Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan tietyille yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajille sekä eräiden digitaalisten palveluiden tarjoajille tietoturvallisuuteen liittyvää riskienhallintaa ja häiriöiden raportointia koskevia velvoitteita. Lisäksi säädettäisiin näiden velvoitteiden valvonnasta, viranomaisten välisestä tietojen vaihdosta sekä yleisestä tietoturvallisuuteen liittyvästä viranomaistoiminnasta. Ehdotetulla lainsäädännöllä saatettaisiin osaksi kansallista lainsäädäntöä toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annettu Euroopan parlamentin ja neuvoston direktiivi.

Esityksellä toteutetaan osaltaan hallitusohjelman tavoitetta digitalisaation edistämisestä ja digitaalisen turvallisuuden varmistamisesta parantamalla yhteiskunnan ja kansalaisten kannalta keskeisten palveluiden tietoturvallisuuden tasoa. Esityksellä kasvatetaan kansalaisten ja yritysten luottamusta digitalisaatioon ja edistetään siten myös digitaalisen liiketoiminnan kasvua ja kilpailukykyä.

Yhteiskunnan toiminnan kannalta keskeisten palvelujen tietoturvallisuuden parantamiseksi tietoyhteiskuntakaareen, ilmailulakiin, rautatielakiin, alusliikennepalvelulakiin, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin, liikenteen palveluista annettuun lakiin, sähkömarkkinalakiin, maakaasumarkkinalakiin sekä vesihuoltolakiin lisättäisiin säännökset keskeisten palveluntarjoajien velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittaa merkittävästä tietoturvallisuuteen liittyvästä häiriöstä valvovalle viranomaiselle ja yleisölle. Tietoyhteiskuntakaaren velvoitteet koskisivat verkossa toimivan markkinapaikan tarjoajaa, hakukonepalvelun tarjoajaa sekä pilvipalvelun tarjoajaa. Ilmailulain velvoitteet koskisivat lennonvarmistuspalvelun tarjoajaa sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjää. Rautatielain velvoitteet koskisivat valtion rataverkon haltijaa sekä liikenteenohjauspalveluita tarjoavaa yhtiötä. Alusliikennepalvelulain velvoitteet koskisivat alusliikennepalvelun tarjoajaa. Eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain velvoitteet koskisivat yhteiskunnan toiminnan kannalta merkittävän sataman pitäjää. Liikenteen palveluista annetun lain velvoitteet koskisivat älykkään liikennejärjestelmän ylläpitäjää. Sähkömarkkinalain velvoitteet koskisivat verkonhaltijaa. Maakaasumarkkinalain velvoitteet koskisivat siirtoverkonhaltijaa ja vesihuoltolain velvoitteet vesihuoltolaitosta, joka toimittaa vettä vähintään tai ottaa vastaan jätevettä 5000 kuutiometriä vuorokaudessa.

Toimivalta valvoa riskienhallinta- ja häiriöraportointivelvoitteita olisi sektorikohtaisilla valvontaviranomaisilla. Tämä tarkoittaisi Viestintävirastoa, Liikenteen turvallisuusvirastoa, Energiavirastoa, Finanssivalvontaa, sekä elinkeino-, liikenne- ja ympäristökeskusta. Viranomaisten välisen yhteistyön turvaamiseksi ehdotetaan viranomaisten toimivaltuuksia koskevan lainsäädännön yhteyteen lisättäväksi säännökset valvovien viranomaisten yhteistyöstä sekä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi tarvittavien salassa pidettävien tietojen vaihdosta.

Lisäksi Viestintävirastolle säädettäisiin velvoite toimia yhteistyössä verkko- ja tietoturvadirektiivin tarkoittamien tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden, valvontaviranomaisten sekä jäsenvaltioiden yhteistyöryhmän kanssa.

Ehdotetut lait on tarkoitettu tulemaan voimaan 1 päivänä toukokuuta 2018.

———————

SISÄLLYS

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ 1
SISÄLLYS 3
YLEISPERUSTELUT 6
1 JOHDANTO 6
2 NYKYTILA 9
2.1 Lainsäädäntö ja käytäntö 9
2.1.1 Yleistä 9
2.1.2 Suomen tietoturvallisuusstrategia ja kyberturvallisuusstrategia 9
2.1.3 Yhteiskunnan toiminnan kannalta keskeiset toiminnot 10
2.1.4 Palvelujen tarjoajien toimintaan liittyvät laatu- ja riskienhallintavaatimukset sekä turvallisuuteen liittyvistä häiriöistä ilmoittaminen viranomaisille 11
2.1.5 Huoltovarmuus ja varautuminen poikkeusoloihin 23
2.1.6 Muu keskeisten palvelujen tietoturvallisuuden kannalta merkityksellinen lainsäädäntö 23
2.1.7 Viranomaisvalvonta ja tilannekuvan muodostaminen 25
2.1.8 Viranomaisten välinen yhteistyö ja tiedonvaihto 29
2.1.9 Seuraamukset 29
2.2 Kansainvälinen kehitys sekä ulkomaiden ja EU:n lainsäädäntö 30
2.2.1 EU:n lainsäädäntö 30
2.2.2 Kansainvälinen kehitys 40
2.3 Nykytilan arviointi 43
2.3.1 Tietoturvallisuusstrategia 43
2.3.2 Tietoturvaloukkauksiin reagointi ja niiden tutkinta 43
2.3.3 Yhteiskunnan toiminnan kannalta keskeiset palvelut ja keskeisten palveluiden tarjoajat 44
2.3.4 Palveluntarjoajien toimintaan liittyvät tietoturvallisuusriskienhallinta- ja raportointivaatimukset 50
2.3.5 Riskienhallinta- ja raportointivelvoitteiden valvonta 55
3 ESITYKSEN TAVOITTEET JA KESKEISET EHDOTUKSET 56
3.1 Tavoitteet 56
3.2 Toteuttamisvaihtoehdot 56
3.3 Keskeiset ehdotukset 58
4 ESITYKSEN VAIKUTUKSET 59
4.1 Taloudelliset vaikutukset 59
4.2 Vaikutukset viranomaisen toimintaan 60
4.3 Yhteiskunnalliset vaikutukset 60
5 ASIAN VALMISTELU 61

5.1 Valmisteluvaiheet ja -aineisto 61
5.2 Lausunnot ja niiden huomioon ottaminen 62
6 RIIPPUVUUS MUISTA ESITYKSISTÄ 62
6.1 Esityksen suhde Ahvenanmaan itsehallintoon 63
YKSITYISKOHTAISET PERUSTELUT 64
1 LAKIEHDOTUSTEN PERUSTELUT 64
1.1 Laki tietoyhteiskuntakaaren muuttamisesta 64
1.2 Laki ilmailulain muuttamisesta 67
1.3 Laki rautatielain muuttamisesta 69
1.4 Laki alusliikennepalvelulain muuttamisesta 71
1.5 Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta 73
1.6 Laki liikenteenpalveluista annetun lain muuttamisesta 75
1.7 Laki sähkömarkkinalain muuttamisesta 77
1.8 Laki maakaasumarkkinalain muuttamisesta 78
1.9 Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 27 ja 28 §:n muuttamisesta 80
1.10 Laki vesihuoltolain muuttamisesta 80
1.11 Laki finanssivalvonnasta annetun lain muuttamisesta 82
2 VOIMAANTULO 83
3 SUHDE PERUSTUSLAKIIN JA SÄÄTÄMISJÄRJESTYS 83
LAKIEHDOTUKSET 85
tietoyhteiskuntakaaren muuttamisesta 85
ilmailulain muuttamisesta 88
rautatielain muuttamisesta 90
alusliikennepalvelulain muuttamisesta 91
eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta 93
liikenteen palveluista annetun lain muuttamisesta 95
sähkömarkkinalain muuttamisesta 96
maakaasumarkkinalain muuttamisesta 97
sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 27 ja 28 §:n muuttamisesta 98
vesihuoltolain muuttamisesta 99
Finanssivalvonnasta annetun lain muuttamisesta 101
RINNAKKAISTEKSTIT 102
tietoyhteiskuntakaaren muuttamisesta 102
ilmailulain muuttamisesta 106
rautatielain muuttamisesta 108
alusliikennepalvelulain muuttamisesta 110
eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta 112
liikenteen palveluista annetun lain muuttamisesta 114
sähkömarkkinalain muuttamisesta 116

maakaasumarkkinalain muuttamisesta 118
sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 27 ja 28 §:n muuttamisesta
..... 119
vesihuoltolain muuttamisesta 121
Finanssivalvonnasta annetun lain muuttamisesta 123

YLEISPERUSTELUT
1 Johdanto

Tieto- ja viestintäteknologia sekä niihin liittyvät palvelut muuttavat yhteiskunnan toimintaa sekä valtarakenteita mullistavalla tavalla. Esineiden internet, liikenteen älykkään automaation kehittyminen, massadatan hyödyntäminen sekä robotiikan ja erilaisten älyteknologioiden yleistyminen ovat esimerkkejä digitalisaatiokehityksen mahdollistamista teknologisista innovaatioista.

Digitalisaatio voi toimia taloudellisen toimeliaisuuden katalyyttinä. Teknologian kehitys mahdollistaa uudenlaisten asiakkaiden tarpeisiin räätälöityjen palveluiden tarjoamisen sekä taloudellisempien ja tehokkaampien toimintatapojen omaksumisen. Juha Sipilän hallituksen tavoitteena onkin digitalisaatiota edistämällä ottaa tuottavuusloikka julkisissa palveluissa ja yksityisellä sektorilla tarttumalla digitalisaation mahdollisuuksiin. Tämän toteuttamiseksi hallitusohjelman yhtenä kärkihankkeena rakennetaan digitaalisen liiketoiminnan kasvuympäristö.

Samaan aikaan, kun digitalisaatio mahdollistaa uusia innovaatioita ja toimintatapoja, tulevat yhä useammat palvelut merkittävämmin riippuvaisiksi viestintäverkkojen ja tietojärjestelmien luotettavasta toiminnasta. Tämä pätee myös esineisiin, laitteisiin ja kulkuneuvoihin, joista yhä suurempi osa on yhteydessä internetiin, ja joiden toimintaa ohjataan digitaalista tietoa käsittelemällä. Tämä kehitys vaikuttaa myös yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjontaan.

On todennäköistä, että yhteiskunnan keskeisiin palveluihin kohdistuvat perinteiset turvallisuusriskit pienenevät uusien teknologioiden ansiosta. Esimerkiksi liikenneonnettomuuksista noin 90 % voidaan katsoa johtuvan inhimillisestä virheestä. Liikenteen älykkään automaation myötä inhimillisen tekijän merkitys turvallisuudelle kuitenkin vähenee. Sen sijaan digitaalisten järjestelmien turvallisuuteen, luotettavuuteen ja tietosuojaan kohdistuu merkittäviä uudenlaisia haasteita. Fyysinen ja digitaalinen turvallisuus kietoutuvatkin yhä läheisemmin yhteen.

Suomalaisilla on vahva luottamus yhteiskunnan ja sen keskeisten palveluiden turvallisuuteen sekä viranomaisten toimintaan. Yhteiskunnan digitalisoituessa on ehdottoman tärkeää kasvattaa edelleen kansalaisten ja yritysten luottamusta digitaalisiin toimintatapoihin. Esimerkiksi robottiauton, verkkopankin tai digitaalisten terveyspalveluiden käyttäjän luottamus on ansaittava, jotta uudet palvelumuodot hyväksyttäisiin asiakkaiden taholta. Palvelun luotettavuutta on mahdollista hyödyntää kilpailuetuna kilpailijoihin nähden ja joidenkin palvelujen kohdalla se voi olla toiminnan harjoittamisen elinehto.

Tietoturvan varmistaminen onkin hallitusohjelman digitaalisen liiketoiminnan kasvuympäristön rakentamisen kärkihankkeen keskeinen tavoite.

Tietoturvallisuudentason kasvattaminen on tärkeää yhteiskunnan kokonaisturvallisuuden kannalta. Yhteiskunnan kannalta keskeisiin palveluihin kohdistuvat tietoturvallisuuteen liittyvät häiriöt voivat vaarantaa näiden keskeisten palveluiden turvallisuuden ja jatkuvuuden. Esimerkiksi tietojärjestelmien tietoturvallisuuteen liittyvät merkittävät häiriöt sähkön jakelussa voisivat vaikuttaa merkittävällä tavalla useimpien yhteiskunnan palveluiden tarjontaan. Yhteiskunnan toiminnan kannalta kriittisten palveluiden tietoturvallisuus on noussut vuoden 2017 alkupuolella sattuneiden laaja-alaisten kiristyshaittaohjelmatapausten seurauksena yhä keskei-

semmin esille. Haittaohjelmat ovat vaikeuttaneet esimerkiksi rautatiejärjestelmien, satamien, sairaaloiden sekä energiayhtiöiden toimintaan maailmalla.

Tietoturvallisuuteen liittyvistä häiriöistä voi lisäksi aiheutua merkittäviä taloudellisia seurauksia, niin yhteiskunnalle kuin yksittäisille kansalaisille ja yrityksille. Yksittäisten kansalaisten ja yritysten kannalta erityisen merkityksellisiä ovat häiriöt, joiden seurauksena ulkopuolinen taho, kuten tietoverkkorikolliset, voi päästä käsiksi heidän luottamuksellisiin tietoihinsa, kuten esimerkiksi verkkopalveluiden salasanoihin. Lisäksi haitallisia voivat olla häiriöt, joiden seurauksena palvelut, tai niissä säilytetyt tiedot, eivät ole käyttäjiensä käytettävissä. Häiriön aiheuttama taloudellinen vahinko voi johtua esimerkiksi omaisuuden vahingoittumisesta, yrityksen liiketoiminnan keskeytymisestä tai kuluista, jotka syntyvät vahingoilta suojautumisesta.

Tietoverkkorikollisuus, laajamittaiset yksityisyyden suojan loukkaukset sekä muut tietoturvallisuuteen liittyvät häiriöt ovat omiaan aiheuttamaan luottamuspulaa palveluiden käyttäjien parissa. Luottamuspulan kasvulla olisi merkittäviä taloudellisia vaikutuksia yhteiskunnalle, sillä luottamuspula voi jarruttaa markkinoiden kehitystä tai vaikuttaa muutoin haitallisilla tavoilla digitaalisten palveluiden käyttöön. Esimerkiksi Euroopan komission tilaaman Eurobarometritutkimuksen mukaan jopa 88 prosenttia haastatelluista 28 000 eurooppalaisesta kertoi muuttaneensa tapojaan käyttää internetiä tietoturvahuolien vuoksi. Kuluttajien käyttäytymisen muutokset voisivat myös hidastaa yleistä digitalisaatiokehitystä ja näin vaikuttaa haitallisesti hallitusohjelman digitalisaatioon liittyvien tavoitteiden toteutumiseen.

Tietoturvallisuuteen voi liittyä monenlaisia riskejä, jotka voivat aiheutua hyvin erilaisten syyyhteyksien seurauksena. Tietoturvariskin toteutuminen voi olla seurausta tahattomasta vahingosta (esimerkiksi tahaton virhe ohjelmoinnissa) tai tahallisesta oikeudettomasta teosta (esimerkiksi kiristyshaittaohjelman levittäminen).

Koska tietoturvallisuuteen liittyy erilaisia riskejä, voidaan näitä riskejä myös hallita monin erilaisin vaihtoehtoisin keinoin. Riskienhallintaan voidaan vaikuttaa esimerkiksi oikean toimintaympäristön valinnalla, riskienhallintasuunnitelmien laadinnalla, tietoturvan huomioimisella sopimussuhteissa, tai ottamalla käyttöön erityisiä luottamusta lisääviä palveluita, kuten esimerkiksi tunnistautumispalveluita, sähköisiä allekirjoituksia tai muita tiedon salaus- ja suojausmenetelmiä. Lisäksi luottamusta voidaan lisätä tunnettuja standardeja noudattamalla ja standardien edellyttämien toimien arvioinnilla ja todentamisella (auditoinnilla). Tietoturvariskejä voidaan myös vakuuttaa.

Tietoturvariskien hallinnassa keskeistä on tiedon jakaminen. Haavoittuvuuksia ja tietoturvaloukkauksia koskeva tieto voi koskettaa useita, myös eri toimialoilla toimivia, toimijoita. Kun tietoturvaan liittyviä häiriöitä koskevaa tietoja jaetaan vastavuoroisesti toimijoiden kesken, kaikki hyötyvät. Suomessa Viestintäviraston järjestämä vapaaehtoiseen tiedonvaihtoon ja luottamukseen perustuva tiedonjakaminen ja yhteistyö toimijoiden välillä ovat osoittautuneet menestykseksi, jota arvostetaan myös kansainvälisessä yhteisössä. Häiriöiden raportointia koskevilla lakisääteisillä velvoitteilla ei tule vaarantaa tätä vapaaehtoisuuteen ja molemminpuoliseen hyötyyn perustuvaa tiedonjakoa.

Kokonaisuutena korkealaatuisten ja luotettavien digitaalista tietoa hyödyntävien palveluiden tarjoaminen edellyttää tietoturva-asioiden kokonaisvaltaista huomioimista liiketoimintaa järjestettäessä. Tietoturva on huomioitava liiketoiminnan koko elinkaaren aikana. Verkko- ja tietoturvadirektiivin voimaan saattamista tukevan työryhmän loppuraportissa onkin tämä huomi-

oiden korostettu, että direktiivin mukaiset tietoturvariskienhallintaa koskevat velvoitteet tulisi pystyä ottamaan osaksi yrityksen normaalia riskien hallintaa.

Tämän hallituksen esityksen keskeinen tavoite on parantaa yhteiskunnan toiminnan kannalta keskeisten palveluiden tietoturvallisuutta. Tämä on edellä kuvatulla tavalla digitaalisen liiketoiminnan kasvuympäristön rakentamisen kannalta välttämätöntä. Lisäksi se on merkittävässä asemassa yhteiskunnan sisäisen turvallisuuden kasvattamiseksi.

Myös Euroopan unionin keskeisenä tavoitteena on lisätä luottamusta unionin digitaalisiin sisämarkkinoihin ja näin tehostaa sisämarkkinoiden toimintaa ja mahdollistaa merkittävää talouskasvua. Osana sisämarkkinoiden toiminnan parantamista Euroopan unionissa, jäljempänä *EU,* hyväksyttiin 6.7.2015 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, jäljempänä *verkko- ja tietoturvadirektiivi*. Verkko- ja tietoturvadirektiivi on saatettava kansallisesti voimaan 9.5.2018 mennessä.

Verkko- ja tietoturvadirektiivillä jäsenvaltiot velvoitetaan laatimaan kansallinen verkko- ja tietojärjestelmien turvallisuutta koskeva strategia sekä määrittämään direktiivistä johtuvia viranomaistehtäviä tietoturvallisuuden varmistamiseksi ja riskien hallitsemiseksi eri toimialoilla. Jäsenvaltiot velvoitetaan myös osallistumaan keskenään yhteistyöhön uusissa EU-tason yhteistyöryhmissä tietoturvaloukkauksia koskevien tietojen sekä parhaiden kansallisten käytäntöjen vaihtamiseksi.

Lisäksi jäsenvaltiot velvoitetaan määrittämään verkko- ja tietoturvadirektiivin soveltamisalan mukaisilla toimialoilla (energia-, liikenne- ja pankkiala, finanssimarkkinoiden infrastruktuurit, terveydenhuoltoala, juomaveden toimittaminen ja jakelu, digitaalinen infrastruktuuri) yhteiskunnan toiminnan kannalta keskeisten palvelujen tarjoajat, jotka ovat sijoittautuneet niiden alueelle. Direktiivin mukaan jäsenvaltioiden on velvoitettava nämä keskeisten palveluiden tarjoajat sekä direktiivissä erikseen määritellyt digitaalisen palvelun tarjoajat (verkossa toimiva markkinapaikka, verkossa toimiva hakukone sekä pilvipalvelu) hallitsemaan verkko- ja tietojärjestelmiensä turvallisuuteen kohdistuvia riskejä sekä raportoimaan verkko- ja tietojärjestelmiin liittyvistä poikkeamista valvovalle viranomaiselle.

Vaikka Suomessa lainsäädäntö turvaa jo nykyisin verrattain korkeatasoisen tietosuojan ja tietoturvan tason, on lainsäädäntöä edelleen tarpeen kehittää tukemaan parhaalla mahdollisella tavalla luottamuksen kasvattamista digitaalisiin toimintatapoihin sekä kasvattamaan yhteiskunnan keskeisten palveluiden turvallisuutta huomioiden verkko- ja tietoturvadirektiivin vaatimukset.

Nykyinen lainsäädäntömme muodostaa yritystoiminnalle kilpailuedun niihin valtioihin nähden, joissa luottamusta ei samalla tavalla ole pystytty rakentamaan. Kilpailuedun säilyttäminen sekä hallitusohjelman mukaisen säädösten sujuvoittamisen kärkihankkeen tavoitteet onkin huomioitu tämän ehdotuksen laadinnassa.

Lisäksi ehdotettu lainsäädäntö voi luoda edellytyksiä luotettavasti digitalisoitujen hyödykkeiden uusien markkinoiden kehittymiselle. Samalla ehdotettu lainsäädäntö parantaa osaltaan julkishallinnon mahdollisuuksia järjestää kansalaisille turvallisempia jokapäiväisiä palveluita, joiden toteuttamisessa on tehokkaasti hyödynnetty digitalisaation tuomia mahdollisuuksia.

2 Nykytila

2.1 Lainsäädäntö ja käytäntö

2.1.1 Yleistä

Tietoturvallisuutta koskevaa lainsäädäntöä ei ole Suomessa koottu yhteen lakiin vaan sitä sisältyy useisiin niin julkista hallintoa kuin erilaisten palveluiden tarjontaa koskeviin säädöksiin. Tietoturvallisuutta koskeva lainsäädäntö sisältää yhtäältä sääntelyä siitä, miten tietyntyyppisiä tietoja tulee käsitellä tietoturvallisesti. Esimerkkejä tällaisesta sääntelystä ovat säännökset henkilötietojen ja turvallisuusluokiteltujen asiakirjojen käsittelystä. Toisaalta tietoturvallisuutta koskevaa lainsäädäntöä sisältyy julkishallinnon sekä yksityisten palveluntarjoajien toiminnan järjestämiseen liittyvään lainsäädäntöön, koskien esimerkiksi toiminnan riskienhallintaa ja jatkuvuutta. Osa tietoturvallisuutta koskevista velvoitteista koskee lähtökohtaisesti vain julkista hallintoa, osa sen sijaan esimerkiksi tiettyjä yksityisten palveluiden tarjoajia.

