin ohjelmiin liittyy kansallisen rahoituksen vaatimus (0—25 %), johon tulee varautua kansallisissa talousarvioissa. Tarvetta ei kuitenkaan vielä pystytä arvioimaan. Direktiivin toimeenpanosta aiheutuvia kansallisia toimia voidaan soveltuvin osin rahoittaa sisäisen turvallisuuden rahastosta.

Ehdotuksesta aiheutuu todennäköisesti sekä valtiolle että kriittisten järjestelmien operaattoreille kustannuksia riippuen siitä, missä laajuudessa direktiiviehdotuksessa esitetyt asiat on jo huomioitu nykyisissä kansallisissa järjestelyissä. Komission ehdotuksessa ei ole tarkemmin arvioitu kansallisille viranomaisille tai yksityiseen sektoriin kohdistuvia kustannusvaikutuksia. Esimerkiksi riskiarvioihin liittyvän kokonaisuuden nähdään tuottavan kustannusvaikutuksia kriittisiksi tunnistetuille toimijoille, joiden suuruutta on mahdollista arvioida vasta myöhemmässä vaiheessa.

Kansallisten toimivaltaisten viranomaisten ja yhteyspisteen tehtävät ovat uusia ja niistä seuraa todennäköisesti resurssitarvetta, josta aiheutuvaa kustannusvaikutusta ei tässä vaiheessa ole vielä mahdollista arvioida. Jos direktiivin edellyttämät uudet tehtävät olisivat esimerkiksi sisäl-

lytettävissä osaksi olemassa olevien viranomaisten tehtäviä, olisi kustannusvaikutus todennäköisesti pienempi kuin siinä tapauksessa, että toimintaa varten perustettaisiin kokonaan uusi viranomainen.

Lisäksi työntekijöiden taustan selvittämistä koskevalla ehdotuksella olisi resurssivaikutuksia ainakin Suojelupoliisiin ja Puolustusvoimien Pääesikuntaan, jotka ovat Suomessa toimivaltaisia tekemään turvallisuusselvityksiä. Lisäksi ehdotuksella voisi olla vaikutuksia mahdollisten yritysturvallisuusselvitysten osalta Liikenne- ja viestintävirastoon.

Direktiivin velvoitteista laajentaa rikosrekisteritietojen vaihtamista koskevaa ECRIS- ja ECRIS-TCN-yhteistyötä aiheutuisi Oikeusrekisterikeskukselle sekä tietojärjestelmä- että henkilöstökustannuksia. Tarkkaa arviota Oikeusrekisterikeskukselle aiheutuvista kustannuksista ei voida tässä vaiheessa tehdä.

6 Muiden jäsenvaltioiden kannat

Muiden jäsenvaltioiden kantoja ei ole vielä tiedossa.

7 Ehdotuksen kansallinen käsittely ja käsittely Euroopan unionissa

Direktiiviehdotus sekä siihen liittyvä luonnos valtioneuvoston kirjelmäksi on ollut lausunnolla EU-asiain komitean oikeus- ja sisäasiat jaoston (EU 7), kilpailukykyjaoston (EU 8), viestintäjaoston (EU 19) ja liikennejaoston (EU 22) kirjallisessa menettelyssä.

Komissio ehdotuksen käsittely ei ole vielä alkanut neuvostossa. Euroopan parlamentti ei ole vielä aloittanut ehdotuksen käsittelyä.

8 Ahvenanmaan toimivalta

Ahvenanmaan itsehallintolain (1144/1991) 18 §:n mukaan maakunnalla on lainsäädäntövaltaa asioissa, jotka koskevat maakunnan hallitusta sekä sen alaisia viranomaisia ja laitoksia sekä eräin rajoituksin lainsäädäntövaltaa asioissa, jotka koskevat elinkeinotoimintaa. Lain 27 §:n mukaan puolestaan valtakunnalla on lainsäädäntövaltaa asioissa, jotka koskevat kauppamerenkulkua, ilmailua, standardisointia sekä valtion viranomaisten järjestysmuotoa ja toimintaa sekä teletoimintaa. Valtioneuvosto arvioi jatkovalmistelussa direktiiviehdotuksen vaikutusta Ahvenanmaan asemaan.

9 Valtioneuvoston kanta

Valtioneuvosto pitää EU:n kriisinkestävyyden kokonaisvaltaista kehittämistä keskeisenä. On erityisen tärkeää, että kriittisten toimijoiden fyysistä ja digitaalista kriisinkestävyyttä edistetään vahvasti EU:ssa ja jäsenmaissa. Näin parannetaan myös EU:n ja jäsenmaiden varautumista hybridiuhkiin. Muuttuva turvallisuusympäristö sekä meneillään oleva COVID-19-pandemia ovat osoittaneet, että EU:ssa on määritettävä ja tunnistettava yhdenmukaisin menettelyin yhteiskuntien toimintakyvyn kannalta kriittiset toimijat ja parannettava niiden kriisinsietokykyä muun muassa kehittämällä suojaustoimenpiteitä, tunnistamalla paremmin jäsenvaltioiden välisiä keskinäisriippuvuuksia sekä estämällä tietojen yhdistelyn ennakoimattomia vaikutuksia.

Valtioneuvosto katsoo, että kriittisten järjestelmien suojelu on tärkeää nähdä kokonaisuutena ja että jatkuvuudenhallinta, häiriönsietokyvyn kehittäminen ovat keskeisessä asemassa Euroopan kriittisen fyysisen ja digitaalisen infrastruktuurijärjestelmien turvallisuuden ja toimintakyvyn

parantamisessa. Valtioneuvosto tukee EU:n kokonaisvaltaista ajattelua, jossa CER-direktiiviehdotus on osa laajempaa pakettia, johon kuuluu myös uusi kyberturvallisuusstrategia sekä verkko- ja tietoturvadirektiivin päivitys.