Tietoturvariskienhallintaan liittyviä velvoitteita sisältyy hallinnon yleislakeihin (viranomaisten toiminnan julkisuudesta annettu laki (621/1999), henkilötietolaki (523/1999)), yleiseen palveluntarjoajien laatuvaatimuksia tai turvallisuusvelvoitteita koskevaan lainsäädäntöön (esimerkiksi tietoyhteiskuntakaaren (917/2014) säännökset viestintäpalvelujen ja viestintäverkkojen tietoturvallisuutta koskien sekä liikenteen turvallisuuteen liittyvät velvollisuudet), liiketoiminnan riskienhallintaa koskevaan lainsäädäntöön (esimerkiksi luottolaitosten operatiivista riskienhallintaa koskeva sääntely) sekä häiriöihin varautumiseen koskevaan lainsäädäntöön (esimerkiksi vesihuoltolaitoksen häiriöihin varautumisvelvoite). Velvoitteiden sisältö vaihtelee toimialoittain. Lainsäädännön lisäksi yhteiskunnan turvallisuuden, kyberturvallisuuden ja tietoturvallisuuden edistämistä ohjaavat useat toisiaan täydentävät strategiat. Tietoturvallisuuden kasvattamiseen tähtääviä toimenpiteitä on linjattu kokoavasti hallituksen toimintasuunnitelman mukaisesti hyväksytyssä Suomen tietoturvallisuusstrategiassa sekä valtioneuvoston periaatepäätöksenä annetussa kyberturvallisuusstrategiassa. Yhteiskunnan turvallisuusstrategiassa on lisäksi määritelty yhteiskunnan elintärkeät toiminnot.

2.1.2 Suomen tietoturvallisuusstrategia ja kyberturvallisuusstrategia

Suomen tietoturvallisuusstrategia hyväksyttiin liikenne- ja viestintäministerin päätöksellä 10.3.2016. Strategia painottuu kilpailukyvyn ja vientiedellytysten varmistamiseen, EU:n digitaalisten sisämarkkinoiden kehittämiseen sekä yksityisyyden suojan ja muiden perusoikeuksien turvaamiseen.

Strategiatyön puitteet on määritelty pääministeri Juha Sipilän hallituksen hallitusohjelman toimintasuunnitelmassa ja esitelty strategian johdannossa. Strategian visio on laadittu näistä lähtökohdista kumpuavien tavoitteiden ja painopisteiden mukaiseksi.

Hallitusohjelman lisäksi strategian sisältöön ovat vaikuttaneet verkko- ja tietoturvadirektiiviehdotuksessa strategialle asetetut vaatimukset. Strategiassa tarkastellaan verkko- ja tietoturvadirektiivin edellyttämällä tavalla tietoturvaan liittyvää osaamista ja yleisen tietoisuuden kehittämistä sekä tutkimus- ja kehitystyön merkitystä. Riskienhallinnan ja niiden tunnistamisen osalta strategian keskeinen viesti on, että toimijoilla on oltava mahdollisuus arvioida tietoturvatoimenpiteitään riskiperusteisesti eli suhteuttaa ne osaksi liiketoimintansa muiden riskien hallintaa. Julkisen ja yksityisen sektorin välistä yhteistyötä verkko- ja tietoturvallisuuteen liit-

tyvässä ennaltaehkäisyssä, reagoinnissa ja korjaavissa toimenpiteissä on myös käsitelty useissa strategian toimenpiteissä.

Strategia on jatkumoa vuosien 2003 ja 2008 tietoturvastrategioille sekä vuoden 2013 kyberturvallisuusstrategialle. Strategia painottuu toimeksiantonsa mukaisesti erityisesti digitaaliseen liiketoimintaan sekä verkko- ja tietoturvadirektiivistä seuraaviin strategisiin vaatimuksiin.

Myös verkko- ja tietoturvadirektiivin kansallisen täytäntöönpanon keskeiset tavoitteet on määritelty tietoturvastrategiassa. Strategian mukaan direktiivin täytäntöönpanon yhteydessä turvataan yritysten mahdollisuudet sovittaa tietoturvariskien hallintaan liittyvät uudet velvoitteet osaksi muiden liiketoiminnan riskiensä hallintaa.

Valtioneuvoston periaatepäätöksenä vuonna 2013 annetulla Suomen kyberturvallisuusstrategian tavoitteena on luoda yhteinen ymmärrys kyberturvallisuudesta ja vahvistaa yhteiskunnan kokonaisturvallisuutta. Strategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. Turvallisuuskomitean 20.4.2017 julkaisemassa kyberturvallisuusstrategian toimeenpano-ohjelmassa vuosille 2017–2020 on tarkemmin kuvattu toimenpiteet strategian täytäntöönpanemiseksi. Osana toimeenpano-ohjelmaa täytäntöönpannaan liikenne- ja viestintäministeriön hyväksymä tietoturvastrategia. Kyberturvallisuusstrategia ja tietoturvastrategia täydentävät näin toisiaan.

2.1.3 Yhteiskunnan toiminnan kannalta keskeiset toiminnot

Kriittistä infrastruktuuria tai yhteiskunnan toiminnan kannalta keskeisiä toimintoja ei ole määritelty Suomessa varsinaisesti lainsäädännön tasolla. Sen sijaan yhteiskunnan elintärkeät toiminnot on määritelty yhteiskunnan turvallisuusstrategiassa.

Valtioneuvosto hyväksyi lokakuussa 2017 periaatepäätöksen yhteiskunnan turvallisuusstrategiaksi. Strategiassa määritellään yhteiskunnan elintärkeät toiminnot. Strategian mukaan suomalaisen yhteiskunnan elintärkeitä toimintoja ovat valtion johtaminen, kansainvälinen ja EU-toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön toimintakyky ja palvelut sekä henkinen kriisinkestävyys.

Strategian mukaan elintärkeissä toiminnoissa välttämättömät tieto- ja viestintäjärjestelmät, digitaaliset palvelut ja tiedot turvataan julkisen hallinnon ja yhteisöjen käytettävissä olevissa toimitiloissa. Toimiva tieto- ja kyberhäiriötilanteiden hallintamalli huomioi Euroopan unionin verkko- ja tietoturvasäännösten velvoitteet.

Lisäksi Valtioneuvosto on antanut huoltovarmuudesta annetun lain (1390/1992) 2 §:n mukaisesti päätöksen maan huoltovarmuuden tavoitteista (VNp 857/2013) jäljempänä *huoltovarmuuspäätös*. Päätöksen mukaan keskeisiä yhteiskunnan toimintakykyä vaarantavia uhkia ovat tieto- ja viestintäjärjestelmien sekä -verkkojen häiriintyminen, energiansaannin keskeytyminen, väestön terveyden ja toimintakyvyn vakava häiriintyminen sekä luonnon- ja ympäristöonnettomuudet. Päätöksessä kriittisen infrastruktuurin turvaaminen on jaettu seuraavasti:

1) Energian tuotanto-, siirto ja jakelujärjestelmät

2) Tieto- ja viestintäjärjestelmät, -verkot ja -palvelut

3) Finanssialan palvelut

4) Liikenne ja logistiikka

5) Vesihuolto

6) Infrastruktuurin rakentaminen ja kunnossapito sekä

7) Jätehuolto erityistilanteissa

Päätöksessä todetaan lisäksi, että kriittisimmät ja keskeisimmät tietotekniikan varassa olevat yhteiskunnan toiminnot tulee tunnistaa ja niihin liittyvät tietojärjestelmäratkaisut ja -palvelut tulee varmistaa erilaisia vakavia häiriöitä ja poikkeusoloja kestävillä järjestelyillä.

2.1.4 Palvelujen tarjoajien toimintaan liittyvät laatu- ja riskienhallintavaatimukset sekä turvallisuuteen liittyvistä häiriöistä ilmoittaminen viranomaisille

Kuten edellä on todettu, yhteiskunnan toiminnan kannalta keskeiset palvelut ovat yhä riippuvaisempia tietoverkkojen ja -järjestelmien luotettavasta toiminnasta. Lisäksi digitaalista tietoa hyödynnetään kiihtyvällä tahdilla palveluiden tarjoamiseen. Monilla yhteiskunnan toiminnan kannalta keskeisillä toimialoilla on palveluiden tarjoajia ja käyttäjiä koskevia lakisääteisiä velvoitteita, joilla turvataan toiminnan laatu ja turvallisuus. Lakisääteisten laatuvaatimusten taustalla on arvopunninnan keinoin määritelty tarve hallita toiminnan yhteiskunnallisesti merkittäviä vaikutuksia.

Seuraavaksi tarkastellaan tarkemmin voimassa olevaan lainsäädäntöön sisältyviä turvallisuusriskien hallintaan liittyviä velvoitteita verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvilla toimialoilla. Verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvat toimialat direktiivin liitteen II mukaisesti digitaalinen infrastruktuuri, liikenne, energia, pankkiala, finanssimarkkinoiden infrastruktuuri, terveydenhuolto sekä juomaveden toimittaminen ja jakelu. Liitteessä II jotkin näistä toimialoista on lisäksi jaoteltu toiminnan osa-alueisiin. Liitteessä kaksi on lisäksi kaikkien toimialojen osalta lueteltu toimijoiden tyyppejä.

Digitaalinen infrastruktuuri

Digitaalisen infrastruktuurin osalta verkko- ja tietoturvadirektiivin liitteessä II ei ole määritelty tarkempia toiminnan osa-alueita, mutta toimijoiden tyyppeinä on mainittu internetin yhdysliikennepisteet (Internet exchange point, IXP), nimipalvelujen tarjoajat sekä aluetunnusrekisterit. Suomessa digitaalista infrastruktuuria koskeva sääntely sisältyy keskeisin osin tietoyhteiskuntakaareen. Tietoyhteiskuntakaaressa säädetään sähköisen viestinnän ja tietoyhteiskunnan palvelujen tarjonnasta. Tietoyhteiskuntakaaren 29 luvussa säädetään viestintäverkkojen ja -palvelujen laatuvaatimuksista. Lain 243 §:n mukaan yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä siten, että sähköinen viestintä on tekniseltä laadultaan hyvää ja tietoturvallista. Tietoturvalla tietoyhteiskuntakaaressa tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Lisäksi viestintäverkkojen ja -palvelujen tulee kestää normaalit odotettavissa olevat tietoturvauhat, niiden laatua ja toimintavarmuutta tulee voida seurata, niihin kohdis-

tuvat merkittävät tietoturvaloukkaukset ja -uhat sekä niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt tulee voida havaita eikä kenenkään tietosuojan, tietoturvan tai muiden oikeuksien tule vaarantua.

Tietoyhteiskuntakaaren 246 §:n mukaan sähköisen viestintäpalvelun tilaaja tai käyttäjä ei saa liittää yleiseen viestintäverkkoon muita kuin toimintakuntoisia ja tietoyhteiskuntakaaren vaatimusten mukaisia radio- ja telepäätelaitteita. Lisäksi tilaajan on ylläpidettävä yleiseen viestintäverkkoon liitettävää laitetta tai järjestelmää teleyrityksen antamien ohjeiden mukaisesti siten, ettei se vaaranna yleisen viestintäverkon ja -palvelun tietoturvallisuutta.

Tietoyhteiskuntakaaren X osassa säädetään viestinnän ja palvelujen jatkuvuuden turvaamisesta ja sen 33 luvussa säädetään tietoturvan ja häiriöiden hallinnasta sekä häiriöistä ilmoittamisesta. Luvussa säädetään niistä toimenpiteistä, joihin teleyrityksellä, yhteisötilaajalla ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus ryhtyä tietoturvasta huolehtimiseksi, teleyrityksen tai muun viestintäverkon tai laitteen haltijan velvollisuudesta korjata häiriö, teleyrityksen ja lisäarvopalvelun tarjoajan velvollisuudesta tehdä häiriöilmoituksia käyttäjille ja viranomaisille.

Tietoyhteiskuntakaaren 275 §:n mukaan teleyrityksen on ilmoitettava viipymättä Viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Teleyrityksen on ilmoitettava myös ilman aiheetonta viivästystä häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään.

Tietoyhteiskuntakaaressa teleyrityksellä tarkoitetaan sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa. Teletoiminnan sääntely on teknologianeutraalia ja se voi olla vastikkeellista tai vastikkeetonta. Yleinen teletoiminta tarkoittaa sähköisten viestintäpalvelujen tarjontaa ennalta rajaamattomalle käyttäjäpiirille.

Internetin yhdysliikennepisteet tarjoavat vähimmillään teknisen paikan (point of presence) autonomisten AS-tunnuksella yksilöityjen viestintäverkkojen välisen liikenteen vaihtamiseen. Yhdysliikennepisteen tarjoaja voi myös tarjota palveluja yhteenliittämisen sopimiseksi.

Viestintävirasto on tulkinnut internetin yhdysliikennepisteen tietoyhteiskuntakaaren tarkoittamaksi yleiseksi teletoiminnaksi ainakin siltä osin, kun niitä käytetään yleisten viestintäverkkojen yhteenliittämiseen. Yhdysliikennepistettä voivat käyttää myös muut kuin yleisiä viestintäverkkoja tarjoavat teleyritykset, tyypillisesti esimerkiksi hajautettujen sisältöverkkojen (content delivery network, CDN) haltijat.

Nimipalvelun (Domain Name System, DNS) tarjoaminen on voimassa olevan sääntelyn mukaan yleistä teletoimintaa tai muuta toimintaa riippuen siitä, liittykö se internetyhteyspalvelun tarjontaan vai ei. Silloin kun se on osa internetyhteyspalvelun tarjoamista, sitä koskee yleistä teletoimintaa koskeva sääntely ja määräykset. Nimipalvelua tarjotaan myös muuten kuin internetyhteyspalvelun osana. Sitä tarjoavat esimerkiksi verkkotunnusvälittäjät ja muut verkon palveluntarjoajat. Nimipalvelua ei tyypillisesti hankita erikseen vaan se hankitaan osana muuta palvelua.

Suomen lainsäädäntövaltaan kuuluvista fi-maatunnusta ja ax-maakuntatunnusta koskevista verkkotunnusrekistereistä säädetään tietoyhteiskuntakaaressa. Viestintävirasto ylläpitää rekisteriä fi-maatunnukseen päättyvistä verkkotunnuksista ja tietokantaa verkkotunnusten teknisistä tiedoista internetliikenteen ohjaamista varten (fi-juuri). Ahvenanmaan maakuntahallitus ylläpitää ax-juurta.

Tietoyhteiskuntakaaren 21 luvussa säädetään verkkotunnuksista. Lain 171 §:ssä säädetään verkkotunnushallinnon järjestämisestä. Pykälän mukaan Viestintäviraston tehtävänä on huolehtia fi-verkkotunnustoiminnan tietoturvasta. Lisäksi lain 172 §:n mukaan Viestintävirastolla on oikeus ryhtyä välttämättömiin toimiin fi-verkkotunnuksia hyödyntämällä toteutettaviin yleisiin viestintäverkkoihin tai -palveluihin taikka niiden käyttäjiin kohdistuvien merkittävien tietoturvaloukkausten havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Viranomaisen toimintaa verkkotunnusrekisterin ja juuren ylläpidossa koskevat tietoyhteiskuntakaaren lisäksi viranomaisten toiminnan julkisuudesta annetussa laissa sekä sen nojalla annetun valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010), jäljempänä *tietoturva-asetus*, tietoturvavaatimukset.

Energia

Energian toimialue on jaettu verkko- ja tietoturvadirektiivin liitteessä II sähkön, öljyn sekä kaasun osa-alueisiin. Näiden osa-alueiden osalta riskienhallintaan liittyviä velvoitteita sisältyy ainakin sähkömarkkinalakiin (588/2013), maakaasumarkkinalakiin (587/2017) sekä öljyn osalta vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annettuun lakiin (2005/390). Myös ydinenergialakiin (990/1987) sisältyy riskienhallintaan liittyvää lainsäädäntöä, mutta ydinenergia ei kuulu verkko- ja tietoturvadirektiivin soveltamisalaan.

Sähkö

Sähkönjakelun kantaverkko on suunniteltava ja rakennettava, ja sitä on ylläpidettävä siten, että verkko täyttää Euroopan unionin lainsäädännössä asetetut verkon käyttövarmuutta ja luotettavuutta koskevat vaatimukset ja järjestelmävastaavalle kantaverkonhaltijalle sähköverkkoluvassa asetetut verkon käyttövarmuutta ja luotettavuutta koskevat ehdot.

Sähköalan yrityksiä, jakeluverkonhaltijoita sekä siirtoverkonhaltijoita koskevat sähkömarkkinalain mukainen verkon kehittämisvelvollisuus (19 §), varautumissuunnitteluvelvoite (28 §), verkonhaltijan yhteistoimintavelvollisuus häiriötilanteissa (29§). Lisäksi sähköalan yrityksiä sekä jakeluverkonhaltijoita koskevat jakeluverkon toiminnan laatuvaatimukset (50–52 §).

Sähkömarkkinalain 28 §:n mukaan verkonhaltijan on asianmukaisella suunnittelulla varauduttava normaaliolojen häiriötilanteisiin ja valmiuslaissa (1552/2011) tarkoitettuihin poikkeusoloihin. Verkonhaltijan on laadittava varautumissuunnitelma sekä osallistuttava tarpeellisessa laajuudessa huoltovarmuuden turvaamiseen tähtäävään valmiussuunnitteluun.

Sähkömarkkinalain 59 §:n mukaan jakeluverkonhaltijan on tiedotettava verkon käyttäjille, mikäli sähkönjakelu keskeytyy jakeluverkossa merkittävässä laajuudessa. Samalla on annettava arvio vian tai keskeytyksen kestosta ja laajuudesta.

Maakaasu

Maakaasumarkkinalakiin sisältyy vain joitakin turvallisuusriskienhallintaa sivuavia velvoitteita. Uudistettu maakaasumarkkinalaki tulee voimaan vuoden 2018 alusta. Lain 4 luvussa säädetään verkonhaltijan yleisistä velvollisuuksista. Lain 27 §:ssä säädetään verkonhaltijan varautumissuunnittelusta. Lain mukaan verkonhaltijan on asianmukaisella suunnittelulla varauduttava maakaasuverkkoonsa kohdistuviin normaaliolojen häiriötilanteisiin, maakaasujärjestelmässä ilmenevien maakaasunsaannin häiriöiden edellyttämien säännöstelytoimenpiteiden täytäntöönpanoon ja valmiuslaissa tarkoitettuihin poikkeusoloihin. Verkonhaltijan on laadittava varautumissuunnitelma sekä osallistuttava tarpeellisessa laajuudessa huoltovarmuuden turvaamiseen tähtäävään valmiussuunnitteluun.

Öljy

Vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetussa laissa ja sen nojalla annetussa valtioneuvoston asetuksessa vaarallisten kemikaalien teollisen käsittelyn ja varastoinnin valvonnasta (658/2015) säädetään muun muassa vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuusvaatimuksista, onnettomuuksien ehkäisemisestä sekä onnettomuuksien ja vaaratilanteiden ilmoittamisesta viranomaisille.

Liikenne

Liikenteen osalta verkko- ja tietoturvadirektiivin liitteessä II on määritelty neljä osa-aluetta: lentoliikenne, rautatieliikenne, vesiliikenne sekä tieliikenne. Liikennettä koskeva kansallinen turvallisuusriskienhallintaan liittyvä lainsäädäntö pohjautuu usein joko kansainvälisiin sopimuksiin taikka EU:n tasolla harmonisoituun lainsäädäntöön. Liikennettä koskeva lainsäädäntö on usein liikennemuotokohtaista ja sääntely voi koostua useiden eri kansainvälisten sopimusten, EU-tason sääntelyn sekä kansallisen sääntelyn yhdistelmästä.

Lentoliikenne

Ilmailu on kansainvälistä toimintaa ja siten siviili-ilmailualan sääntely perustuu yhteisiin sääntöihin, jotka on sovittu Kansainvälisen siviili-ilmailujärjestön (ICAO), Euroopan unionilainsäädännön, Euroopan lentoturvallisuusviranomaisen (EASA), Euroopan lennonvarmistusjärjestön eli Eurocontrolin ja Euroopan siviili-ilmailukonferenssin (ECAC) puitteissa. Kansallista liikkumavaraa siviili-ilmailun ja lentoliikenteen sääntelyssä on vähän.

Kansainvälisten ilmailusopimusten peruslähtökohtina ovat olleet turvallisuus, tehokkuus ja taloudellisuus. Kansainvälisen siviili-ilmailun yleissopimuksen (Chicagon yleissopimuksen) (SopS 11/1949) 37 artiklassa asetetaan ICAO:lle tehtäväksi hyväksyä ja tarvittaessa muuttaa kansainvälisiä standardeja, suositettuja menetelmiä ja menettelytapoja ilmailun turvallisuuteen, säännöllisyyteen ja tehokkuuteen liittyen.

Euroopan unionin ilmailualan lainsäädäntö on annettu viime vuosina enenevässä määrin asetustasolla direktiivien sijasta. Näin on pyritty varmistamaan se, että ilmailualan lainsäädäntöä sovelletaan Euroopan unionin jäsenvaltioissa mahdollisimman yhdenmukaisella tavalla.

Lentotoiminnan yleisistä edellytyksistä on säädetty yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan lentoturvallisuusviraston perustamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 216/2008, jäljempänä *EASA-asetus,* 8 artiklassa, asetuksen liitteissä IV (8 artiklassa tarkoitetut lentotoimintaa koskevat keskeiset vaatimukset), V a (lento-

paikkoja koskevat keskeiset vaatimukset) ja V b (ilmaliikenteen hallintaa ja lennonvarmistuspalveluja sekä lennonjohtajia koskevat keskeiset vaatimukset) sekä asetuksen nojalla annetuissa täytäntöönpanoasetuksissa. Komissio on antanut ehdotuksen EASA-asetuksen uudistamiseksi ((COM(2015) 613 FINAL) ja ehdotusta käsitellään parhaillaan unionissa.

EU-lainsäädännön vaatimuksilla ja niiden täytäntöönpanemiseksi hyväksytyillä säännöillä varmistetaan, että jäsenvaltiot täyttävät Chicagon yleissopimuksen mukaiset velvoitteensa. EASA-asetuksella, sen liitteillä ja asetuksen perusteella annetuilla täytäntöönpanosäännöillä säädetään verrattain kattavista turvallisuusriskienhallintavelvoitteista koskien lentotoiminnan harjoittajaa, lentopaikkoja sekä ilmaliikenteen hallintaa, lennonvarmistuspalveluja sekä lennonjohtoa.

Poikkeamien ilmoittamisesta, analysoinnista ja seurannasta siviili-ilmailun alalla annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) N:o 376/2014, jäljempänä *poikkeama-asetus*, säädetään ilmailun turvallisuuteen vaikuttavien poikkeamien ilmoittamisesta toimivaltaiselle viranomaiselle.

Asetuksen 4 artiklassa säädetään pakollisesta ilmoittamisvelvollisuudesta poikkeamista, jotka voivat muodostaa merkittävän riskin ilmailun turvallisuudelle. Ilmoittaminen on pakollista poikkeamista, jotka liittyvät esimerkiksi ilma-aluksen toimintaan, ilma-aluksen tekniseen kuntoon, huoltoon ja korjaukseen, lennonvarmistuspalveluihin ja -laitteisiin sekä lentopaikkoihin ja maapalveluihin.

Kansallisella tasolla ilmailun sääntelyä täydentää ilmailulaki (864/2014). Ilmailulakiin sisältyy kuitenkin vain muutamia turvallisuuteen liittyviä vaatimuksia liittyen esimerkiksi lentokelpoisuuden ylläpitämiseen (33 ja 34 §), lentoaseman hyväksymistodistukseen (83 §), maahuolintapalvelujen tarjoamiseen (93 §) sekä varautumiseen poikkeusoloihin ja häiriötilanteisiin (160 §).

Ilmailulain 118 §:n mukaan siviili-ilmailun onnettomuudesta ja vakavasta vaaratilanteesta on ilmoitettava Liikenteen turvallisuusvirastolle. Lain 125 §:n 1 momentin mukaan EU:n poikkeama-asetusta sovelletaan Suomessa kaikkiin ilma-aluksiin. Saman pykälän 2 momentin mukaisesti poikkeamista, joissa osallisena on Suomessa rekisteröity tai Suomeen sijoittautuneen organisaation käyttämä ilma-alus, on ilmoitettava siten kuin poikkeama-asetuksessa säädetään myös silloin, kun ne ovat tapahtuneet ulkomailla. Liikenteen turvallisuusvirasto vastaa ja ylläpitää poikkeama-asetuksen mukaista ilmoitusjärjestelmää, johon ilmoitetaan pakolliset ja vapaaehtoiset poikkeamatiedot (126 §).

Liikenteen turvallisuusvirasto on antanut ilmailuohjeen (GEN TI-4), jossa kuvataan tarkemmat menettelyt ja ohjeet, joita noudatetaan ilmailun onnettomuuksista, vakavista vaaratilanteista ja poikkeamisesta ilmoittamisessa, analysoinnissa ja seurannassa.

Rautatieliikenne

Rautateiden turvallisuudesta on säädetty yleisesti EU:n laajuisesti koskien viranomaisia ja toimijoita. Säädöksissä on asetettu vaatimukset mm. turvallisuusjohtamisjärjestelmälle, ilmoitusvelvollisuudelle ja valvonnalle. Keskeiset EU-tason säädökset ovat rautateiden turvallisuudesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/798 rautatieyritysten, turvallisuustodistuksen tai turvallisuusluvan saaneiden infrastruktuurin haltijoiden sekä kun-

nossapidosta vastaavien yksiköiden soveltamasta omavalvontaa koskevasta yhteisestä turvallisuusmenetelmästä annettu komission asetus (EU) N:o 1078/2012 sekä yhteisestä turvallisuusmenetelmästä kansallisten turvallisuusviranomaisten turvallisuustodistuksen tai turvallisuusluvan myöntämisen jälkeen harjoittamaa valvontaa varten annettu komission asetus (EU) N:o 1077/2012. Kansallisesti rautateiden turvallisuudesta on säädetty rautatielailla (304/2011), valtioneuvoston asetuksella ja Liikenteen turvallisuusviraston määräyksellä.

Rautatielain 6 luvussa on säädetty rautatiejärjestelmän turvallisuudesta. Lain 39 §:n mukaan rautatiejärjestelmän turvallisuustaso on säilytettävä ja sitä on kehitettävä Euroopan unionin lainsäädännön ja alan teknisen ja tieteellisen kehityksen mahdollistamalla tavalla. Pykälän mukaan rataverkon haltija ja rautatieliikenteen harjoittaja vastaavat rautatiejärjestelmän turvallisesta käytöstä ja käyttöön liittyvien riskien hallinnasta. Lain 40 §:n mukaan rautatieliikenteen harjoittajalla ja rataverkon haltijalla on oltava rautatieturvallisuutta koskevien säännösten ja määräysten mukainen turvallisuusjohtamisjärjestelmä. Lain 75 §:n mukaan Liikenteen turvallisuusvirasto voi rautatiejärjestelmän turvallisuuden ja teknisen toimivuuden varmistamiseksi antaa tarkempia määräyksiä mm. turvallisuusjohtamisjärjestelmästä ja varautumisesta onnettomuuteen tai vaaratilanteeseen. Liikenteen turvallisuusvirasto on antanut määräyksen rautatieliikenteen harjoittajan ja rataverkon haltijan turvallisuusjohtamisjärjestelmästä.

Rautatielain 79 §:n mukaan rautatieliikenteen harjoittajan ja rataverkon haltijan on riittävällä tavalla varauduttava rautateitä uhkaavan vaaran tai onnettomuuden varalta. Lisäksi 81 §:n mukaan turvallisuustodistuksen tai -luvan haltijoiden on varauduttava poikkeusoloihin ja huolehdittava siitä, että niiden toiminta jatkuu mahdollisimman häiriöttömästi myös valmiuslaissa tarkoitetuissa poikkeusoloissa ja niihin rinnastettavissa normaaliolojen häiriötilanteissa.

Rautatielain 81 a §:ssä säädetään toimenpiteistä, jotka rataverkon haltijan on toteutettava, jos rautatiejärjestelmässä esiintyy teknisistä ongelmista tai onnettomuudesta johtuvia häiriöitä tilanteen palauttamiseksi ennalleen.

Rautatielain 82 §:n mukaan rautatieliikenteen harjoittajien ja rataverkon haltijoiden tulee ilmoittaa Liikenteen turvallisuusvirastolle niiden tietoon tulleista onnettomuuksista ja vaaratilanteista. Lain mukaan nämä tiedot ovat salassa pidettäviä.

Valtioneuvoston asetuksella rautatiejärjestelmän turvallisuudesta ja yhteentoimivuudesta (372/2011) säädetään tarkemmin ilmoitusvelvollisuudesta.

Vesiliikenne

Merenkulun kansainvälisen sääntelyn pohjana ovat Yhdistyneiden kansakuntien alaisen Kansainvälisen merenkulkujärjestön (IMO) yleissopimukset. Keskeisiä kansainvälisiä yleissopimuksia ovat meriturvallisuutta sääntelevä vuoden 1974 kansainvälinen yleissopimus ihmishengen turvallisuudesta merellä (SOLAS (International Convention for the Safety of Life at Sea) -yleissopimus (SopS 11/1981)) sekä ympäristönsuojelua koskeva vuoden 1978 pöytäkirja, joka liittyy vuonna 1973 tehtyyn kansainväliseen yleissopimukseen alusten aiheuttaman meren pilaantumisen ehkäisemisestä (MARPOL (International Convention for the Prevention of Pollution from Ships)-yleissopimus).

Riskienhallintaan liittyviä velvoitteita on yhtiöiden (varustamot) osalta kansainvälisessä turvallisuusjohtamissäännöstössä (International Safety Management Code, ISM-säännöstö), joka

perustuu SOLAS-yleissopimukseen. EU:n alueella säännöstö on toimeenpantu kansainvälisen turvallisuusjohtamissäännöstön täytäntöönpanosta yhteisössä annetulla Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 336/2006. Myös poikkeamaraportointijärjestelmä sisältyy ISM-säännöstön vaatimuksiin. Poikkeamaraportoinnin perusteena on, että analysoimalla läheltä piti -tilanteita ja vähäisiä onnettomuuksia sekä toteuttamalla ennakoivia korjaustoimenpiteitä voidaan pienentää vakavan onnettomuuden riskiä.

Lisäksi kaupallisen merenkulun onnettomuuksien raportointivelvoitteesta Liikenteen turvallisuusvirastolle on säädetty merilailla (674/1994). Lain mukaan merionnettomuusilmoitus on annettava merilain 18 luvun 6 ja 8 pykälissä tarkoitetuissa tapauksissa. Saman luvun 15 §:ssä säädetään onnettomuudesta ja vaaratilanteesta ilmoittamisesta. Alusturvallisuuden valvonnasta annetun lain (370/1995) 20 §:n mukaan valvontaviranomaiselle on tehtävä, mikäli mahdollista, kirjallinen ilmoitus alusturvallisuutta koskevan säännöksen tai määräyksen rikkomisesta.

Alusliikennepalvelu

Alusliikennepalvelulaissa (623/2005) säädetään eräistä merenkulkuun liittyvistä liikenteenohjaustehtävistä, joista vastaava viranomainen (VTS-viranomainen) on lain mukaan Liikennevirasto (2 §:n 1 ja 4 kohta). Lain 19 §:n mukaan VTS-viranomaisen on pidettävä toimintakäsikirjaa, jossa on määritelty VTS-keskuksen toiminnan ja teknisten järjestelmien ylläpitämiseen liittyvät tehtävät ja toimenpiteet sekä varautuminen alusliikennepalvelun ylläpitämiseen poikkeustilanteissa. Toimintakäsikirjassa on määriteltävä luotsauslaissa säädettyjä velvoitteita koskevat menettelytavat, ilmoituskäytännöt ja yhteistyö Liikenteen turvallisuusviraston kanssa.

Lain 20 a §:ssä on säädetty merenkulun tiedonhallintajärjestelmästä ja sille asetutuista vaatimuksista. Pykälän mukaan Liikennevirasto antaa tarkempia määräyksiä tiedonhallintajärjestelmän ilmoitusmenettelyistä, rakenteesta, sisällöstä, käyttöoikeuksista, tietojen jakelusta viranomaisille ja tietojen vaihdosta muiden jäsenvaltioiden sekä Euroopan unionin merenkulun tiedonhallintajärjestelmän (SafeSeaNet-keskusjärjestelmän) kanssa.

VTS-viranomaisella on velvollisuus ilmoittaa asianomaisille merenkulku-, meripelastus-, ympäristö-, aluevalvonta-, poliisi- tai tulliviranomaisille sekä asianomaisille satamanpitäjille havaitsemistaan tai sille ilmoitetuista tiettyä alusta koskevista aluksen tai siinä olevien ihmisten turvallisuuteen, meripelastukseen, ympäristönsuojeluun tai alue- taikka tullivalvontaan liittyvistä olennaisista seikoista (18 §). Lisäksi aluksen päällikön on Suomen vesialueella ilmoitettava VTS-viranomaiselle kaikista aluksen turvallisuuteen vaikuttavista tai merenkulun turvallisuutta vaarantavista vaaratilanteista tai onnettomuuksista sekä kaikista tilanteista, jotka voivat aiheuttaa vesien tai rannikon pilaantumista ja kaikista merellä ajelehtivista ympäristöstä pilaavien aineiden laitoista sekä konteista ja pakkauksista (23 §).

Satamat

Satamien osalta turvavelvoitteita on ISPS (International Ship and Port Facility Security Code) -säännöstössä, jonka tavoitteena on lisätä turvallisuutta aluksilla ja satamissa. Säännöstön on laatinut Kansainvälinen merenkulkujärjestö IMO. ISPS-säännöstö on myös liitetty kansainväliseen SOLAS-sopimukseen (luku XI-2 "Special measures to enhance maritime security") ja se on toimeenpantu EU:ssa alusten ja satamarakenteiden turvatoimien parantamisesta annetulla Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 725/2004, jäljempänä *turvatoi-*

miasetus. Kansallisesti eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetussa laissa säädetään satamissa noudatettavista turvatoimista. Lain mukainen toimivaltainen viranomainen on Liikenteen turvallisuusvirasto, jonka tehtävänä on valvoa turvatoimiasetuksen ja kyseisen lain säädösten noudattamista. Rajavartiolaitoksen, poliisin ja tullilaitoksen tehtävänä on ilmoittaa turvatoimiasetuksen ja kyseisen lain säännöksien noudattamisessa havaitsemistaan puutteista Liikenteen turvallisuusvirastolle, jonka on viipymättä ryhdyttävä toimiin puutteellisuuksien korjaamiseksi. Laissa säädetään myös Liikenteen turvallisuusvirastolle, rajavartiolaitokselle, poliisille ja tullilaitokselle kuuluvista erityistehtävistä (4–7 §).

Tieliikenne

Tienkäyttäjää koskevat säännöt, eli liikennesäännöt, sisältyvät tieliikennelakiin (267/1981). Tieliikenteen ohjaukseen liittyviä toimintoja kuuluu eri toimijoille. Maantielain mukaan Liikennevirasto ja elinkeino- liikenne ja ympäristö -keskukset ovat tienpitoviranomaisia. Ne voivat mm. kieltää tai rajoittaa tilapäisesti liikennettä (35 §) ja antaa lupia erilaisten rakennelmien, laitteiden ja kaapeleiden sijoittamiselle tiealueelle (42 ja 42 a §). Myös tieliikennelaissa Liikennevirastolla on toimivaltuuksia mm. liikenteen ohjauslaitteiden asettamiseen sekä liikenteen ohjaukseen tien ja rautatien tasoristeyksessä sekä tieliikenneasetuksen 49 §:ssä tarkoitetussa tien tilapäisessä sulkemisessa. Kunnilla on myös liikenteenohjaustehtäviä, esimerkiksi tieliikennelain 51 §:n mukaan kunta asettaa liikenteen ohjauslaitteen kadulle, rakennuskaavatielle, torille ja muulle vastaavanlaiselle liikennealueelle.

Tieliikenteen älykkäät liikennejärjestelmät

Automaattisesti ohjautuvat ajoneuvot ovat osa älykkäiden liikennejärjestelmien toteutumista. Älykkäissä liikennejärjestelmissä automaattisesti ohjautuvat ajoneuvot käyttävät liikkumiseensa itse tuottamaansa tietoa, jota ne keräävät ympäristöstä omilla sensoreillaan, tutkillaan ja kameroillaan. Sen lisäksi ne käyttävä sitä laajapohjaista tietoa, mitä ajoneuvoihin välittyy verkon kautta muusta liikenneympäristöstä, muista liikkuvista ajoneuvoista, tieympäristöstä, liikenteen ohjausjärjestelmistä ja kaupallisista palveluista.

EU:n tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista annetun Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU (jäljempänä *ITS-direktiivi*) tavoitteena on nopeuttaa älykkäiden liikennejärjestelmien koordinoitua käyttöönottoa ja käyttöä tieliikenteessä kaikkialla Euroopassa. ITS-direktiiviä sovelletaan kaikkiin tieliikennealan älykkäisiin liikennejärjestelmiin sekä tieliikenteen ja muiden liikennemuotojen välisiin rajapintoihin. ITS-direktiivissä korostetaan eurooppalaista älyliikennearkkitehtuuria, jolla voidaan edistää myös multimodaalista, eli eri liikennemuodot yhdistävää lipunmyyntiä. ITS-direktiivi sisältää säännöksen, jonka nojalla Euroopan komissiolle on siirretty säädösvalta antaa delegoituja asetuksia niiden teknisten määritysten osalta, jotka ovat tarpeen ITS-järjestelmien käyttöönoton ja operatiivisen käytön yhteensopivuuden, yhteentoimivuuden ja jatkuvuuden varmistamiseksi koko unionin alueella. ITS-direktiivi onkin luonteeltaan puitelaki, joka saa sisältönsä sen 6 ja 7 artiklojen nojalla annettujen delegoitujen säädösten sisällöstä. Ne ovat komission asetuksia, minkä johdosta ne ovat suoraan sovellettavaa oikeutta ja edellyttävät ainoastaan rajallisesti kansallista sääntelyä.

ITS-direktiivi on Suomessa saatettu osaksi liikenteen palveluista annettua lakia (320/2017). Lain III osan 2 luvun 6 §:ssä säädetään älykkäiden liikennejärjestelmien käyttöönotosta. Pykä-

län 2 momentissa asetettaisiin Liikenteen turvallisuusvirasto toimivaltaiseksi viranomaiseksi arvioimaan vaatimustenmukaisuuden täyttymistä. Tällä hetkellä ITS-direktiivin nojalla annetuista komission asetuksista yhteentoimivaa EU:n laajuista eCall-hätäpuhelujärjestelmää koskevan asetuksen N:o 305/2013 4 artikla sekä dataa ja menettelyitä, joiden avulla mahdollisuuksien mukaan tarjotaan liikenneturvallisuuteen liittyviä yleisiä vähimmäisliikennetietoja ilmaiseksi käyttäjille koskevan asetuksen N:o 886/2013 9 artikla edellyttävät vaatimustenmukaisuutta arvioivan toimijan nimeämistä.

Komission delegoitua asetusta (EU) N:o 886/2013 Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU täydentämisestä datan ja menettelyjen osalta, joiden avulla mahdollisuuksien mukaan tarjotaan liikenneturvallisuuteen liittyviä yleisiä vähimmäisliikennetietoja ilmaiseksi käyttäjille, sovelletaan liikenneturvallisuuteen liittyvien yleisten vähimmäistason liikennetietopalvelujen tarjontaan Euroopan laajuisessa tieverkossa. Liikenneturvallisuuteen liittyvillä yleisellä vähimmäistason liikennetietopalvelulla tarkoitetaan reaaliaikaista liikennetietopalvelua, joka tarjoaa sovitun liikenneturvallisuuteen liittyvän vähimmäissisällön ja joka on mahdollisimman monen loppukäyttäjän saatavissa mahdollisimman helposti.

Pankkiala ja finanssimarkkinoiden infrastruktuuri

Pankkialan ja finanssimarkkinoiden infrastruktuuria ei ole verkko- ja tietoturvadirektiivin liitteessä II jaettu tarkempiin osa-alueisiin. Toimijoiden tyyppeinä on mainittu pankkialan osalta luottolaitokset ja finanssimarkkinoiden infrastruktuurin osalta unionin direktiivissä 2014/65/EU määritellyt kauppapaikkojen ylläpitäjät sekä keskusvastapuolet.

Pankkialan ja finanssimarkkinoiden infrastruktuurien sääntely ja valvonta on erittäin yhdenmukaistettua unionin tasolla. Tämä näkyy unionin primaari- ja sekundaarioikeuden soveltamisessa sekä yhdessä Euroopan valvontaviranomaisten kanssa kehitettyjen standardien käyttämisessä. Näiden vaatimusten soveltaminen ja valvonta varmistetaan pankkiunionissa yhteisellä valvontamekanismilla. Rahoitusalan sääntelyn muilla aloilla myös Euroopan finanssivalvojien järjestelmä varmistaa valvontakäytäntöjen yhdenmukaisuuden ja yhtenäisyyden korkean tason. Pankkialalla riskienhallinnan keskeisenä tavoitteena on turvata riittävät omat varat suhteessa riskien ottoon ja riskienhallintajärjestelmien tasoon. Toimintaan kohdistuvat riskit voidaan jaotella esimerkiksi luottoriskien, operatiivisten riskien, markkinariskien sekä likviditeetin hallintaan.

Operatiivinen riski on keskeinen osa vakavaraissääntelyä ja -valvontaa pankkialalla ja finanssimarkkinoiden infrastruktuurien alalla. Operatiivisella riskeillä voidaan tarkoittaa esimerkiksi riskiä, joka aiheutuu riittämättömistä tai epäonnistuneista sisäisistä prosesseista, henkilöstöstä, järjestelmistä tai ulkoisista tekijöistä. Operatiivisten riskien hallinta kattaa kaikki toiminnot, mukaan lukien verkko- ja tietojärjestelmien turvallisuuden, eheyden ja häiriönsietokyvyn.

Luottolaitokset

Luottolaitostoiminnasta annetun lain (610/2014) 5 luvun 10 ja 11 §:ssä säädetään luottolaitoksen merkittävän toiminnan ulkoistamisesta ja ulkoistamisen edellytyksistä. Varautumisvelvollisuudesta on säädetty 16 §:ssä. Yleiset luottolaitoksen riskienhallintajärjestelmälle asetettavat vaatimukset on annettu luottolaitostoiminnasta annetun lain 9 luvun 2 §:ssä ja operatiivisten riskien hallinnan osalta 16 §:ssä, jonka mukaan luottolaitoksella on oltava riittävät, turvalliset

ja toimintavarmat maksu-, arvopaperi- ja muut tietojärjestelmät. Lisäksi pykälässä säädetään varautumissuunnittelusta.

Lain 24 §:n mukaan Finanssivalvonta voi antaa tarkempia määräyksiä 16 §:ssä tarkoitetusta operatiivisesta riskistä. Finanssivalvonta on antanut määräykset operatiivisen riskin hallinnasta rahoitussektorin valvottavissa (Määräykset ja ohjeet 8/2014) sekä ulkoistamisesta (Määräykset ja ohjeet 1/2012). Määräyksen operatiivisen riskin hallinnasta rahoitussektorin valvottavissa 6 luku sisältää määräykset tietojärjestelmien tietoturvallisuudesta.

Finanssivalvonnasta annetun lain 18 §:n 2 momentin mukaan Finanssivalvonta voi antaa määräyksiä valvottavan taloudellista asemaa, omistajia, sisäistä valvontaa ja riskienhallintaa, hallinto- ja valvontaelinten jäseniä ja toimihenkilöitä sekä toimipaikkoja koskevien tietojen säännöllisestä toimittamisesta Finanssivalvonnalle.Finanssivalvonnan operatiivista riskinhallintaa koskevassa määräyksessä määrätään tarkemmin tietojärjestelmiin kohdistuvien häiriöiden ilmoittamisesta Finanssivalvonnalle.