CER-direktiiviehdotuksen tavoitteena on parantaa yhteiskunnan elintärkeiden toimintojen tai taloudellisen toiminnan ylläpitämisen kannalta kriittisten palvelujen tarjoamista sisämarkkinoilla ja siten parantaa sisämarkkinoiden toimintaa myös kriisitilanteissa. Samalla tunnistetaan eri toimijoiden ja toimialojen keskinäisriippuvuudet, joihin myös Suomen kriittiset toimijat ovat kytkeytyneitä. Valtioneuvosto katsoo, että sisämarkkinoiden kriittisten palveluiden toimintavarmuuden paraneminen tukee osaltaan myös Suomen huoltovarmuuden ylläpitoa ja kehittämistä.

Valtioneuvosto toteaa, että ehdotus on osin lähtökohdiltaan ja periaatteeltaan erilainen kuin Suomen huoltovarmuusjärjestelmä, mutta ehdotuksen voidaan katsoa lisäävän EU-tasoista kriisinkestävyyttä sekä EU-maiden välistä yhteistyötä. Valtioneuvosto arvioi valmistelun edetessä tarkemmin direktiiviehdotuksen vaikutuksia kansalliseen lainsäädäntöön sekä ehdotuksen yritys- sekä hallinnollisia vaikutuksia, erityisesti kansallisen huoltovarmuusjärjestelmän osalta.

CER-direktiivi huomioi kriittisten järjestelmien kytköksen kybermaailmaan. Valtioneuvosto pitää hyvänä, että direktiiviehdotus on yhdenmukainen NIS 2 direktiiviehdotuksen kanssa, jossa säännellään keskeisten toimijoiden kyberturvallisuudesta ja digitaalisesta infrastruktuurista. Molempien ehdotusten myötä sekä kansallinen että rajat ylittävä viranomaisyhteistyö ja tietojenvaihto tulevat lisääntymään, mikä parantaa ymmärrystä fyysisten ja digitaalisten järjestelmien keskinäisriippuvuuksista. Keskusteluun tulisi nostaa myös paikkatieto eli paikkaan sidottu tieto, joka on tietoyhteiskunnan toiminnan kannalta kriittinen elementti, ja johon yhdistyy aina myös muita tärkeitä kohdetietoja. Paikkatieto muodostaa kokonaiskuvan yhteiskuntien toiminnollisuuksista ja niiden sijainneista. Tätä kokonaisuutta tulisi suojella nykyistä kattavammin. Valtioneuvosto lisäksi korostaa, että erityistä huomiota tulee kiinnittää omistajuuteen ja määräysvallan säilymiseen unionissa kriittisten toimijoiden osalta.

Direktiiviehdotus tukee jäsenvaltioiden kansallisia toimenpiteitä ja viranomaistoimintaa. Esityksen velvoitteet sekä jäsenvaltioille että kriittisille toimijoille on tärkeää suunnitella siten, etteivät velvoitteet lisää tarpeettomasti hallinnollista taakkaa tai kustannuksia. Mahdollisesta kansallisesta rahoituksesta päätetään julkisen talouden suunnitelman ja valtion talousarvion valmistelun yhteydessä. Toimenpiteiden edellyttämä valtion rahoitus toteutetaan valtiontalouden kehysten puitteissa tarvittaessa kohdentamalla määrärahoja uudelleen.

Valtioneuvosto kiinnittää valmistelun edetessä huomiota jäsenvaltioiden raportointivelvoitteiden oikeasuhtaisuuteen. Perussopimusten mukaan kansallinen turvallisuus säilyy kunkin jäsenvaltion vastuulla. Valtioneuvosto katsoo, että komissiolle delegoitavien toimivaltuuksien tulisi olla tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja hyvin perusteltuja.

Valtioneuvosto suhtautuu komission ehdotukseen direktiivin oikeusperustaksi alustavasti myönteisesti, mutta arvioi asiaa vielä valmistelun edetessä. Direktiiviehdotuksen voidaan katsoa liittyvän jäsenvaltioiden lainsäädännön yhteensovittamiseen ja sisämarkkinoiden kehittämiseen, sekä kriittisten infrastruktuuritoimijoiden suojaamiseen ja niiden kriisinkestävyyden parantamiseen. Lisäksi direktiiviehdotuksella varmistetaan, että jäsenvaltiot soveltavat yhtenäistä tapaa yhteiskuntien kannalta kriittisten toimijoiden tunnistamisessa sekä huomioidaan kansalliset erityispiirteet, kuten jäsenvaltiokohtaiset riskitasot.

Direktiiviehdotuksessa tarkoitettuun taustan selvittämiseen liittyviä taloudellisia ja lainsäädäntövaikutuksia tulisi arvioida vielä tarkemmin. Lisäksi kyseisen ehdotuksen perusoikeuksia rajoittavia vaikutuksia tulisi arvioida huolellisesti ehdotuksen käsittelyn aikana. Neuvottelujen

aikana on tärkeää kiinnittää huomiota siihen, että turvallisuusselvityksiin sovelletaan kansallista lainsäädäntöä ja myös niihin käytettävät lähderekisterit ja toimivaltaiset viranomaiset voivat poiketa toisistaan. Tulisi pyrkiä vaikuttamaan siihen, että täytäntöönpanoon jää riittävästi kansallista liikkumavaraa. Erityisesti työntekijöiden taustan selvittämiseen sovellettava henkilötietojen käsittelyä koskeva yleislaki ja EU-rikosrekisteritietojen käyttäminen olisi syytä jättää kansalliseen harkintaan.