Säännelty markkina, monenkeskinen kaupankäyntijärjestelmä, organisoitu kaupankäyntijärjestelmä sekä pörssi

Pörssitoiminnan harjoittamisen kannalta riskienhallintavaatimuksia ja häiriöiden ilmoittamista koskevat säännökset sisältyvät eduskunnalle 26.10 2017 annetun hallituksen esityksen sijoituspalvelulain muuttamisesta ja kaupankäynnistä rahoitusvälineillä annetuiksi laeiksi sekä eräiksi niihin liittyviksi laeiksi (HE 151/2017 vp) 3 lukuun. Lain 1 §:ssä säädetään säännellyn markkinan toiminnan järjestämistä koskevista vaatimuksista. Lain mukaan Pörssin on varmistettava, että sen käyttämät järjestelmät ja menettelytavat turvaavat kaupankäyntijärjestelmän toiminnan luotettavuuden ja jatkuvuuden myös häiriötilanteissa. Pörssin tulee voida varmistaa, että sillä on riittävä kaupankäyntijärjestelmien häiriönsietokyky, riittävä kapasiteetti toimeksiantojen ja viestien ruuhkahuippujen käsittelyyn ja varmistaa asianmukainen kaupankäynti markkinoiden vakavissa stressiolosuhteissa. Pörssin on testattava säännöllisesti kuormituskokein kaupankäyntijärjestelmän toimintaa edellä kuvattujen vaatimusten täyttämiseksi. Lain 2 §:n mukaan Pörssin on ilmoitettava Finanssivalvonnalle ilman aiheetonta viivästystä rahoitusvälineeseen liittyvistä järjestelmän toimintahäiriöstä.

Terveydenhuoltoala

Terveydenhuoltoa koskien verkko- ja tietoturvadirektiivin liitteessä II on määritelty tarkempina osa-alueina terveydenhuoltolaitokset (mukaan lukien sairaalat ja yksityisklinikat). Suomessa terveydenhuoltolakia (1326/2010) sovelletaan kansanterveyslaissa (66/1972) ja erikoissairaanhoitolaissa (1062/1989) säädetyn kunnan järjestämisvastuuseen kuuluvan terveydenhuollon toteuttamiseen ja sisältöön. Lain 8 §:ssä on säädetty terveydenhuollon toiminnan laatuvaatimuksista ja potilasturvallisuudesta. Lain mukaan terveydenhuollon toiminnan on oltava laadukasta, turvallista ja asianmukaisesti toteutettua. Tämän lisäksi terveydenhuollon toimintayksikön on laadittava suunnitelma laadunhallinnasta ja potilasturvallisuuden täytäntöönpanosta. Sosiaali- ja terveysministeriön asetuksella säädetään tarkemmin asioista, joista on suunnitelmassa sovittava.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) tarkoituksena on edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä. Lailla toteutetaan yhtenäinen sähköinen potilastietojen käsittely- ja arkistointijärjes-

telmä terveydenhuollon palvelujen tuottamiseksi potilasturvallisesti ja tehokkaasti sekä potilaan tiedonsaantimahdollisuuksien edistämiseksi. Lakia sovelletaan julkisten ja yksityisten sosiaali- ja terveydenhuollon palvelujen antajien järjestäessä taikka toteuttaessa sosiaali- tai terveydenhuoltoa.

Lain 5 a luvussa on säädetty sosiaali- tai terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän olennaisista vaatimuksista. Lisäksi 5 b luvussa on säädetty palvelun tarjoajan velvollisuudesta tehdä niin kutsuttu omavalvontasuunnitelma, jossa se määrittelee riskienhallintatoimenpiteitä.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 19 i §:n mukaan palvelun tarjoajan on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle merkittävistä poikkeamista tietojärjestelmän olennaisten vaatimusten täyttymisessä, jos poikkeama voi aiheuttaa merkittävän riskin potilasturvallisuudelle, tietoturvalle tai tietosuojalle.

Terveydenhuollon laitteista ja tarvikkeista annetun lain (629/2010) tarkoituksena on ylläpitää ja edistää terveydenhuollon laitteiden ja tarvikkeiden sekä niiden käytön turvallisuutta. Lakia sovelletaan terveydenhuollon laitteiden ja tarvikkeiden ja niiden lisälaitteiden suunnitteluun ja valmistukseen sekä toimenpidepakkausten ja järjestelmien kokoamiseen. Lisäksi lakia sovelletaan mainittujen tuotteiden markkinoille saattamiseen ja sitä varten steriloimiseen, käyttöönottoon, asennukseen, huoltoon, ammattimaiseen käyttöön, markkinointiin ja jakeluun.

Lain 5 §:n määritelmän mukaan terveydenhuollon laitteella tarkoitetaan instrumenttia, laitteistoa, välinettä, ohjelmistoa, materiaalia tai muuta yksinään tai yhdistelmänä käytettävää laitetta tai tarviketta, jonka valmistaja on tarkoittanut käytettäväksi ihmisen

a) sairauden diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen;

b) vamman tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin;

c) anatomian tai fysiologisen toiminnon tutkimiseen, korvaamiseen tai muunteluun; taikka

d) hedelmöittymisen säätelyyn.

Lain 2 luvussa on säännökset terveydenhuollon laitteita koskevista vaatimuksista. Lain 6 §:n 3 momentin mukaan laitteen tulee olla käyttötarkoitukseensa sopiva ja sen tulee käyttötarkoituksensa mukaisesti käytettynä saavuttaa sille suunniteltu toimivuus ja suorituskyky. Laitteen asianmukainen käyttö ei saa tarpeettomasti vaarantaa potilaan, käyttäjän tai muun henkilön terveyttä tai turvallisuutta.

Lain 17 §:ssä on säädetty toiminnanharjoittajan velvollisuuksista. Sen mukaan toiminnanharjoittajan on noudatettava valmistajan antamia tietoja ja ohjeita terveydenhuollon laitteen kuljetuksesta, säilytyksestä, asennuksesta, huollosta ja muusta laitteen käsittelystä.

Lain 25 §:n mukaan ammattimaisen käyttäjän on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle ja valmistajalle tai valtuutetulle edustajalle vaaratilanteista, jotka ovat johtaneet tai olisivat saattaneet johtaa potilaan, käyttäjän tai muun henkilön terveyden vaarantu-

miseen ja jotka johtuvat muun muassa terveydenhuollon laitteen ominaisuuksista, suorituskyvyn poikkeamasta, riittämättömästä merkinnästä tai virheellisestä käyttöohjeesta.

Sosiaali- ja terveysalan lupa- ja valvontavirasto voi antaa määräyksiä siitä, millä tavalla vaaratilanteista ilmoitetaan ja mitä tietoja niistä on ilmoitettava. Sosiaali- ja terveysalan lupa- ja valvontavirasto on antanut määräyksen terveydenhuollon laitteesta ja tarvikkeesta tehtävän ammattimaisen käyttäjän vaaratilanneilmoituksesta.

Juomaveden toimittaminen ja jakelu

Juomaveden toimittamisen ja jakelun osalta verkko- ja tietoturvadirektiivin liitteessä II ei ole määritelty tarkempia toiminnan osa-alueita. Suomessa vesihuoltolain (119/2001) tavoitteena on turvata sellainen vesihuolto, että kohtuullisin kustannuksin on saatavissa riittävästi terveydellisesti ja muutoinkin moitteetonta talousvettä sekä terveydensuojelulain ja ympäristönsuojelulain kannalta asianmukainen viemäröinti. Vesihuoltolain 14 §:n mukaan vesihuoltolaitoksen tulee huolehtia siitä, että laitoksen toimittama talousvesi täyttää terveydensuojelulaissa (763/1994) säädetyt laatuvaatimukset. Lain 15 §:n mukaan vesihuoltolaitoksen on oltava selvillä käyttämänsä raakaveden määrään tai laatuun kohdistuvista riskeistä sekä laitteistonsa kunnosta. Tässä tarkoituksessa vesihuoltolaitoksen on tarkkailtava käyttämänsä raakaveden määrää ja laatua, laitteistonsa kuntoa sekä vuotovesien määrää laitoksen vesijohto- ja viemäriverkostoissa. Lain 15 a §:n mukaan vesihuoltolaitoksen on vastattava verkostoihinsa liitettyjen kiinteistöjen vesihuoltopalvelujen saatavuudesta häiriötilanteissa. Vesihuoltolain muuttamista koskevaan hallituksen esityksen (HE 218/2013 vp) mukaan häiriötilanteella tarkoitettaisiin kaikkia vesihuollon palvelutuotantoa vaikeuttavia tai vaarantavia häiriötilanteita lukuun ottamatta tavanomaisia toimintahäiriöitä. Tällaisia häiriötilanteita olisivat esimerkiksi vaikutuksiltaan merkittävät laiterikot, muut vakavat vesihuollon laitteistojen, järjestelmien tai palvelujen häiriöt, teknisten järjestelmien häiriöt sekä vedenhankintaan ja energia- ja tietojärjestelmiin kohdistuvat häiriötilanteet. Häiriöitä voisivat aiheuttaa muun muassa luonnononnettomuudet, äärimmäiset sääolosuhteet, paikalliset tai valtakunnalliset onnettomuudet, ilkivalta ja rikokset. Häiriötilanteella tarkoitetaan sekä normaaliolojen että valmiuslaissa tarkoitettujen poikkeusolojen häiriötilanteita.

Vesihuoltolain 15 a §:n mukaan palvelujen turvaamiseksi laitoksen on oltava yhteistyössä muiden samaan verkostoon liitettyjen vesihuoltolaitosten, kunnan, kunnan valvontaviranomaisten, pelastusviranomaisten, sopimuskumppanien ja asiakkaiden kanssa. Vesihuoltolaitoksen on laadittava ja pidettävä ajan tasalla suunnitelma häiriötilanteisiin varautumisesta sekä ryhdyttävä suunnitelman perusteella tarvittaviin toimenpiteisiin. Laitoksen tulee toimittaa suunnitelma valvontaviranomaisille, pelastusviranomaiselle ja kunnalle.

Talousveden turvallisuutta koskevat laatuvaatimukset perustuvat ihmisten käyttöön tarkoitetun veden laadusta annettuun Euroopan parlamentin ja neuvoston direktiiviin 98/83/EY. Kansallisesti talousveden laatuvaatimuksista on säädetty terveydensuojelulain 17 §:ssä sekä laadun valvonnasta lain 20 §:ssä.

Sosiaali- ja terveysministeriö on antanut terveydensuojelulain 17 ja 20 §:n nojalla asetuksen talousveden laatuvaatimuksista ja valvontatutkimuksista (1352/2015). Asetuksessa säädetään talousveden laatuvaatimuksista, laatutavoitteista ja desinfioinnista, menettelystä, jos talousvesi ei täytä laatuvaatimuksia tai -tavoitteita, talousveden säännöllisestä valvonnasta, talousvettä toimittavan laitoksen toimintaa koskevan hakemuksen sisällöstä, talousveden terveydelliseen

laatuun vaikuttavien riskien arvioinnista ja hallinnasta, talousveden radioaktiivisista aineista aiheutuvan säteilyaltistuksen rajoittamisesta ja kunnan terveydensuojeluviranomaisen häiriötilanteisiin varautumista koskevan suunnitelman sisällöstä ja laatimisesta.

2.1.5 Huoltovarmuus ja varautuminen poikkeusoloihin

Huoltovarmuudella tarkoitetaan huoltovarmuuden turvaamisesta annetun lain mukaan niitä taloudellisia toimintoja ja niihin liittyviä teknisiä järjestelmiä, jotka turvaavat väestön toimeentulon, maan talouselämän ja maanpuolustuksen poikkeusolojen ja niihin verrattavissa olevien vakavien häiriöiden varalta. Huoltovarmuuspäätöksen mukaan Suomen huoltovarmuuden kannalta kriittisiä toimialoja ovat tietoyhteiskuntasektorin lisäksi energiahuolto, rahoitushuolto, kuljetuslogistiikka, terveydenhuolto, elintarvikehuolto ja kriittinen teollisuustuotanto. Kaikkien näiden alojen toimivuus on eri tavoin riippuvaista tieto- ja viestintäjärjestelmien häiriöttömästä toiminnasta.

Kaikkein vakavimpien yhteiskunnan kriisien varalle on säädetty vuonna 2012 voimaan tullut valmiuslaki. Valmiuslaissa säädetään valtionsisäisistä Suomen viranomaisten toimivaltuuksista poikkeusolojen aikana väestön turvallisuuden ja elinmahdollisuuksien sekä yhteiskunnan toimivuuden varmistamiseksi. Poikkeusoloja ovat valmiuslain 3 §:n mukaan 1) Suomeen kohdistuva aseellinen tai siihen vakavuudeltaan rinnastettava hyökkäys ja sen välitön jälkitila; 2) Suomeen kohdistuva huomattava aseellisen tai siihen vakavuudeltaan rinnastettavan hyökkäyksen uhka, jonka vaikutusten torjuminen vaatii valmiuslain mukaisten toimivaltuuksien välitöntä käyttöön ottamista; 3) väestön toimeentuloon tai maan talouselämän perusteisiin kohdistuva erityisen vakava tapahtuma tai uhka, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti vaarantuvat; 4) erityisen vakava suuronnettomuus ja sen välitön jälkitila; sekä 5) vaikutuksiltaan erityisen vakavaa suuronnettomuutta vastaava hyvin laajalle levinnyt vaarallinen tartuntatauti. Lain 13 §:n mukaan varautumista johtaa ja valvoo valtioneuvosto sekä kukin ministeriö toimialallaan. Kukin ministeriö sovittaa yhteen varautumista omalla toimialallaan.

Varautumista poikkeusoloihin ja normaaliolojen häiriötilanteisiin koskevia säännöksiä sisältyy myös useisiin sektorikohtaisiin erityislakeihin.

2.1.6 Muu keskeisten palvelujen tietoturvallisuuden kannalta merkityksellinen lainsäädäntö

Myös muuhun lainsäädäntöön sisältyy tietoturvariskienhallintaan sekä tietoturvahäiriöiden ilmoittamiseen liittyvää sääntelyä, joka vaikuttaa palveluiden tarjontaan sektorikohtaisen erityislainsäädännön lisäksi. Esimerkiksi henkilötietojen käsittelyä koskevat tietoturvavelvoitteet koskevat lähtökohtaisesti palvelun tarjoajia kaikilla toimialoilla. Silloin kun palvelun tarjoajana on viranomainen, niitä koskevat myös julkisuuslain nojalla annetussa tietoturva-asetuksessa asetetut tietoturvallisuusvaatimukset.

Henkilötietojen käsittelyä koskevat tietoturvavelvoitteet

Henkilötietolain (523/1999) tarkoitus on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Henkilötietolaki on yleislaki, jonka säännöksiä on noudatettava henkilötietoja käsiteltäessä, jollei muualla laissa toisin säädetä. Henkilötietolain

säännöksiä on pääsääntöisesti siis noudatettava myös yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjonnassa suoritettuun henkilötietojen käsittelyyn.

Lain 7 luvussa säädetään henkilötietojen käsittelyn tietoturvallisuudesta ja tietojen säilytyksestä. Lain 32 §:n mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.

Henkilötietolailla on pantu täytäntöön yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annettu Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, jäljempänä *henkilötietodirektiivi*. Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta annettu Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, jäljempänä *yleinen tietosuoja-asetus,* korvaa henkilötietodirektiivin 25.5.2018 lähtien. Asetus on Suomessa suoraan sovellettava. Yleisen tietosuoja-asetuksen 32 artiklassa säädetään henkilötietojen käsittelyn turvallisuudesta. Asetuksen 33 artiklassa säädetään velvollisuudesta ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle. Sen mukaan rekisterinpitäjän on ilmoitettava ilman aiheetonta viivytystä valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta. Artiklassa säädetään lisäksi ilmoituksen vähimmäissisällöstä sekä tietoturvaloukkauksien dokumentointivelvollisuudesta.

Viranomaisen tiedonhallintaa koskevat tietoturvavelvoitteet

Viranomaisen asiakirjan julkisuudesta ja asiakirjan saamista koskevan pyynnön käsittelystä sekä hyvään tiedonhallintatapaan kuuluvista yleisistä velvollisuuksista säädetään julkisuuslaissa.

Julkisuuslain 36 §:n asetuksenantovaltuuden nojalla annetussa tietoturva-asetuksessa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista. Mikäli yhteiskunnan toiminnan kannalta keskeisiä palveluita tarjoaa viranomainen, on sen noudatettava tietoturva-asetuksen velvoitteita.

Sähköistä tunnistamista koskevat tietoturvavelvoitteet

Vahvasta sähköisestä tunnistamisesta sekä tunnistuspalveluiden tarjoamisesta palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (617/2009) (tunnistuspalvelulaki). Lain 8 §:ssä säädetään sähköisen tunnistamisen järjestelmälle asetettavista vaatimuksista mukaan lukien tietoturvavaatimukset. Lain 13 §:n mukaan tunnistamispalvelun tarjoajan on huolehdittava palvelujensa henkilötietolain 32 §:ssä tarkoitetusta tietojen suojaamisesta sekä riittävästä tietoturvasta. Lain 16 §:n mukaan tunnistuspalvelun tarjoajan on salassapitosäännösten estämättä ilmoitettava ilman aiheetonta viivästystä tunnistuspalveluunsa luottaville osapuolille, tunnistusvälineiden haltijoille, muille luottamusverkostossa toimiville sopimuspuolilleen sekä Viestintävirastolle palvelun toimivuuteen, tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhista tai häiriöistä. Viestintävirasto voi tekni-

sesti välittää tietoja luottamusverkostossa osapuolten välillä ilmoittajan lukuun sen estämättä, mitä julkisuuslaissa säädetään. Lain 29 §:n mukaan tunnistuspalvelun tarjoajan on määräajoin teetettävä palvelulleen laissa määritellyn arviointielimen arviointi siitä, täyttääkö tunnistuspalvelulaissa säädetyt yhteentoimivuutta, tietoturvaa, tietosuojaa ja muuta luotettavuutta koskevat vaatimukset.

2.1.7 Viranomaisvalvonta ja tilannekuvan muodostaminen

Suomessa edellä kuvattuja toiminnan laatu- ja turvallisuusvelvoitteita valvovat eri viranomaiset riippuen toiminnan luonteesta. Toiminnan turvallisuuteen tai tietoturvallisuuteen liittyviä velvoitteita ei ole järjestetty yhden viranomaisen valvottavaksi. Näin esimerkiksi teletoimintaan liittyviä turvallisuus- ja tietoturvallisuusvelvoitteita valvoo Viestintävirasto, luottolaitosten toimintaan liittyviä Finanssivalvonta ja terveyden huollon asiakastietojen käsittelyyn liittyviä Sosiaali- ja terveysalan lupa- ja valvontavirasto. Viestintävirastossa ei ole varsinaisia yleisiä yhteiskunnan keskeisten palvelujen tietoturvallisuuteen liittyviä valvontatehtäviä, vaikka Viestintävirasto yleisesti tukee ja auttaa kansalaisia ja yrityksiä tietoturvasta huolehtimisessa (esimerkiksi tarjoamalla tietoturvaloukkausten ja -uhkien kansallinen yhteyspisteen eli CERT (Computer Emergency Response Team) -toimintoa, jonka tehtävänä on selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia kerätä tietoa tällaisista tapahtumista ja tiedottaa tietoturva-asioista yleensä) sekä muodostaa yleistä tietoturvallisuuden tilannekuvaa. Viestintävirasto saa merkittävän osan tietoturvaloukkaus- ja haavoittuvuustiedoista elinkeinonharjoittajien vapaaehtoisesti tekemien ilmoituksien kautta.

Valtion tasolla yleisen turvallisuuden tilannekuvan muodostamisesta vastaa Valtioneuvoston tilannekeskus, joka koostaa tilannekuvaa myös eri toimialojen valvontaviranomaisten sekä muiden viranomaisten toimittamien tietojen pohjalta.

Valtioneuvoston tilannekeskus

Valtioneuvostosta annetun lain (175/2003) nojalla annetun valtioneuvoston ohjesäännön (262/2003) 12 §:n 7 kohdan mukaan valtioneuvoston kanslian toimialaan kuuluu valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus sekä häiriötilanteiden hallinnan yleinen yhteensovittaminen.

Ympärivuorokautisesti toimiva valtioneuvoston tilannekeskus perustettiin valtionjohdon ja viranomaisten jatkuvaa tiedonsaantia varten syyskuussa 2007. Laki valtioneuvoston tilannekeskuksesta tuli voimaan heinäkuussa 2017. Laissa säädetään valtioneuvoston tilannekeskuksen tehtävistä ja viranomaisten välisestä tiedonvaihdosta. Lain 1 §:n mukaan valtioneuvoston tilannekeskuksen tehtävänä on tasavallan presidentin ja valtioneuvoston päätöksenteon ja toiminnan tueksi koota ja analysoida tietoa turvallisuustilanteesta ja sellaisista häiriöistä ja niiden uhista, jotka vaarantavat yhteiskunnan elintärkeitä toimintoja, hoitaa ja koordinoida tilannekuvan ylläpitämiseen, kokoamiseen, yhteensovittamiseen ja välittämiseen liittyviä poikkihallinnollisia tehtäviä sekä jakaa yhteen sovitettua tietoa tasavallan presidentille, valtioneuvostolle ja muille viranomaisille. Lisäksi laissa säädetään ministeriöiden sekä hallinnonalan viraston ja laitoksen velvollisuudesta ilmoittaa onnettomuudesta, vaaratilanteesta, poikkeuksellisesta tapahtumasta tai muusta vastaavasta häiriöstä tilannekeskukselle sekä tilannekeskuksen tiedonsaantioikeudesta sekä salassa pidettävän tiedon luovuttamisesta.

Valtioneuvoston tilannekeskus tuottaa reaaliaikaista turvallisuustapahtumatietoa ja toimivaltaisten viranomaisten tiedoista koottua tilannekuvaa. Tilannekeskus yhdistää eri viranomaisilta ja avoimista lähteistä saadut tiedot ja raportoi niiden pohjalta valtionjohdolle ja eri viranomaisille.

Viestintävirasto

Viestintäviraston tehtävät ja erityiset tehtävät on määritelty tietoyhteiskuntakaaressa ja eräissä muissa laeissa. Tietoyhteiskuntakaaren mukaan Viestintäviraston erityisiin tehtäviin kuuluu muun muassa edistää sähköisen viestinnän toimivuutta, häiriöttömyyttä ja turvallisuutta, kerätä tietoa verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista, tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta sekä selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.

Liikenteen turvallisuusvirasto

Liikenteen turvallisuusvirastosta annetun lain mukaan Liikenteen turvallisuusvirasto vastaa liikennejärjestelmän sääntely- ja valvontatehtävistä ja edistää liikenteen turvallisuutta. Liikenteen turvallisuusvirasto ylläpitää myös liikennejärjestelmän tilakuvaa, joka kertoo Suomen liikennejärjestelmän turvallisuuden tilasta.

Ilmailulaissa säädetään Liikenteen turvallisuusviraston tehtävistä koskien ilmailun turvallisuusvaatimusten noudattamista ja ilmailutoiminnan vaatimustenmukaisuutta. Sen lisäksi, mitä ilmailulaissa säädetään Liikenteen turvallisuusviraston tehtävistä, virasto toimii muun muassa EASA-asetuksessa ja poikkeama-asetuksessa tarkoitettuna toimivaltaisena kansallisena viranomaisena. Liikenteen turvallisuusvirasto toimii myös Suomen kansainvälisissä liikennesopimuksissa tarkoitettuna ilmailuviranomaisena, josta säädetään ilmailulain 173 §:ssä. Lentoturvallisuutta mahdollisesti vaarantavista poikkeamista on ilmoitettava Liikenteen turvallisuusvirastolle voimassa olevan lainsäädännön mukaisesti.

Liikenteen turvallisuusviraston valvontaan kuuluu yleinen meriturvallisuuden sekä hyvän merimiestaidon noudattamisen valvonta. Alusliikennepalvelulain mukaan Liikenteen turvallisuusvirasto ja VTS-viranomainen valvovat lain nojalla asetettujen säännösten ja määräysten noudattamista. Alusliikennepalvelulain 18 §:ssä säädetään VTS-viranomaisen velvollisuudesta ilmoittaa liikenteen turvallisuusvirastolle tietvistä merenkulun turvallisuuteen liittvvistä olennaisista seikoista ja luotsauslain (940/2003) noudattamiseen liittyvistä havainnoista. Liikenteen turvallisuusvirasto toimii myös eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain mukaisena toimivaltaisena viranomaisena.

Liikenteen turvallisuusvirasto valvoo rautatiejärjestelmän turvallisuusvaatimusten noudattamista sekä rautatieliikenteen harjoittajan ja rataverkon haltijan turvallisuusjohtamisjärjestelmien vaatimustenmukaisuutta. Valvontaa sääntelee kansallisen viranomaisen suorittamasta valvonnasta turvallisuusluvan tai -todistuksen myöntämisen jälkeen annettu Euroopan komission asetus (EU) N:o 1077/2012.

Sosiaali- ja terveysalan lupa- ja valvontavirasto

Terveydenhuollon laitteista ja tarvikkeista annetun lain 38 §:n mukaan Sosiaali- ja terveysalan lupa- ja valvontaviraston tehtävänä on valvoa ja edistää terveydenhuollon laitteiden sekä niiden käytön turvallisuutta ja vaatimustenmukaisuutta.

Tämän tehtävän toteuttamiseksi Sosiaali- ja terveysalan lupa- ja valvontavirasto ylläpitää vaaratilannerekisteriä. Sosiaali- ja terveysalan lupa- ja valvontaviraston on arvioitava ilmoitusvelvollisilta tulleet vaaratilanneilmoitukset ja ryhdyttävä tarpeellisiin terveyden ja turvallisuuden edellyttämiin toimiin.

Lisäksi Sosiaali- ja terveysalan lupa- ja valvontavirasto valvoo sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyyn tarkoitettujen tietojärjestelmien olennaisten vaatimusten toteutumista. Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain mukaan Sosiaali- ja terveysalan lupa- ja valvontaviraston tehtävänä on valvoa ja edistää tietojärjestelmien vaatimustenmukaisuutta. Lain mukaan sosiaali- tai terveydenhuollon palvelujen antajan on ilmoitettava Sosiaali- ja terveysalan lupa- ja valvontavirastolle tietojärjestelmän olennaisten vaatimusten täyttymisessä havaitsemistaan merkittävistä poikkeamista silloin, kun poikkeama voi aiheuttaa merkittävän riskin potilasturvallisuudelle, tietoturvalle tai tietosuojalle.

Terveyden ja hyvinvoinnin laitos

Sosiaali- ja terveysministeriön alainen Terveyden ja hyvinvoinnin laitos toimii siitä annetun lain mukaan väestön hyvinvoinnin ja terveyden edistämiseksi, sairauksien ja sosiaalisten ongelmien ehkäisemiseksi sekä sosiaali- ja terveydenhuollon ja sen palvelujen kehittämiseksi. Terveyden ja hyvinvoinnin laitoksesta annetun lain 2 §:n 4 b kohdan mukaan laitoksen tehtävänä on vastata sosiaali- ja terveydenhuollon asiakastiedon sähköisen käsittelyn, siihen liittyvän tietohallinnon ja valtakunnallisten tietojärjestelmäpalvelujen käytön ja toteuttamisen suunnittelusta, ohjauksesta ja seurannasta. Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 19 a §:n mukaan Terveyden ja hyvinvoinnin laitos voi tarvittaessa antaa tarkempia määräyksiä sosiaali- tai terveydenhuollon asiakastietojen käsittelyssä käytettävän tietojärjestelmän olennaisten vaatimusten sisällöstä.

Finanssivalvonta

Finanssivalvonnasta annetun lain mukaan Finanssivalvonnan toiminnan tavoitteena on finanssimarkkinoiden vakauden edellyttämä luotto-, vakuutus- ja eläkelaitosten ja muiden valvottaviksi säädettyjen vakaa toiminta, vakuutettujen etujen turvaaminen sekä yleinen luottamus finanssimarkkinoiden toimintaan. Finanssivalvonta valvoo, että finanssimarkkinoilla toimivat noudattavat niihin sovellettavia finanssimarkkinoita koskevia säännöksiä, niiden nojalla annettuja määräyksiä, toimilupansa ehtoja ja toimintaansa koskevia sääntöjä. Finanssivalvonnasta annetun lain mukaan Finanssivalvonta voi antaa määräyksiä valvottavan taloudellista asemaa, omistajia, sisäistä valvontaa ja riskienhallintaa, hallinto- ja valvontaelinten jäseniä ja toimihenkilöitä sekä toimipaikkoja koskevien tietojen säännöllisestä toimittamisesta Finanssivalvonnalle.

Energiavirasto

Energiaviraston tehtävistä on säädetty sähkö- ja maakaasumarkkinoiden valvonnasta annetussa laissa (590/2013). Lain 2 §:n mukaan lakia sovelletaan niiden valvonta- ja seurantatehtävi-

en hoitamiseen, jotka säädetään Energiaviraston tehtäviksi muun muassa sähkömarkkinalaissa ja maakaasumarkkinalaissa sekä niiden nojalla annetuissa säännöksissä ja viranomaisten määräyksissä.

Energiaviraston toimivallasta valvonta-asioissa säädetään lain 9 §:ssä. Lain mukaan, jos joku rikkoo tai laiminlyö lain 2 §:ssä tarkoitetussa kansallisessa tai Euroopan unionin lainsäädännössä säädettyjä velvoitteitaan, Energiaviraston on velvoitettava hänet korjaamaan rikkomuksensa tai laiminlyöntinsä. Päätöksessä voidaan määrätä, millä tavoin rikkomus tai laiminlyönti tulee korjata.

Lain 30 §:ssä säädetään Energiaviraston tiedonsaanti- ja tarkastusoikeudesta. Lain mukaan valvottavaa toimintaa harjoittavan elinkeinonharjoittajan on annettava Energiavirastolle tässä laissa tarkoitettujen valvontatehtävien hoitamiseksi tarpeelliset tiedot ja asiakirjat. Tämän lisäksi Energiavirastolle on annettava muiden tässä laissa tarkoitettujen tehtävien hoitamiseksi tai kansainvälisten sopimusvelvoitteiden täyttämiseksi tarpeellisia tilasto- ja muita tietoja.

Juomaveden toimittaminen ja jakelu

Vesihuoltolain toimeenpanon yleinen ohjaus ja seuranta kuuluvat maa- ja metsätalousministeriölle. Vesihuoltolain mukaisia valvontaviranomaisia ovat toimialoillaan elinkeino-, liikenne- ja ympäristökeskus sekä kunnan ympäristönsuojeluviranomainen ja terveydensuojeluviranomainen.

Elinkeino-, liikenne- ja ympäristökeskus ja kunnan ympäristönsuojeluviranomainen valvovat, että vesihuoltolaitos täyttää laissa säädetyn yhteistyö- ja suunnitteluvelvollisuutensa häiriötilanteisiin varautumiseksi. Laitoksille ei ole kuitenkaan vesihuoltolaissa säädetty velvollisuutta ilmoittaa viranomaisille jakelun keskeytymisestä tai muista häiriötilanteista. Terveydensuojelulain 4 §:n mukaan sosiaali- ja terveysministeriölle kuuluu terveydensuojelun yleisen suunnittelun ja valvonnan ylin johto ja ohjaus. Sosiaali- ja terveysministeriö vastaa talousveden laatuvaatimuksista ja valvonnasta Suomessa. Terveydensuojelulain mukaan annetulla sosiaali- ja terveysministeriön asetuksella säädetään talousveden laatuvaatimuksista ja valvontatutkimuksista.

Talousveden laatua valvotaan säännöllisesti. Valvonnan tarkoituksena on seurata veden laatua terveydelle haitattoman veden jakelun varmistamiseksi. Jos talousvesi ei täytä sille asetettuja laatuvaatimuksia ja vedestä voi aiheutua haittaa terveydelle, kunnan terveydensuojeluviranomaisen on yhdessä vettä toimittavan laitoksen kanssa selvitettävä, mistä veden laadun häiriö johtuu. Terveydensuojeluviranomaisen on määrättävä veden toimittaja korjaamaan tilanne pikaisesti ja annettava veden käyttäjille ohjeet siitä, miten terveyshaitta voidaan ehkäistä.

Terveydensuojelulainsäädännössä vesihuoltolaitokset on jaoteltu suuriin ja pieniin laitoksiin. Suuria laitoksia ovat ne, jotka toimittavat vettä vähintään 10 kuutiometriä päivässä tai vähintään 50 henkilön tarpeisiin. Kaikkein suurimpien talousvettä toimittavien laitosten – sellaisten, jotka toimittavat vettä vähintään 1000 kuutiometriä päivässä taikka vähintään 5000 käyttäjälle veden laatutiedot toimitetaan Euroopan komissiolle.

Kuntien terveydensuojeluviranomaisten pitää toimittaa tällaisten laitosten valvontatutkimustulokset aluehallintovirastolle. Terveyden ja hyvinvoinnin laitos laatii vuosittain raportin näiden

laitosten veden laadusta, ja raportti julkaistaan Sosiaali- ja terveysalan lupa- ja valvontaviraston verkkosivuilla.

Sosiaali- ja terveysalan lupa- ja valvontavirasto ohjaa kuntien terveydensuojeluviranomaisia talousveden laatua ja valvontaa koskevissa asioissa. Lisäksi aluehallintovirasto ohjaa ja valvoo terveydensuojelua toimialueellaan.

2.1.8 Viranomaisten välinen yhteistyö ja tiedonvaihto

Verkko- ja tietoturvadirektiivi velvoittaa tietoturvallisuudesta vastaavat viranomaiset tekemään tarvittavaa yhteistyötä direktiivin mukaisten velvoitteiden valvomiseksi. Suomessa viranomaisten välisen yhteistyön yleisistä perusteista on säädetty hallintolaissa. Hallintolain 10 §:n mukaan viranomaisen on toimivaltansa rajoissa ja asian vaatimassa laajuudessa avustettava toista viranomaista tämän pyynnöstä hallintotehtävän hoitamisessa sekä muutoinkin pyrittävä edistämään viranomaisten välistä yhteistyötä. Viranomaisten välisestä virka-avusta säädetään erikseen.

Julkisuuslaissa on säädetty salassa pidettävän tiedon antamisesta viranomaisesta. Lain 26 §:n mukaan viranomainen voi antaa salassa pidettävästä viranomaisen asiakirjasta tiedon, jos tiedon antamisesta tai oikeudesta tiedon saamiseen on laissa erikseen nimenomaisesti säädetty, tai se, jonka etujen suojaamiseksi salassapitovelvollisuus on säädetty, antaa siihen suostumuksensa.

Saman pykälän mukaan viranomainen voi antaa salassa pidettävästä asiakirjasta tiedon antamansa virka-aputehtävän suorittamiseksi sekä toimeksiannostaan tai muuten lukuunsa suoritettavaa tehtävää varten, jos se on välttämätöntä tehtävän suorittamiseksi. Viranomaisen on ennakolta varmistuttava siitä, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti. Viranomaisten oikeudesta tai velvollisuudesta tehdä yhteistyötä ja vaihtaa salassa pidettäviä tietoja muiden viranomaisten kanssa on säädetty useiden viranomaisten toimintaa sääntelevässä erityslainsäädännössä.

2.1.9 Seuraamukset

Perustuslain mukaan julkisen vallan käytön tulee perustua lakiin. Laissa on siis säädettävä viranomaisten toimivaltuuksista ja niistä seuraamuksista, joita lain rikkomisesta seuraa. Useisiin lakeihin sisältyykin säännöksiä valvontaviranomaisen oikeudesta antaa sille, joka rikkoo lakia, huomautuksen, velvoittaa korjaamaan virheen tai määrätä muun hallinnollisen sanktion, kuten seuraamusmaksun. Esimerkiksi tietoyhteiskuntakaaren 330 §:n mukaan valvontaviranomainen voi lain mukaisia tehtäviä hoitaessaan antaa huomautuksen sille, joka rikkoo lakia taikka sen nojalla annettuja säännöksiä, määräyksiä, päätöksiä ja lupaehtoja sekä velvoittaa tämän korjaamaan virheensä tai laiminlyöntinsä kohtuullisessa määräajassa. Rautatielain 86 §:n mukaan Liikenteen turvallisuusvirasto voi antaa rautatieyritykselle tai muulle tässä laissa tarkoitetulle rautatieliikenteen harjoittajalle tai rataverkon haltijalle huomautuksen tai varoituksen, jos tämä toimii rautatielain tai sen nojalla annettujen säännösten vastaisesti. Lisäksi lain 87 §:n mukaan Liikenteen turvallisuusvirasto voi määrätä rautatieliikenteen harjoittajan tai rataverkon haltijan korjaamaan virheensä tai laiminlyöntinsä sekä asettaa sille velvoitteita taikka kieltää toimenpiteen, jos asianomainen toimii huomautuksesta tai varoituksesta huolimatta rautatielain vastaisesti. Liikenteen palveluista annetun lain VI osan 1 luvun 4 §:n mukaan, jos joku rikkoo lakia, siinä tarkoitettua toimintaa koskevia EU-asetuksia tai lain nojalla annettuja säännöksiä tai

määräyksiä, Liikenteen turvallisuusvirasto voi velvoittaa tämän korjaamaan virheensä tai laiminlyöntinsä. Eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain 19 §:n mukaan, jos satamanpitäjä ei noudata turvatoimiasetuksen tai lain säännöksiä, Liikenteen turvallisuusviraston on laiminlyöjää kuultuaan annettava asianmukaiset ohjeet ja määräykset puutteellisuuksien korjaamiseksi tai epäkohtien poistamiseksi. Virasto voi asettaa puutteellisuuksien korjaamiselle tai epäkohtien poistamiselle määräajan. Finanssivalvonnasta annetun 33 §:n mukaan Finanssivalvonta voi kieltää valvottavan tai muun finanssimarkkinoilla toimivan tekemän päätöksen tai valvottavan tai muun finanssimarkkinoilla toimivan suunnitteleman toimenpiteen toteutuksen taikka velvoittaa valvottavan tai muun finanssimarkkinoilla toimivan lopettamaan toiminnassaan soveltamansa menettelyn, jos päätös, toimenpide tai menettely on ristiriidassa valvottavaan tai muuhun finanssimarkkinoilla toimivaan sovellettavien finanssimarkkinoita koskevien säännösten tai niiden nojalla annettujen määräysten, toimiluvan ehtojen taikka valvottavan tai muun finanssimarkkinoilla toimivan toimintaa koskevien sääntöjen kanssa. Vesihuoltolain 29 §:n mukaan valvontaviranomainen voi kieltää sitä, joka rikkoo lakia tai sen nojalla annettua säännöstä, jatkamasta tai toistamasta säännöksen vastaista menettelyä taikka määrätä hänet täyttämään velvollisuutensa.

Hallintolain 67 §:n mukaan viranomainen voi tehostaa antamaansa kieltoa, velvoitetta tai vaatimusta uhkasakolla, teettämisuhalla taikka keskeyttämisuhalla tai muulla hallinnollisella seuraamuksella siten kuin erikseen säädetään. Säännöksiä tällaisista hallinnollisista seuraamuksista sisältyy tietoyhteiskuntakaaren 332 §:ään, ilmailulain 151 §:ään, rautatielain 87 §:ään, liikenteen palveluista annetun lain VI osan 1 luvun 4 §:ään, sähkö- ja maakaasunmarkkinoiden valvonnasta annetun lain 31 §:ään, finanssivalvonnasta annetun lain 33 a §:ään, vesihuoltolain 30 §:ään, sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain 20 f §:ään sekä terveydenhuollon laitteista ja tarvikkeista annetun lain 52 §:ään.

2.2 Kansainvälinen kehitys sekä ulkomaiden ja EU:n lainsäädäntö

2.2.1 EU:n lainsäädäntö

Komissio antoi vuonna 2013 tiedonannon *Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö* (JOIN(2013) 1 final). Strategian yhtenä tavoitteena on kehittää tietoyhteiskunnan vankkarakenteisuutta parantamalla varautuneisuutta, yhteistyötä, osaamista ja tiedonvaihtoa verkko- ja tietoturvan saralla. Osana strategian täytäntöönpanoa komissio antoi ehdotuksen verkko- ja tietoturvadirektiiviksi.

Verkko- ja tietoturvadirektiivin yleisenä tavoitteena on kasvattaa suojan tasoa verkko- ja tietoturvaloukkauksia, -riskejä ja -uhkia vastaan. Tarkoituksena saavuttaa korkeatasoinen verkko- ja tietojärjestelmien turvallisuus EU:n alueella parantamalla varautumista kansallisella tasolla, lisäämällä EU-tason yhteistyötä sekä säätämällä riskienhallinta- ja raportointivelvoitteita yhteiskunnan toiminnan kannalta keskeisille palveluntarjoajille sekä tietyille digitaalisten palveluiden tarjoajille.

Verkko- ja tietoturvadirektiivin mukaan jäsenvaltioiden tulee laatia kansallinen verkko- ja tietojärjestelmien turvallisuutta koskeva strategia sekä määrittämään direktiivistä johtuvia viranomaistehtäviä tietoturvallisuuden varmistamiseksi ja riskien hallitsemiseksi eri toimialoilla. Jäsenvaltiot velvoitetaan myös osallistumaan keskenään yhteistyöhön uusissa EU-tason yhteistyöryhmissä tietoturvaloukkauksia koskevien tietojen sekä parhaiden kansallisten käytäntöjen vaihtamiseksi.

Viranomaistehtävien määrittely

Verkko- ja tietoturvadirektiivin mukaan jäsenvaltioiden tulee laatia kansallinen verkko- ja tietojärjestelmien turvallisuutta koskeva strategia sekä määrittämään direktiivistä johtuvia viranomaistehtäviä tietoturvallisuuden varmistamiseksi ja riskien hallitsemiseksi eri toimialoilla. Jäsenvaltiot velvoitetaan myös osallistumaan keskenään yhteistyöhön uusissa EU-tason yhteistyöryhmissä tietoturvaloukkauksia koskevien tietojen sekä parhaiden kansallisten käytäntöjen vaihtamiseksi.

Toimivaltainen viranomainen

Direktiivin 8 artiklan 1 kohdan mukaan jäsenvaltioiden on nimettävä yksi tai useampi verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen viranomainen, jonka toiminta kattaa ainakin liitteessä II tarkoitetut toimialat ja liitteessä III tarkoitetut palvelut. Jäsenvaltiot voivat antaa tämän tehtävän olemassa olevalle viranomaiselle tai olemassa oleville viranomaisille. Direktiivin 8 artiklan 2 kohdan mukaan toimivaltaisten viranomaisten on seurattava direktiivin soveltamista kansallisesti. Direktiivin 15 ja 17 artiklan mukaan toimivaltaisella viranomaisella on oltava tarvittavat valtuudet ja keinot arvioida, noudattavatko keskeisten palvelujen tarjoajat ja digitaalisten palveluiden tarjoajat direktiivin mukaisia velvollisuuksiaan, sekä tämän vaikutuksia verkko- ja tietojärjestelmien turvallisuuteen. Direktiivin 14 ja 16 artiklan mukaan direktiivissä määritellyistä poikkeamista on ilmoitettava toimivaltaiselle viranomaiselle tai CSIRT(Computer security incident response teams)-toimijalle.

Keskitetty kansallinen yhteyspiste

Toimivaltaisten viranomaisten lisäksi jäsenvaltioiden on nimettävä verkko- ja tietojärjestelmien turvallisuudesta vastaava keskitetty kansallinen yhteyspiste. Jäsenvaltiot voivat antaa tämän tehtävän olemassa olevalle viranomaiselle. Keskitetyn yhteyspisteen tehtävänä on yhteydenpito, jotta voidaan varmistaa jäsenvaltion viranomaisten rajat ylittävä yhteistyö. Keskitetyn yhteyspisteen olisi toimitettava yhteistyöryhmälle tiivistelmäraportti, joka sisältää tiedot vastaanotettujen ilmoitusten lukumäärästä sekä maininta ilmoitettujen poikkeamien luonteesta, kuten turvallisuusloukkausten tyypit, niiden vakavuus tai niiden kesto.

CSIRT-toimija

Jäsenvaltion on direktiivin mukaan nimettävä yksi tai useampi CSIRT-toimija. Toimijan on täytettävä direktiivin liitteessä I asetetut vaatimukset. CSIRT-toimija vastaa riskien ja poikkeamien käsittelystä. CSIRT-toimijan tehtäviin on sisällytettävä vähintään seuraavat tehtävät:

- poikkeamien seuranta kansallisella tasolla;
- ennakkovaroitusten, varoitusten, ja tiedotusten antaminen sekä tiedon levittäminen riskeistä ja poikkeamista asiaankuuluville sidosryhmille;
- poikkeamiin reagointi;
- dynaamisen riskin ja poikkeamien analysointi sekä tilannetietoisuus;
- CSIRT-verkostoon osallistuminen.

Lisäksi CSIRT-toimijoiden on luotava yhteistyösuhteita yksityiseen sektoriin ja edistettävä yhteisten tai standardoitujen toimintatapojen omaksumista ja käyttöä poikkeamien ja riskien käsittelymenettelyissä sekä luokittelujärjestelmissä

EU-tason yhteistyö

Verkko- ja tietoturvadirektiivissä säädetään, että EU-tasolla perustetaan yhteistyöryhmä jäsenvaltioiden keskinäisen strategisen yhteistyön ja tietojen vaihtamisen tukemiseksi ja helpottamiseksi, luottamuksen ja luotettavuuden kehittämiseksi sekä verkko- ja tietojärjestelmien korkeatasoisen ja yhtenäisen suojan varmistamiseksi unionissa. Yhteistyöryhmä muodostuu jäsenvaltioiden edustajista, komissiosta ja Euroopan unionin verkko- ja tietoturvavirasto ENISAsta (European Union Agency for Network and Information Security). Yhteistyöryhmän tehtävät on määritelty direktiivissä.

Direktiivissä säädetään myös kansallisten CSIRT-toimijoiden verkoston perustamisesta EU-tasolla. CSIRT-verkosto muodostuu jäsenvaltioiden CSIRT-toimijoiden ja EU:n instituutioiden tietotekniikan kriisiryhmän (CERT-EU) edustajista. Verkoston tehtävät on määritelty direktiivissä.

Keskeisten palveluiden tarjoajien määritteleminen

Verkko- ja tietoturvadirektiivin mukaan jäsenvaltion on määritettävä direktiivin soveltamisalan mukaisilla toimialoilla sektorikohtaiset keskeisten palvelujen tarjoajat, jotka ovat sijoittautuneet niiden alueelle. Direktiivin soveltamisalan mukaiset toimialat on määritelty direktiivin liitteessä II.

LIITE II

4 ARTIKLAN 4 KOHDASSA TARKOITETTUJEN TOIMIJOIDEN TYYPIT

Toimiala	Osa-alue	Toimijan tyyppi
1. Energia	a) Sähkö	- Sähköalan yritykset sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/72/EY (1) 2 artiklan 35 kohdassa, jotka harjoittavat kyseisen direktiivin 2 artiklan 19 kohdassa määriteltyä toimitusta - Jakeluverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/72/EY 2 artiklan 6 kohdassa - Siirtoverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/72/EY 2 artiklan 4 kohdassa
	b) Öljy	- Öljynsiirtoputkistojen haltijat - Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit
	c) Kaasu	- Maakaasun toimittajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/73/EY (2) 2 artiklan 8 kohdassa - Jakeluverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 6 kohdassa

		- Siirtoverkonhaltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 4 kohdassa - Varastointilaitteiston haltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 10 kohdassa - Nesteytetyn maakaasun käsittelylaitteiston haltijat, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 12 kohdassa - Maakaasualan yritykset, sellaisina kuin ne määritellään direktiivin 2009/73/EY 2 artiklan 1 kohdassa - Maakaasun jalostus- ja käsittelylaitteistojen haltijat
2. Liikenne	a) Lentoliikenne	- Lentoliikenteen harjoittajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 300/2008 (3) 3 artiklan 4 kohdassa

		- Lentoaseman pitäjät, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/12/EY (4) 2 artiklan 2 kohdassa, lentoasemat, sellaisina kuin ne määritellään kyseisen direktiivin 2 artiklan 1 kohdassa, mukaan lukien Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1315/2013 (5) liitteessä II olevassa 2 jaksossa luetellut ydinlentoasemat, sekä lentoasemilla sijaitsevia lisärakennelmia ja -laitteita hoitavat toimijat - Liikenteenhallinnan ylläpitäjät, jotka tarjoavat lennonjohtopalvelua, sellaisena kuin se määritellään Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004 (6) 2 artiklan 1 kohdassa
	b) Rautatieliikenne	- Rataverkon haltijat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2012/34/EU (7) 3 artiklan 2 kohdassa - Rautatieyritykset, sellaisina kuin ne määritellään direktiivin 2012/34/EU 3 artiklan 1 kohdassa, mukaan lukien palvelupaikan ylläpitäjät, sellaisina kuin ne määritellään direktiivin 2012/34/EU 3 artiklan 12 kohdassa

	c) Vesiliikenne	- Sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, sellaisina kuin ne määritellään meriliikennettä varten Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 725/2004 (8) liitteessä I, lukuun ottamatta noiden yhtiöiden liikennöimiä yksittäisiä aluksia - Euroopan parlamentin ja neuvoston direktiivin 2005/65/EY (9) 3 artiklan 1 kohdassa määriteltyjen satamien hallinnointielimet, mukaan lukien niiden satamarakenteet, sellaisina kuin ne määritellään asetuksen (EY) N:o 725/2004 2 artiklan 11 kohdassa, sekä toimijat, jotka huolehtivat tuotantolaitoksista ja laitteista satamien alueella - Euroopan parlamentin ja neuvoston direktiivin 2002/59/EY (10) 3 artiklan o alakohdassa määriteltyjen alusliikennepalvelujen tarjoajat
	d) Tieliikenne	- Tieviranomaiset, sellaisina kuin ne määritellään komission delegoidun asetuksen (EU) 2015/962 (11) 2 artiklan 12 kohdassa, jotka vastaavat liikenteenhallinnasta - Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU (12) 4 artiklan 1 kohdassa määriteltyjen älykkäiden liikennejärjestelmien ylläpitäjät

3. Pankkiala		- Luottolaitokset, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 575/2013 (13) 4 artiklan 1 kohdassa
4. Finanssimarkkinoiden infrastruktuurit		- Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU (14) 4 artiklan 24 kohdassa määriteltyjen kauppapaikkojen ylläpitäjät - Keskusvastapuolet, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 (15) 2 artiklan 1 kohdassa
5. Teveydenhuoltoala	Terveydenhuoltolaitokset (mukaan lukien sairaalat ja yksityisklinikat)	- Terveydenhuollon tarjoajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU (16) 3 artiklan g alakohdassa
6. Juomaveden toimittaminen ja jakelu		- Neuvoston direktiivin 98/83/EY (17) 2 artiklan 1 kohdan a alakohdassa määritellyn ihmisten käyttöön tarkoitetun veden toimittajat ja jakelijat, lukuun ottamatta jakelijoita, joille ihmisten käyttöön tarkoitetun veden jakelu on ainoastaan osa niiden yleistä toimintaa, joka muodostuu sellaisten muiden hyödykkeiden ja tavaroiden jakelusta, joita ei katsota keskeisiksi palveluiksi.

7. Digitaalinen infrastruktuuri		- IXP:t - Nimipalvelujen tarjoajat -Aluetunnusrekisterit

Direktiivissä on määritelty kriteerit keskeisten palvelujen tarjoajien määrittämiseksi. Direktiivin mukaan keskeisen palvelun tarjoajan on tarjottava palvelua, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi. Tämän palvelun on oltava riippuvainen verkko- ja tietojärjestelmistä. Lisäksi palveluun kohdistuvalla poikkeamalla tulisi olla merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen.

Direktiivin mukaan jäsenvaltioiden on laadittava luettelo keskeisistä palveluista. Palveluiden luettelon on sisällettävä kaikki jäsenvaltion alueella tarjottavat palvelut, jotka täyttävät direktiivin vaatimukset. Direktiivin mukaan keskeisten palvelujen tarjoajien määrittely voitaisiin tehdä esimerkiksi hyväksymällä luettelo, jossa luetellaan kaikki keskeisten palvelujen tarjoajat tai hyväksymällä toimenpiteitä, joiden avulla palvelun tarjoajat voitaisiin määrittää.

Keskeisten palveluiden tarjoajien määrittämisen kriteerinä käytettyä merkittävää haitallista vaikutusta arvioidessa jäsenvaltioiden on direktiivin mukaan huomioitava direktiivissä määritellyt seikat, kuten esimerkiksi palvelusta riippuvaisten käyttäjien lukumäärä ja toimijan markkinaosuus. Myös toimialakohtaisia tekijöitä olisi otettava huomioon määritettäessä sitä, olisiko poikkeamalla merkittävä haitallinen vaikutus keskeisen palvelun tarjoamiseen. Direktiivin johdanto-osassa on annettu tästä seuraavia esimerkkejä:

”Energiantoimittajien osalta tällaisiin tekijöihin voisi sisältyä tuotetun kansallisen energian määrä tai osuus siitä; öljyntoimittajien osalta päiväkohtainen määrä; lentoliikenteen, mukaan lukien lentoasemat ja lentoliikenteen harjoittajat, sekä rautatieliikenteen ja merisatamien osalta osuus kansallisesta liikennemäärästä ja matkustajien tai rahtikuljetusten lukumäärä vuodessa; pankkialan tai finanssimarkkinoiden infrastruktuurien osalta niiden järjestelmäkohtainen merkitys perustuen kokonaisvaroihin tai näiden kokonaisvarojen ja bruttokansantuotteen suhteeseen; terveydenhuoltoalan osalta palvelun tarjoajan hoidossa olevien potilaiden lukumäärä vuodessa; veden tuotannon, käsittelyn ja toimittamisen osalta vesimäärä sekä käyttäjien lukumäärä ja tyypit, mukaan lukien esimerkiksi sairaalat, julkiset palveluorganisaatiot tai henkilöt, sekä vaihtoehtoisten veden lähteiden olemassaolo saman maantieteellisen alueen kattamiseksi.

Jäsenvaltioiden on säännöllisesti (vähintään kahden vuoden välein) tarkistettava ja tarvittaessa saatettava ajan tasalle määritettyjen keskeisten palvelujen tarjoajien luettelo. Direktiivin mukaan keskeisten palvelujen tarjoajia määritettäessä sijoittautuminen jäsenvaltioon edellyttää tosiasiallista toimintaa ja kiinteää toimipaikkaa. Mikäli toimijat tarjoavat sekä keskeisiä että muita palveluita, on niihin sovellettava direktiivin vaatimuksia vain keskeisiksi katsottujen palveluiden osalta.

Tietoturva- ja raportointivelvoitteet

Direktiivin mukaan jäsenvaltioiden on velvoitettava keskeisten palveluiden tarjoajat sekä digitaalisen palvelun tarjoajat hallitsemaan verkko- ja tietojärjestelmiensä turvallisuuteen kohdistuvia riskejä sekä raportoimaan poikkeamista toimivaltaiselle viranomaiselle tai CSIRT-toimijalle.

Keskeisten palveluiden tarjoajia koskevat turvallisuusriskien hallitaan liittyvät velvoitteet

Direktiivin mukaan jäsenvaltioiden on velvoitettava keskeisten palveluiden tarjoajat huolehtimaan verkko- ja tietojärjestelmien tietoturvallisuuteen liittyvästä riskien hallinnasta sekä ilmoittamaan merkittävistä tietoturvapoikkeamista viranomaiselle. Verkko- ja tietojärjestelmien turvallisuudella tarkoitetaan näiden järjestelmien kykyä suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä verkko- ja tietojärjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.

Palveluntarjoajille määrättävät riskienhallintatoimenpiteet eivät saisi edellyttää jonkin tietyn kaupallisen tieto- ja viestintäteknologiatuotteen suunnittelua, kehittämistä tai valmistamista tietyllä tavalla.

Palvelun tarjoajien olisi varmistettava käyttämiensä verkko- ja tietojärjestelmien turvallisuus. Näitä ovat ensisijaisesti yksityiset verkko- ja tietojärjestelmät, joita hallinnoi niiden oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Turvallisuus- ja ilmoitusvaatimuksia olisi sovellettava huolimatta siitä, huolehtivatko palvelun tarjoajat verkko- ja tietojärjestelmiensä ylläpidosta sisäisesti vai ulkoistavatko ne sen.

Digitaalisten palveluiden tarjoajia koskevat turvallisuusriskien hallintaan liittyvät velvoitteet

Direktiivin 16 artiklan mukaan myös digitaalisen palvelun tarjoajat on velvoitettava hallitsemaan verkko- ja tietojärjestelmiin kohdistuvia riskejä ja ilmoittamaan poikkeamista toimivaltaiselle viranomaiselle tai CSIRT-toimijalle.

Digitaalisia palvelun tarjoajia ovat direktiivin liitteen III mukaisesti verkossa toimivat markkinapaikat, verkossa toimivat hakukoneet sekä pilvipalvelut. Direktiivissä on katsottu, että keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien välillä on sen kaltaisia perustavanlaatuisia eroja, että digitaalisten palveluiden tarjoajia koskevan lainsäädännön on oltava yhdenmukaisempaa.

Kun keskeisten palvelujen tarjoajien osalta jäsenvaltioden on määritettävä velvoitteiden soveltamisalaan kuuluvat keskeisten palvelujen tarjoajat, direktiiviä on sen sijaan sovellettava kaikkiin sen soveltamisalaan kuuluviin digitaalisen palvelun tarjoajiin. Komissio voi myös antaa täytäntöönpanosäädöksiä yhdenmukaistaakseen digitaalisen palvelun tarjoajia koskevat turvallisuus- ja ilmoitusvaatimukset. Jäsenvaltiot eivät voisi säätää digitaalisen palvelun tarjoajille direktiiviä pidemmälle meneviä velvollisuuksia.

Raportointivelvollisuus

Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat ilmoittavat ilman aiheetonta viivästystä toimivaltaiselle viranomaiselle tai CSIRT-toimijalle poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien keskeisten palvelujen jatkuvuuteen. Poikkeamalla tar-

koitetaan direktiivissä mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen.

Lisäksi jäsenvaltioiden tulee velvoittaa digitaalisten palveluiden tarjoajat ilmoittamaan kansallisille viranomaisille kaikista poikkeamista, joilla on merkittävä vaikutus sellaisen direktiivin liitteessä III tarjotun palvelun tarjoamiseen, jota ne tarjoavat unionissa. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää mahdollisen rajat ylittävän vaikutuksen merkittävyyden.

2.2.2 Kansainvälinen kehitys

Tietoturvallisuus on useissa valtioissa ja kansainvälisessä yhteistyössä nostettu viime vuosina keskeisempään poliittiseen asemaan. Kyberturvallisuusstrategioita on laadittu esimerkiksi lähes kaikissa EU:n-jäsenvaltioissa, Yhdysvalloissa, Australiassa, Uudessa-Seelannissa, Kanadassa, Japanissa ja Intiassa. Kyberturvallisuusstrategioiden painotukset ja kyberturvallisuuteen liittyvän viranomaistoiminnan järjestäminen valtioissa vaihtelee. Joissakin valtioissa viranomaistoiminta on liitetty läheisellä tavalla puolustushallinnon tai tiedusteluviranomaisten toimintaan, kun taas toisissa esimerkiksi viestintäpalveluja valvoville viranomaisille. Osassa valtioissa kyberturvallisuuteen liittyvät tehtävät on voitu keskittää yhden viranomaisen hoidettavaksi, kun taas toisissa ne ovat sen sijaan hajautettu useille eri viranomaisille.

Verkko- ja tietoturvadirektiivin kansallinen täytäntöönpano on edelleen käynnissä EU:n jäsenvaltioissa ja se tulee todennäköisesti vaikuttamaan merkittävällä tavalla jäsenvaltioiden lainsäädännön kehittymiseen.

Saksa

Saksassa julkaistiin vuonna 2011 kansallinen kyberturvallisuusstrategia. Strategiassa kriittisen infrastruktuurin suojaaminen kyberloukkauksilta on nostettu keskeiseksi prioriteetiksi. Kyberturvallisuusstrategiassa asetettiin tavoitteeksi arvioida mahdollisuuksia säätää yhteistyöstä lainsäädännöllä. Saksassa monisektorinen julkisen ja yksityisen välinen yhteistyö kyberloukkauksien ehkäisemiseksi ja niihin varautumiseksi sekä tiedon jakamiseksi oli toiminut jo vuodesta 2005 niin kutsutun *UP KRITIS*-toimintasuunnitelman puitteissa. Vuonna 2014 tätä toiminta suunnitelmaa edelleen vahvistettiin. Vuonna 2015 voimaan tullut ”*tietoturvallisuuslaki*” (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheits gesetz)) loi lainsäädännölliset kehykset UP KRITIS-toimintasuunnitelman mukaiselle julkisen ja yksityisen väliselle yhteistyölle yhteiskunnan kriittisten palveluiden tietoturvallisuuden parantamiseksi. Laissa asetetaan tietyille kriittisen infrastruktuurin toimijoille velvoitteita huolehtia tietoturvasta ja ilmoittaa tietoturvaloukkauksista valvovalle viranomaiselle. Lailla annetaan myös valvovalle viranomaiselle toimivalta järjestää tarkastuksia sekä määrätä sanktioita. Laissa ei määritellä tarkemmin tietoturvavelvoitteiden sisältöä, vaan tämä on jätetty toimijoille itselleen. Näiden on kuitenkin pystyttävä näyttämään, että tietoturvasta on riittävällä tasolla huolehdittu.

Saksan tietoturvallisuuslain mukaisesti BSI (Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security) eli Saksan tietoturvallisuusviranomainen on toimivaltainen valvontaviranomainen, jolle tehdään myös tietoturvallisuuslain mukaiset tietoturvaloukkausilmoitukset. Televiestintä- ja energiasektorilla sekä osittain myös posti- ja rautatiesektorin kohdalla toimivaltaisena viranomaisena toimii kuitenkin myös BnetzA (Bundes-

netzagentur). BIS:llä on myös monia muita tietoturvallisuuteen liittyviä tehtäviä, sillä se on Saksan kansallinen tietoturvaviranomainen. Viraston tehtäviin kuuluu muun muassa valtionhallinnon tietoturvallisuuden edistäminen, tietoturvallisuuden tilannekuvaa ylläpitäminen, CERT-Bund -tilannekeskuksen toiminnot, salausteknologioihin liittyvät arvioinnit sekä standardisointiin ja sertifiointiin liittyviä tehtäviä.

Ranska

Rankassa yhteiskunnan keskeisten toimintojen tietoturvallisuutta on pyritty parantaman osana kriittisen infrastruktuurin sääntelyä. Tietoturvallisuus otettiin osaksi kriittistä infrastruktuuria koskevaa vleistä lainsäädäntöä vuonna 2013 tehdyllä lainmuutoksella (niin kutsuttu *CIIP-laki,* loi n° 2013-1168 du 18 décembre 2013*).* Lakiin sisältyy tietoturvallisuutta koskevia säännöksiä riskienhallintavelvoitteista sekä velvoitteista poikkeamista ilmoittamiseksi. CIIP-laissa määritellyistä tietoturvaloukkauksista tulee ilmoittaa Ranskan kansalliselle kyberturvallisuusviranomaiselle (ANSSI, Agence nationale de la sécurité des systèmes d'information).

CIIP-lakia tarkentavat toimialakohtaiset pääministerin määräykset (arrêté du Premier ministre). Määräykset on valmisteltu ANSSI:n toimesta perustuen julkisen ja yksityisen yhteistyössä kehitettyihin toimenpidesuosituksiin.

ANSSI on Ranskan puolustushallinnon alainen viranomainen. Se on kansallinen kyberpuolustus- sekä verkko- ja tietoturvaviranomainen (decree n°2011-170) ja toimii ulkoisesta ja kansallisesta turvallisuudesta vastaavan viranomaisen (Secrétariat général de la Défense et de la Sécurité nationale) yhteydessä. ANSSI:n yhteydessä toimii myös tietoturvallisuudentilannekeskus (CERT-FR).

Ranska on antamassa verkko- ja tietoturvadirektiivin täytäntöönpanoa koskevan lakiehdotuksen vuoden 2017 aikana.

Ruotsi

Ruotsissa ei ole verkko- ja tietoturvadirektiivin kaltaista kansallista lainsäädäntöä. Ruotsissa verkko- ja tietoturvadirektiivin kansallisen täytäntöönpanon valmistelusta vastannut selvitysmies on antanut alkuvuodesta 2017 raportin (Informationssäkerhet för samhällsviktiga ocg digitala tjänster, Betänkande av Utredningen om genomförande av NIS-direktivet, SOU 2017:36) direktiivin implementointia koskevista toimenpiteistä sekä ehdotuksen kansallisen lainsäädännön sisällöksi. Selvitysmies ehdottaa, että verkko- ja tietoturvadirektiivin saattamiseksi osaksi Ruotsin lainsäädäntöä säädettäisiin kokonaan uusi yhteiskunnan toiminnan kannalta keskeisten palvelujen tietoturvallisuutta koskeva laki sekä annettaisiin sitä täydentävä asetus.

Selvitysmiehen raportissa ehdotetaan huoltovarmuudesta vastaavan kansallisen viranomaisen MSB:n (Myndigheten För Samhällsskydd och Beredskap, Swedish Civil Contingencies Agency) tehtäväksi arvioida ja päivittää luetteloa yhteiskunnan toiminnan kannalta keskeisistä palveluista. Raportin mukaan arvioinnissa tulisi erityisesti huomioida, millainen vaikutus tietoturvahäiriöllä olisi palvelun tarjoamiseen.

Raportissa ehdotetaan, että verkko- ja tietoturvadirektiivin mukaisista poikkeamista ilmoitettaisiin MSB:lle. Lisäksi MSB:lle ehdotetaan verkko- ja tietoturvadirektiivin mukaisen keskite-

tyn yhteyspisteen ja kansallisen CSIRT-toimijan tehtäviä. MSB:n lakisääteisiin tehtäviin kuuluu kuitenkin kyberturvallisuusasioita laajemmin yleisestä turvallisuuteen, siviilien suojaamiseen sekä hätä- ja poikkeustilanteiden organisoimiseen liittyviä tehtäviä. Tämän vuoksi raportissa ehdotetaan, että sektorikohtaisille valvontaviranomaisille (Statens energimyndigheten (energia), Transportstyrelsen (liikenne), Finansinspektionen (pankkiala ja finanssimarkkinoiden infrastruktuuri), Inspektionen för vård och omsorg (terveydenhuolto), Livsmedelsverket (juomaveden toimittaminen ja jakelu), Post- och telestyrelsen (digitaalinen infrastruktuuri ja digitaalisten palveluiden tarjoajat)) annettaisiin direktiivin mukaiset toimivaltaisen viranomaisen valvontatehtävät.

Iso-Britannia

Iso-Britannian hallitus on julkaisut kyberturvallisuutta koskevan kansallisen strategian vuosille 2016-2020. Strategian yhtenä toimenpiteenä Britanniassa perustettiin uusi keskitetty kyberturvallisuusviranomainen, jonka tehtäviä ovat muun muassa kriittisen infrastruktuurin tietoturvallisuuden parantaminen, tietoturvaloukkauksien tutkiminen, haavoittuvuuksien tiedottaminen sekä yleinen tietoturvallisuustietoisuuden edistäminen (The National Cyber Security Centre). Kyberturvallisuuskeskus on osa Yhdistyneen kuningaskunnan tiedustelu- ja turvallisuuspalvelu GCHQ:ta (Government Communications Headquarters), joka on vastuussa muun muassa hallituksen ja armeijan puolesta suoritettavasta signaalitiedustelusta ja tietoturvasta. Kyberturvallisuuskeskuksessa toimii myös tietoturvallisuuden tilannekeskus (CERT UK). Tietosuojaan ja sähköiseen viestintään liittyviä tietoturvallisuustehtäviä on Iso-Britanniassa myös tietosuojaviranomaisella (Information Commissioner's Office ICO).

Iso-Britanniassa ei ole verkko- ja tietoturvadirektiivin kaltaista kansallista lainsäädäntöä. Direktiivi tullaan Britannian EU-erosta huolimatta todennäköisesti saattamaan osaksi kansallista lainsäädäntöä. Iso-Britannia on aloittanut elokuussa 2017 julkisen kuulemisen direktiivin täytäntöönpanosta. Julkista kuulemisen tueksi julkaistussa muistiossa (Security of Network and Information Systems, Public Consultation) on määritelty kansallisen täytäntöönpanon alustavia suuntaviivoja.

Yhdysvallat

Yhdysvalloissa kyberturvallisuuden poliittisia ja strategiasia linjauksia on kuvattu useissa eri strategioissa. Myös tietoturvallisuuteen liittyvää lainsäädäntöä sisältyy vähäisesti niin liittovaltion kuin osavaltioiden lakeihin, muihin säännöksiin sekä käytäntöihin. Osa lainsäädännöstä koskee joitakin tiettyjä toimintoja, kun taas osa ulottuu laajemmin yhteiskunnan eri sektoreille (esimerkiksi tietosuojaliitännäisten tietoturvaloukkausten ilmoitusvelvollisuus). Myös tietoturvallisuuteen liittyvää viranomaistoimintaa on niin liittovaltion kuin osavaltioidenkin tasolla. Huolimatta voimassa olevasta lainsäädännöstä, liittovaltion tasolla ei ole säädetty varsinaisesti tietoturvavelvoitteista yhteiskunnan toiminnan kannalta keskeisille toimijoille. Sen sijaan yhteiskunnan toiminnan kannalta keskeisten palveluiden tietoturvallisuutta on pyritty parantamaan yritysten kanssa yhteistyössä. Kansallinen standardointeihin ja teknologiaan erikoistunut instituutti (National Institute of Standards and Technology, NIST) on laatinut suosituksen kriittisen infrastruktuurin tietoturvallisuuden edistämiseksi (Framework for Improving Critical Infrastructure Cybersecurity, 2014). Suositus sisältää konkreettisia riskienhallintaan liittyviä toimenpidesuosituksia sekä ohjeita, jotka perustuvat olemassa oleviin tietoturvastandardeihin. Suosituksen laatiminen liittyi läheisesti presidentti Obaman antamaan presidentin asetukseen (Executive order 13636 – Improving Critical Infrastructure Cybersecurity), joka asettaa valti-

on virastoille velvoitteita esimerkiksi kehittää teknologianeutraali ja vapaaehtoinen kyberturvallisuuskehikko, edistää ja kannustaa kyberturvallisten käytäntöjen omaksumista, lisätä oikea-aikaista, määrällistä ja laadullista tietojen jakamista kyberturvallisuusuhista, sisällyttää vahva yksityisyyden ja kansalaisvapauksien suoja jokaiseen aloitteeseen jahankkeeseen sekä suojata kriittistä infrastruktuuria ja tutkia voimassa olevan sääntelyn käyttö kyberturvallisuuden edistämiseksi.

2.3 Nykytilan arviointi

2.3.1 Tietoturvallisuusstrategia

Verkko- ja tietoturvadirektiivi edellyttää, että kunkin jäsenvaltion tulee laatia kansallinen strategia, jossa määritellään puitteet, visio, tavoitteet ja painopisteet verkko- ja tietoturvallisuudesta kansallisella tasolla.

Liikenne- ja viestintäministerin maaliskuussa 2016 hyväksymässä tietoturvallisuusstrategiassa on korostettu, että Suomen oikeusjärjestyksen mukaisena lähtökohtana voidaan pitää sitä, että verkko- ja tietoturvallisuuden puitteet, tavoitteet ja painopisteet määritellään ensisijaisesti voimassaolevassa lainsäädännössä. Perustuslain oikeusvaltioperiaate edellyttää, että julkisen vallan käytön tulee perustua lakiin. Myös tietoturvaan liittyvien viranomaisvastuiden tulee perustua lainsäädäntöön. Strategiassa esitetään tavoitteita lainsäädännön laadun varmistamiseksi siltä osin kuin lainsäädännöllä voi olla vaikutuksia verkko- ja tietoturvallisuuteen ja sitä kautta digitaalisen liiketoiminnan kasvuympäristön kehittymiseen. Strategian toimenpiteiden täytäntöönpano on osoitettu strategiassa vastuullisille viranomais- tai muille tahoille. Vastuunjako perustuu nykyiseen lainsäädäntöön viranomaisten toimivaltuuksista. Strategialla laitetaan täytäntöön verkko- ja tietoturvadirektiivin 7 artikla.

2.3.2 Tietoturvaloukkauksiin reagointi ja niiden tutkinta

Viestintäviraston tietoyhteiskaaren mukaiset tehtävät ovat kattavat tietoturvaloukkauksiin reagoimiseksi sekä loukkauksien tutkimiseksi.

Verkko- ja tietoturvadirektiivin 9 artiklan mukaisten CSIRT-toimijoiden tehtävät sisältyvät lähtökohtaisesti Viestintäviraston tietoyhteiskuntakaaren mukaisiin lakisääteisiin tehtäviin. Viestintäviraston CERT-toiminnon nykyiset tehtävät vastaavat pitkälti CSIRT-toimijan tehtäviä, mutta ne eivät rajoitu vain verkko- ja tietoturvadirektiivin soveltamisalueelle. CERT-toiminto tarjoaa apua tietoturvaloukkausten käsittelyssä kaikille suomalaisille, Suomessa asuville ja Suomessa toimiville oikeustoimihenkilöille. Kuka tahansa voi ilmoittaa Viestintävirastolle Suomea tai suomalaisia koskevista tietoturvaloukkauksista tai sellaisen uhasta. Lisäksi Viestintävirasto on valtiovarainministeriön toimeksiannosta Suomen GovCERT, eli valtionhallintoon vaikuttavia tietoturvaloukkauksia ja -uhkia käsittelevä viranomainen. Viestintävirasto tuottaa lisäksi CERT-palveluja Suomeen sijoittuneille huoltovarmuuskriittisille yrityksille Huoltovarmuuskeskuksen myöntämällä rahoituksella.

Viestintäviraston toiminta täyttää jo nykyisellään verkko- ja tietoturvadirektiivin artiklassa 9 ja direktiivin liitteessä I luetellut CSIRT-toimijalle asetetut vaatimukset, mukaan lukien kyvykkyys reagoida poikkeamiin ympäri vuorokauden, analysoida poikkeamia, muodostaa tilannekuvaa, antaa ennakkovaroituksia ja levittää tietoa tietoturvariskeistä. Lisäksi Viestintävirastolla on aktiiviset suhteet yksityiseen sektoriin. Suhteet perustuvat vapaaehtoisuuteen, yhteis-

työn luottamuksellisuuteen ja siihen, että Viestintävirasto pystyy tarjoamaan palveluntarjoajille tietoturvallisuuden ylläpitämiseen liittyvää tukea poikkeamien havainnointiin, tietoa poikkeamista toipumiseen ja varoituksia riskeistä. Virasto tarjoaa myös mahdollisuuden verkostoitua muiden toimijoiden tietoturva-asiantuntijoiden kanssa. Poikkeamista ilmoittaminen ja tiedonvaihto perustuvat toimijoiden keskinäiseen luottamukseen ja tiedon analysointi toimijoiden suostumukseen. Viestintävirastolla on lisäksi toimivat yhteydet muiden EU:n jäsenmaiden olemassa oleviin CSIRT tai CERT-toimijoihin.

Verkko- ja tietoturvadirektiivin 8 artiklan mukaisen keskitetyn yhteyspisteen tehtävänä on direktiivin mukaan yhteydenpito jäsenvaltioiden viranomaisten rajat ylittävän yhteistyön varmistamiseksi.

Keskitetyn yhteyspisteen olisi tarkoituksenmukaista toimia CSIRT-toimijan yhteydessä Viestintävirastossa.

Vaikka edellä kuvatut viranomaistehtävät lähtökohtaisesti sisältyvät jo Viestintäviraston nykyisiin lakisääteisiin tehtäviin, johtuen verkko- ja tietoturvadirektiivin laajasta soveltamisalasta, olisi Viestintäviraston erityisiä tehtäviä sekä oikeutta tehdä yhteistyötä muiden viranomaisten ja verkko- ja tietoturvadirektiivin mukaisten yhteistyöelinten kanssa tarpeen tarkentaa.

2.3.3 Yhteiskunnan toiminnan kannalta keskeiset palvelut ja keskeisten palveluiden tarjoajat

Verkko- ja tietoturvadirektiivi velvoittaa jäsenvaltiot määrittämään direktiivin soveltamisalan mukaisilla toimialoilla ja niiden osa-alueilla keskeisten palvelujen tarjoajat, jotka ovat sijoittautuneet niiden alueelle. Direktiivin soveltamisalan mukaiset toimialat ja niiden osa-alueet on määritelty direktiivin liitteessä II.

Direktiivin 5 artiklassa on määritelty kriteerit keskeisten palvelujen tarjoajien määrittämiseksi. Direktiivin mukaan keskeisen palvelun tarjoajan on tarjottava palvelua, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi. Tämän palvelun on oltava riippuvainen verkko- ja tietojärjestelmistä. Lisäksi palveluun kohdistuvalla poikkeamalla tulisi olla direktiivin 6 artiklassa tarkoitettu merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen. Direktiivi jättääkin jäsenvaltioille erittäin huomattavaa liikkumavaraa keskeisten palveluiden määrittelemisessä.

Direktiivin johdanto-osan mukaan keskeisten palveluiden tarjoajat voidaan määritellä hyväksymällä luettelo keskeisten palveluiden tarjoajista tai hyväksymällä kansallisia toimenpiteitä, joiden avulla voidaan määrittää, mihin toimijoihin sovelletaan verkko- ja tietojärjestelmien turvallisuutta koskevia kriteerejä.

Kuten nykytilan kuvauksen yhteydessä on todettu, Suomessa ei ole määritelty kriittistä infrastruktuuria tai yhteiskunnan toiminnan kannalta keskeisiä toimintoja lainsäädännön tasolla eikä voimassa olevaan lainsäädäntöön sisälly varsinaisesti menettelyjä, joiden nojalla verkko- ja tietoturvadirektiivin mukaisia keskeisiä palveluntarjoajia voitaisiin esimerkiksi valvontaviranomaisten puolesta suoraan määrittää. Olemassa olevat hallinnolliset rakenteet ja voimassa oleva lainsäädäntö huomioiden keskeisten palveluiden tarjoajien määrittäminen olisi luontevinta tehdä verkko- ja tietoturvadirektiivin täytäntöönpanoa koskevan lainsäädännön antamisen yhteydessä.

Verkko- ja tietoturvadirektiivin mukaan keskeisten palvelun tarjoajien on tarjottava palvelua, joka on yhteiskunnan toiminnan kannalta keskeistä. Direktiivi jättää keskeisyyden arvioinnin jäsenvaltioiden harkintaan.

Yhteiskunnan toiminnan kannalta keskeisten palveluiden määrittäminen on kullakin direktiivin mukaisella toimialalla ja niiden osa-alueella riippuvaista toimialakohtaisista erityispiirteistä. Palveluiden keskeisyyteen vaikuttaa muun muassa palveluiden merkitys kansalaisille ja yrityksille, teollisuuden riippuvaisuus kyseisistä palveluista sekä se kuinka paljon erilaisia kilpailevia palveluita on markkinoilla saatavilla. Yhteiskunnan toiminnan kannalta keskeiset palvelut voivat olla huoltovarmuuskriittisiä tai kriittistä infrastruktuuria laajempi joukko toimijoita.

Direktiivin mukaan keskeisen palvelun on oltava lisäksi riippuvaista verkko- ja tietojärjestelmistä. Direktiivi jättää myös tämän riippuvuuden arvioinnin jäsenvaltioiden harkintaan. Arvioidessa riippuvuutta on huomioitava, miten palvelun tarjoaminen on järjestetty. Lähtökohtaisesti voidaan olettaa, että suuri osa palveluista on nykyään tavalla tai toisella riippuvaisia viestintäverkkojen ja tietojärjestelmien käytöstä.

Direktiivissä säädetään myös, että palveluun kohdistuvalla poikkeamalla tulisi olla merkittäviä haitallisia vaikutuksia palvelun tarjoamiseen. Direktiivissä on määritelty, että merkittävää haitallista vaikutusta arvioitaessa on otettava huomioon palvelusta riippuvaisten käyttäjien lukumäärä, muiden keskeisten palveluiden riippuvaisuus kyseisen toimijan tarjoamasta palvelusta, poikkeamien vaikutus talouden ja yhteiskunnan toimintoihin tai yleiseen turvallisuuteen, toimijan markkinaosuus, toimijan maantieteellinen levinneisyys alueella, johon poikkeama saattaa vaikuttaa sekä palvelun tarjoamista koskevien vaihtoehtoisten keinojen saatavuus. Direktiivissä luetellut velvoitteet ovat sellaisia, että niitä on arvioita kansallisesti toimiala- ja palvelukohtaisesti.

Liikenne- ja viestintäministeriö asetti lokakuussa 2016 poikkihallinnollisen työryhmän tukemaan verkko- ja tietoturvadirektiivin kansallisessa täytäntöönpanossa. Työryhmä on esittänyt loppuraportissaan, että direktiivin mukaiset keskeisten palveluiden tarjoajat määriteltäisiin lain tasolla. Velvoitteiden kohdentamiseksi on arvioitava mitä palveluita on kansallisesti pidettävä direktiivin tarkoittamina yhteiskunnan kannalta keskeisinä palveluina direktiivin soveltamisalan mukaisilla toimialoilla. Tämän jälkeen on tarkasteltava, onko näiden palveluiden tarjoajat jo voimassa olevan lainsäädännön nojalla velvoitettu huolehtimaan tietoturvasta vähintään direktiivin velvoitteita vastaavalla tasolla. Mikäli vastaus on kyllä, ei uusia velvoitteita ei ole tarpeellista säätää. Sen sijaan sellaisten palveluiden, joiden tarjoajille ei ole säädetty direktiivin valossa riittäviä velvoitteita voimassa olevassa lainsäädännössä, osalta keskeisten palvelun tarjoajien määrittäminen on tehtävä osana uusien velvoitteiden säätämistä.

Energia

Verkko- ja tietoturvadirektiivin mukaan keskeiset palvelut ja keskeisten palveluiden tarjoajat on määriteltävä energian toimialalla sähkön, öljyn ja kaasun osa-alueella.

Yhteiskunnan toiminta on nykyisin erittäin riippuvaista erilaisista sähköisistä järjestelmistä. Myös lähes kaikki yhteiskunnan toiminnan kannalta keskeiset palvelut tarvitsevat palveluidensa tuottamiseen sähköä. Sähkönjakelulla on niin merkittävä rooli yhteiskunnan toiminnan kannalta merkittävien palveluiden tarjoamisen ja jatkuvuuden kannalta, että sen on katsot-

tava olevan aina keskeistä palvelua sen asiakkaille riippumatta esimerkiksi sähkönjakeluverkon koosta.

Suomen sähköverkkoon kuuluvat kantaverkko, alueverkot ja jakeluverkot. Kantaverkossa sähköä siirretään voimantuotantoalueilta ja ulkomailta kulutuskeskittymiin. Valtaosa Suomessa käytettävästä sähköstä kulkee kantaverkon kautta. Osa sähköä tuottavista voimalaitoksista on liittynyt suoraan kantaverkkoon samoin kuin suuret kuluttajat, esimerkiksi isot tehtaat. Voimalaitokset voivat liittyä myös alue- tai jakeluverkkoon. Esimerkiksi sähköistetyt rautatieosuudet ottavat ajosähkön kantaverkosta, samoin Helsinki-Vantaan lentokenttä. Suomessa on 77 sähkönjakeluverkon haltijaa sekä 11 suurjännitteisen jakeluverkon haltijaa. Sähkön järjestelmävastuullinen kantaverkonhaltija on Fingrid Oyj.

Sähkönjakelun osalta verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisena palveluna, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi, voidaan pitää lähtökohtaisesti

1) siirtopalvelua kantaverkossa ja järjestelmävastaavan kantaverkonhaltijan tarjoamia järjestelmäpalveluita

2) sähkönjakelua jakeluverkossa, ei kuitenkaan sähkönjakelua suljetussa jakeluverkossa

3) sähkönjakelua suurjännitteisessä jakeluverkossa, ei kuitenkaan sähkönjakelua suljetussa jakeluverkossa

Kaasun osa-alueella maakaasulla on merkittävä asema Suomen energiankulutuksessa. Maakaasun osuus Suomen energiankulutuksesta on noin kahdeksan prosenttia. Maakaasua käytetään erityisesti kaukolämmön ja sähkön yhteistuotannossa. Lisäksi merkittävä käyttökohde maakaasulle ovat teollisuuden valmistusprosessit. Suomessa käytettiin vuonna 2016 maakaasua 23,8 terawattituntia.

Maakaasun käytön kannalta on keskeistä, että maakaasun siirtotoiminta ja maakaasun siirtoverkko toimii häiriöttömästi. Tämän johdosta verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisena palveluna, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi, voidaan pitää lähtökohtaisesti maakaasumarkkinalain mukaistaen siirtopalvelua siirtoverkossa ja järjestelmävastaavan siirtoverkonhaltijan tarjoamia järjestelmäpalveluita.

Öljyn osa-alueella ei ole tunnistettu direktiivissä asetetut kriteerit täyttäviä keskeisiä palveluita tai keskeisten palveluiden tarjoajia.

Liikenne

Liikenteen alueella tarjottavat palvelut voidaan karkeasti jaotella kolmeen eri tasoon, liikenteenohjauspalveluihin, keskeisen infrastruktuurin ylläpitämiseen sekä liikennepalveluiden tarjontaan. Palveluiden luonne liikennejärjestelmän eri tasoilla vaihtelee.

Liikenteenohjauspalvelut

Liikenteenohjaus on liikennejärjestelmän toimivuuden kannalta keskeistä ja vaikuttaa välittömästi koko liikennejärjestelmän turvallisuuteen. Häiriöt liikenteenohjauksessa voivat johtaa

suoraan liikenneturvallisuuden vaarantumiseen taikka liikenteen keskeytymiseen. Lisäksi liikenteenohjaustoiminnot ovat keskitetysti riippuvaista pienestä joukosta toimijoita. Liikenteenohjauksen merkitys liikennejärjestelmän toimivuudelle ja turvallisuudelle tullee tulevaisuudessa edelleen korostumaan liikenteen älykkään automaation yleistyessä.

Ilmailun osalta liikenteenohjauksesta vastaavat lennonvarmistuspalvelut. Lennonvarmistuspalvelulla tarkoitetaan ilmailulain 160 §:n mukaan ilmaliikennepalvelua, viestintä-, suunnistus- ja valvontapalvelua, lennonvarmistukseen tarkoitettua sääpalvelua sekä ilmailutiedotuspalvelua. Suomessa lennonvarmistuspalveluja tarjoaa valtion kokonaan omistama yhtiö Air Navigation Services Finland Oy (ANS Finland). ANS Finland vastaa lennonvarmistukseen liittyvistä erityistehtävistä, kuten ilmatilan hallinnasta, aluevalvonnasta, palveluista valtion ilmailulle ja lentopelastuspalvelusta. Valtioneuvosto on nimennyt Ilmatieteen laitoksen ilmailulain 108 §:n mukaiseksi lentosääpalvelujen tarjoajaksi Suomessa.

Rautatieliikenteen osalta liikenteenohjauksesta vastaa rautatielain 36 §:n mukaan hallinnoimallaan rataverkolla rataverkon haltija. Rataverkon haltija voi järjestää liikenteenohjauspalvelut itse tai hankkia ne julkisilta tai yksityisiltä palvelujen tuottajilta. Liikennevirasto vastaa rautatieliikenteen ohjauksen operatiivisen toiminnan valvonnasta ja koordinoinnista. Itse operatiivinen rautatieliikenteen ohjaus on ostettu Finrail Oy:ltä.

Vesiliikenteessä liikenteenohjauksesta vastaa alusliikennepalvelu. Alusliikennepalvelulain mukaan alusliikennepalvelulla (Vessel Traffic Service, VTS) tarkoitetaan alusliikenteen valvontaa ja ohjausta, jolla on valmiudet toimia vuorovaikutuksessa liikenteen kanssa ja reagoida muuttuviin liikennetilanteisiin. VTS-viranomainen hoitaa alusliikennepalvelua. Alusliikennepalvelulain mukaan VTS-viranomaisena toimii Liikennevirasto.

Liikenteenohjauksen rooli tieliikenteen osalta eroaa vaikutuksiltaan osittain muista liikennemuodoista. Vielä toistaiseksi liikennettä ohjataan merkittävissä määrin liikennesäännöillä ja sellaisilla liikenteenohjauslaitteilla, jotka eivät ole riippuvaisia viestintäverkoista ja tietojärjestelmistä (tiemerkinnät, liikennemerkit).

Liikenteenohjauspalvelua voidaan pitää lähtökohtaisesti verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisena palveluna, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi. Eri liikennemuotoja koskien keskeisiä palveluita olisivat siis lennonvarmistuspalvelu, rautatieliikenteen ohjauspalvelu sekä alusliikennepalvelu. Tieliikenteen ohjausta ei toistaiseksi olisi pidettävä verkko- ja tietoturvadirektiivin kannalta yhteiskunnan kannalta keskeisenä palveluna. Liikenteen älykkään automaation kehittyessä tätä tulee kuitenkin arvioida uudelleen.

Keskeisen liikenneinfrastruktuurin ylläpitäminen

Liikenteenohjauksen lisäksi useiden liikennepalvelujen tarjoaminen on riippuvaista keskeisestä liikenneinfrastruktuurista eikä liikennepalveluja ole usein mahdollista tarjota vaihtoehtoisella tavalla, mikäli keskeinen infrastruktuuri olisi poissa käytöstä. Keskeistä liikenneinfrastruktuuria ovat erityisesti lentoasemat, satamat, rautatiet ja tieverkko.

Lentoasemat ovat Suomessa merkittävässä asemassa matkustajaliikenteessä ja lentomatkustajien määrä kasvaa jatkuvasti. Suomen lentomatkustajien määrä ylitti vuonna 2016 16 miljoonan matkustajan rajan. Finavian lentokenttien kautta kulki kahdeksan prosenttia enemmän

matkustajia kuin vuotta aiemmin. Tavaraliikennettä Finavian lentokenttien kautta kulki vuonna 2016 yhteensä 183 442 tonnia. Lentorahdin osuus ulkomaankaupan arvosta on noin kymmenen prosenttia.

Lentoasemalla palveluja tarjoaa useat eri palveluiden tarjoajat. Infrastruktuurin ylläpidon kannalta keskeisimmässä asemassa on kuitenkin lentoaseman pitäjä, joka vastaa lentoaseman hallinnasta. Ilmailulaissa on säädetty lentoaseman hyväksyntätodistuksen myöntämisen edellytyksistä. Lentoaseman pitäjä vastaa myös esimerkiksi ilmailun turvaamiseen tähtäävien toimenpiteiden ja järjestelyiden toimeenpanosta. Lentoaseman pitäjälle on säädetty myös varautumiseen liittyviä velvoitteita.

Lentoasemien lisäksi osa keskeistä liikenneinfrastruktuuria ovat satamat. Ulkomaan kaupan kuljetuksista merikuljetuksia oli vuonna 2014 96 milj. tonnia ja maakuljetuksia n. 11 miljoonaa tonnia. Suomen ulkomaankaupassa liikkuvasta tavarasta tonnikilometreissä 96 prosenttia kulkee merirahtina. Siten elinkeinoelämä ja koko muu yhteiskunta ovat hyvin riippuvaisia satamien toiminnasta. Kuten lentoasemalla, myös satamassa palveluita tarjoaa useita eri toimijoita. Satamanpitäjän vastuulla on ylläpitää satamaa ja satamarakennetta. Satamanpitäjän vastuista säädetään eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetussa laissa.

Myös rautatiet ovat keskeisiä niin henkilö- kuin tavarakuljetuksessa. Henkilömatkustajien määrä vuonna 2016 rautateillä oli noin 82 miljoonaa. Rautateiden tavarakuljetusten määrä oli vuonna 2014 37 miljoonaa tonnia ja kuljetussuorite oli noin 9,6 miljardia tonnikilometriä. Rataverkonhaltija ylläpitää, kehittää ja pitää kunnossa rataverkkoa. Valtion rataverkonhaltijalla tarkoitetaan rautatielain mukaan Liikennevirastoa. Yksityisraiteilla tarkoitetaan sen sijaan muuta kuin valtion omistamaa ja Liikenneviraston hallinnoimaa raidetta. Tällaisten raiteiden haltijoita voivat olla esimerkiksi kunnat, satamat tai yritykset. Yksityisraiteet voivat sinänsä olla esimerkiksi tietyn teollisuuslaitoksen tai esimerkiksi sataman kannalta merkityksellisiä. Niiden ylläpitäminen ei kuitenkaan ole samalla tavalla yhteiskunnan toiminnan kannalta keskeistä kuin valtion rautateiden.

Myös tieverkko on keskeinen osa liikenneinfrastruktuuria. Tietoturvallisuuden kannalta tieverkon ylläpitämisessä keskeistä on erityisesti tieinfrastruktuurin liittyvät digitaaliset tietojärjestelmät. Tällaisia tietojärjestelmiä ovat erityisesti ITS-direktiivin mukaiset ITS-järjestelmät. ITS-direktiivi on Suomessa saatettu osaksi liikennekaarta. Liikennekaaren III osan 2 luvun 6 §:ssä säädetään älykkäiden liikennejärjestelmien käyttöönotosta. Tällä hetkellä eCall-hätäpuhelujärjestelmää sekä Liikenneviraston ylläpitämiä Digiroad (väylätieto)- ja Digitraffic (liikennetieto)-palveluita voidaan pitää ITS-direktiivin mukaisena älykkäinä liikennejärjestelminä. ECall järjestelmää ylläpitää Hätäkeskuslaitos.

Digiroad on Liikenneviraston ylläpitämä kansallinen tietojärjestelmä, johon on koottu koko Suomen tie- ja katuverkon keskilinjageometria sekä tärkeimmät ominaisuustiedot. Digiroad tarjoaa digitaalisessa muodossa oleva liikenneverkon kuvauksen. Digitraffic on Liikenneviraston palvelu, jonka kautta on saatavissa ajantasaista liikennetietoa Suomen tieverkolta sekä rautatie- ja vesiliikenteestä.

Keskeisen liikenneinfrastruktuurin hallintaa voidaan pitää lähtökohtaisesti verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisena palveluna, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi. Eri liikennemuotoja koskien keskeisiä palveluita

olisivat siis lentoaseman, sataman ja valtion rataverkon hallinta sekä ITS direktiivin tarkoittamien ITS-järjestelmien ylläpitäminen.

Liikennepalvelut

Liikenteenohjauksen ja liikenneinfrastruktuurin ylläpitämisen lisäksi liikenteen alueella tarjotaan monenlaisia liikennepalveluita (esimerkiksi lentoliikenteen harjoittajat, varustamot, rautatieliikenteen harjoittajat). Liikennepalveluiden keskeisyys yhteiskunnan toiminnan kannalta eroaa osittain kuitenkin edellä kuvatuista liikenteenohjaukseen ja infrastruktuurin ylläpitämiseen liittyvistä palveluista. Liikennepalveluita voi tarjota useita kilpailevia toimijoita. Tämän lisäksi voi olla keinoja järjestää palvelu vaihtoehtoisella tavalla. Vaikka joidenkin liikennemuotojen osalta kotimaisten palveluiden tarjoaminen on keskittynyt harvoille tai jopa vain yhdelle toimijalle (esimerkiksi lentoliikenne ja raideliikenne), vaihtoehtoisia tapoja järjestää palvelu on kuitenkin yleensä saatavilla johtuen joko kansainvälisestä kilpailusta tai vaihtoehtoisesta kuljetusmuodosta. Liikennepalvelujen luonne on kasvavasti muuttumassa kansainväliseen suuntaan. Esimerkiksi ilmailun osalta tämä on jo johtanut siihen, että globaalia yhteistä ilmailujärjestelmää pyritään säätelemään kansainvälisesti yhtenevällä tavalla. Tämän johdosta onkin katsottava, että liikennepalvelujen tarjoajien osalta myös tietoturvallisuutta voidaan tulevaisuudessa kehittää kohdennetummin ja harmonisoidummin osana kulkumuotokohtaisten kansainvälisten sopimusvelvoitteiden ja EU-säädösten valmistelua. Näin voitaisiin välttää erilaisesta kansallisesta sääntelystä mahdollisesti aiheutuvat liikennejärjestelmän toimintaan, turvallisuuteen ja kansainvälisiin kilpailuedellytyksiin kohdistuvat häiriöt.

Pankkiala ja finanssimarkkinoiden infrastruktuurit

Pankkialan ja finanssimarkkinoiden infrastruktuurin osalta ei verkko- ja tietoturvadirektiivin liitteessä II ole määritelty tarkempia osa-alueita, joilla direktiivin mukaiset yhteiskunnan toiminnan kannalta keskeiset palvelut on määriteltävä. Direktiivin liitteessä on toimijoiden tyyppeinä mainittu luottolaitokset, Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU 4 artiklan 1 kohdassa määriteltyjen kauppapaikkojen ylläpitäjät sekä keskusvastapuolet. Pankkialalla ja finanssimarkkinoiden keskeisen infrastruktuurin osalta verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisena palveluna, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi olisi Suomessa pidettävä luottolaitoslain mukaista luottolaitostoimintaa sekä kaupankäynnistä rahoitusvälineillä annetun lain mukaisen pörssitoiminnan harjoittamista. Suomessa ei toimi direktiivin soveltamisalaan kuuluvia keskusvastapuolia.

Terveydenhuoltoala

Terveydenhuollon tavoitteena on edistää ja ylläpitää väestön terveyttä, hyvinvointia, työ- ja toimintakykyä ja sosiaalista turvallisuutta sekä kaventaa terveyseroja. Terveydenhuollon häiriötön toimiminen ja jatkuvuus ovat yhteiskunnan toiminnan kannalta keskeistä. Palveluntarjoajina terveydenhuollon alueella toimivat julkisten ja yksityisten sosiaalihuollon ja terveydenhuollon palvelujen antajat. Tietoturvallisuuden näkökulmasta yhteiskunnan kannalta merkittävimmät haitalliset vaikutukset voisivat olla sellaisiin järjestelmiin kohdistuvilla tietoturvallisuuteen liittyvillä häiriöillä, joissa käsitellään potilaiden asiakastietoja tai jotka sisältyvät terveydenhuollossa käytettäviin laitteisiin. Tämän johdosta verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisena palveluna, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi, olisi pidettävä terveydenhuollon asiakastietojen sähköistä kä-

sittelyä sekä terveyden huollon laitteiden ylläpitäminen ja käyttäminen julkisten ja yksityisten sosiaalihuollon ja terveydenhuollon palvelujen tarjonnassa.

Juomaveden toimittaminen ja jakelu

Toimiva vesihuolto on yhteiskunnan perustoimintojen kannalta elintärkeää. Vesihuolto on sähkönsaannin ohella yhteiskunnan tärkeimpiä palveluita, jonka tulisi toimia kaikissa olosuhteissa. Vesihuollon merkitys on suuri erityisesti kotitalouksissa juomavetenä ja hygienian ylläpidossa, terveydenhuollossa sekä elintarvike - ja muussa teollisuudessa.

Vesihuoltolaitokset huolehtivat yhdyskunnan vesihuollosta. Vesihuoltoa olisi pidettävä verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisena palveluna, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi.

Digitaalinen infrastruktuuri

Tietoyhteiskuntakaaressa määritelty teleyritys tarkoittaa sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa. Teleyritysten määritelmä on laaja ja se kattaa keskeisimmät digitaalisen infrastruktuurin toiminnot, mukaan lukien. internetin yhdysliikennepisteet ainakin niiltä osin, kun niitä käytetään yleisten viestintäverkkojen yhteenliittämiseen sekä nimipalvelun tarjoaminen silloin, kun se liittyy internetyhteyspalvelun tarjontaan.

Vaikka yleistä teletoimintaa voitaisiin pitää digitaalisen infrastruktuurin alueella yhteiskunnan toiminnan kannalta keskeisinä, on teleyritykset pääsääntöisesti suljettu verkko- ja tietoturvadirektiivin velvoitteiden soveltamisalan ulkopuolelle. Lisäksi teleyrityksiä koskevasta tietoturvariskienhallinnasta ja velvollisuudesta ilmoittaa häiriöistä säädetään jo nykyisin tietoyhteiskuntakaaressa.

Yleisen teletoiminnan lisäksi aluetunnusrekisterin ylläpitoa voidaan pitää digitaalisen infrastruktuurin kannalta keskeisenä. Suomessa keskeistä on aluetunnusrekisterin ylläpito fi-maatunnuksen ja ax-maakuntatunnuksen osalta. Aluetunnusrekisterin ylläpitoa voidaan pitää lähtökohtaisesti verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisena palveluna, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen ylläpitämiseksi.

2.3.4 Palveluntarjoajien toimintaan liittyvät tietoturvallisuusriskienhallinta- ja raportointivaatimukset

Energia

Sähkön osa-alueella verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaisiksi yhteiskunnan toiminnan kannalta keskeisiksi palveluiksi on edellä tunnistettu

1) siirtopalvelu kantaverkossa ja järjestelmävastaavan kantaverkonhaltijan tarjoamat järjestelmäpalvelut

2) sähkönjakelu jakeluverkossa, ei kuitenkaan sähkönjakelu suljetussa jakeluverkossa

3) sähkönjakelu suurjännitteisessä jakeluverkossa, ei kuitenkaan sähkönjakelu suljetussa jakeluverkossa

Verkko- ja tietoturvadirektiivin 5 artiklan mukaan direktiivin tarkoittaman keskeisen palvelun tarjoamisen on oltava myös riippuvaista verkko- ja tietojärjestelmistä. Lisäksi palveluun kohdistuvalla poikkeamalla tulisi olla merkittäviä haitallisia vaikutuksia palvelun tarjoamiseen. Sähkönjakelua voidaan pitää lähtökohtaisesti aina riippuvaisena verkko- ja tietojärjestelmistä, sillä sähköverkot toimivat nykyisin pitkälle automatisoituina järjestelminä, joiden toimintavarmuus on keskeistä energian saatavuuden turvaamiseksi. Sähkönjakeluun kohdistuvalla tietoturvallisuuteen liittyvällä häiriöllä voi olla merkittäviä haitallisia vaikutuksia sähkönjakelun lisäksi myös muiden yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjontaan. Vaikutukset voivat olla merkittäviä jakeluverkon koosta riippumatta. Tästä johtuen verkko- ja tietoturvadirektiivin mukaisina keskeisten palveluiden tarjoajina voitaisiin siis sähkön osa-alueella pitää järjestelmävastaavaa kantaverkonhaltijaa ja mahdollisia muita kantaverkonhaltijoita, kaikkia jakeluverkonhaltijoita niiden koosta riippumatta sekä suurjännitteisen jakeluverkon haltijoita pois lukien kuitenkin suljetut jakeluverkot.

Maakaasun osalta verkko- ja tietoturvadirektiivin tarkoittamana yhteiskunnan kannalta keskeisenä palveluna on edellä katsottu pidettävän maakaasumarkkinalain mukaistaen siirtopalvelua siirtoverkossa ja järjestelmävastaavan siirtoverkonhaltijan tarjoamia järjestelmäpalveluita. Nämä palvelut ovat lähtökohtaisesti aina riippuvaisia verkko- ja tietojärjestelmistä, sillä maakaasuverkot toimivat nykyisin pitkälle automatisoituina järjestelminä, joiden toimintavarmuus on keskeistä energian saatavuuden turvaamiseksi. Lisäksi palveluun kohdistuvalla tietoturvallisuuteen liittyvällä merkittävällä häiriöllä voisi olla merkittäviä haitallisia vaikutuksia maakaasun siirtopalvelun jatkuvuuteen. Verkko- ja tietoturvadirektiivin tarkoittamana keskeisten palveluiden tarjoajana voitaisiin siis pitää järjestelmävastaavaa siirtoverkonhaltijaa ja mahdollisia muita siirtoverkonhaltijoita.

Vaikka sähkömarkkinalakiin ja maakaasumarkkinalakiin sisältyy joitakin riskienhallintavelvoitteita, ei edellä määriteltyjä keskeisten palveluiden tarjoajia koskevia velvoitteita viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallitsemiseksi ole säädetty. Häiriöistä ilmoittamisesta ei myöskään ole laeissa säädetty, muutoin kuin sähkömarkkinalain 59 §:ssä tarkoitetuissa tapauksissa käyttäjille. Tämän vuoksi sähkömarkkinalakiin ja maakaasumarkkinalakiin olisi otettava säännökset velvoittamaan keskeisten palveluiden tarjoajia huolehtimaan viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittamaan merkittävistä järjestelmien tietoturvallisuuteen liittyvistä häiriöistä Energiavirastolle.

Liikenne

Liikenteen alueella verkko- ja tietoturvadirektiivin 5(2) artiklan a kohdan mukaisena yhteiskunnan toiminnan kannalta keskeisinä palveluksina on edellä tunnistettu

1) lennonvarmistuspalvelu,

2) rautatieliikenteen ohjauspalvelu,

3) alusliikennepalvelu,

4) lentoaseman hallinta,

5) valtion rataverkon hallinta,

6) sataman hallinta sekä

7) ITS-direktiivin tarkoittaman ITS-järjestelmän ylläpito

Lennonvarmistuspalvelua, rautatieliikenteen ohjauspalvelua, alusliikennepalvelua, valtion rataverkonhallintaa sekä ITS-direktiivin tarkoittamien ITS-järjestelmien ylläpitoa voidaan lähtökohtaisesti aina pitää verkko- ja tietojärjestelmistä riippuvaisena. Myös näihin palveluihin kohdistuvalla tietoturvallisuuteen liittyvällä merkittävällä häiriöllä voisi olla merkittäviä haitallisia vaikutuksia liikennejärjestelmän turvallisuuteen ja jatkuvuuteen. Näin kaikkia näiden palveluiden tarjoajia olisi pidettävä verkko- ja tietoturvadirektiivin tarkoittamina keskeisten palveluiden tarjoajina.

Lentoaseman ja sataman hallinta eroavat joiltakin osin edellä kuvatuista palveluista. Lentoasemien ja satamien koko vaihtelee. Näin vaihtelee myös niiden riippuvuus verkko- ja tietojärjestelmistä samoin kuin se, kuinka merkittävä vaikutus tietoturvallisuuteen liittyvällä häiriöllä voisi olla yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjontaan. Esimerkiksi kymmenen suurinta satamaa käsittelee noin 80 prosenttia merikuljetusten kokonaisvolyymista. Näihin satamiin kohdistuvilla häiriöillä voisi olla huomattavasti merkittävämpi vaikutus, kuin pienempiin satamiin kohdistuvilla häiriöillä. Tämän johdosta kaikkia satamanpitäjiä tai lentoasemanpitäjiä ei tulisi pitää verkko- ja tietoturvadirektiivin tarkoittamina keskeisten palveluiden tarjoajina. Velvoitteiden kohdistamista tulisi arvioida etenkin verkko- ja tietoturvadirektiivin 6 artiklan kriteerien valossa. Velvoitteiden kohdistaminen verkko- ja tietoturvadirektiivin tarkoittamiin keskeisten palveluiden tarjoajiin voitaisiin tehdä tarkemmin valtioneuvoston asetuksella.

Liikenteen alueella verkko- ja tietoturvadirektiivin mukaisina keskeisten palveluiden tarjoajina voitaisiin pitää siis

- lennonvarmistuspalvelujen tarjoajaa,

- rautatieliikenteenohjauspalveluja tarjoavaa yhtiötä ja valtion rataverkonhaltijaa,

- alusliikennepalvelun tarjoajaa,

- Liikennekaaren III-osan 2 luvun 6 §:n mukaisten ITS-järjestelmien ylläpitäjiä,

- yhteiskunnan toiminnan kannalta keskeisen sataman pitäjää (määriteltäisiin valtioneuvoston asetuksella),

- yhteiskunnan toiminnan kannalta keskeisen lentoaseman pitäjää (määriteltäisiin valtioneuvoston asetuksella).

Vaikka liikenteen keskeisten palveluiden tarjoajien riskienhallintaan liittyvään lainsäädäntöön voisi sinänsä katsoa sisältyvän myös viestintäverkkojen ja tietojärjestelmien turvallisuutta sivuavia velvoitteita, ei varsinaisia velvoitteita huolehtia viestintäverkkojen ja tietojärjestelmien turvallisuuteen liittyvästä riskienhallinnasta sisälly voimassa olevaan liikennemuotokohtaiseen lainsäädäntöön. Tietoturvallisuuden vaarantuessa myös liikenteen turvallisuus tai keskeisten

palvelujen jatkuvuus voisi vaarantua. Tämän vuoksi tulisi velvoitteet viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä merkittävistä järjestelmien tietoturvallisuuteen liittyvistä häiriöistä ilmoittamisesta Liikenteen turvallisuusvirastolle ottaa

- lennonvarmistuspalvelujen tarjoajaa ja lentoaseman pitäjää koskien ilmailulakiin,

- rautatieliikenteenohjauspalveluja tarjoavaa yhtiötä ja valtion rataverkonhaltijaa koskien rautatielakiin,

- alusliikennepalvelun tarjoajaa koskien alusliikennepalvelulakiin,

- satamanpitäjää koskien eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lakiin,

- Liikennekaaren III-osan 2 luvun 6 §:n ITS-järjestelmien ylläpitäjiä koskien liikennekaareen.

Pankkiala ja finanssimarkkinoiden infrastruktuurit

Kuten edellä on todettu, verkko- ja tietoturvadirektiivin 5(2) artiklan a kohdan mukaisia yhteiskunnan toiminnan kannalta keskeisiä palveluita pankkialalla ja finanssimarkkinoiden infrastruktuuria koskien olisivat luottolaitoslain mukainen luottolaitostoiminta sekä kaupankäynnistä rahoitusvälineillä annetun lain mukaisen pörssitoiminnan harjoittaminen.

Luottolaitostoimintaa koskevista operatiiviseen riskienhallintaan liittyvistä velvoitteista, joita täydentää Finanssivalvonnan antama määräys operatiivisten riskien hallinnasta, säädetään kattavasti luottolaitoslaissa. Velvoitteiden voi katsoa sekä riskienhallinta- sekä häiriöraportointivelvoitteiden osalta suoraan täyttävän verkko- ja tietoturvadirektiivin 14 artiklan mukaiset keskeisten palvelujen tarjoajien verkko- ja tietojärjestelmien turvallisuutta koskevat vaatimukset. Nämä vaatimukset koskevat kaikkia Suomessa toimivia luottolaitoksia.

Pörssitoimintaa voidaan pitää verkko- ja tietoturvadirektiivissä tarkoitetulla tavalla riippuvaisena verkko- ja tietojärjestelmistä. Lisäksi toimintaan kohdistuvalla tietoturvallisuuteen liittyvällä häiriöllä voisi olla merkittäviä haitallisia vaikutuksia pörssitoiminnan harjoittamiseen. Näin pörssiä tulisi pitää finanssimarkkinoiden infrastruktuuria koskien verkko- ja tietoturvadirektiivin 5 artiklan tarkoittamana keskeisten palvelujen tarjoajana.

Pörssitoiminnan harjoittamisen kannalta riskienhallintavaatimuksia ja häiriöiden ilmoittamista säännökset sisältyvät eduskunnalle 26.10 annettuun hallituksen esitykseen laeiksi sijoituspalvelulain muuttamisesta ja kaupankäynnistä rahoitusvälineillä sekä eräiksi niihin liittyviksi laeiksi (HE 151/2017 vp) 3 lukuun (1 ja 2.2 §). Velvoitteet täyttävät verkko- ja tietoturvadirektiivin 14 artiklan mukaiset keskeisten palvelujen tarjoajien verkko- ja tietojärjestelmien turvallisuutta koskevat vaatimukset.

Terveydenhuoltoala

Verkko- ja tietoturvadirektiivin 5(2) artiklan a kohdan mukaisena yhteiskunnan toiminnan kannalta keskeisenä palveluna terveydenhuoltoalalla olisivat terveydenhuollon asiakastietojen sähköinen käsittely sekä terveyden huollon laitteiden ylläpitäminen ja käyttäminen julkisten ja yksityisten sosiaalihuollon ja terveydenhuollon palvelujen tarjonnassa.

Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettuun lakiin sekä terveydenhuollon laitteista ja tarvikkeista annettuun lakiin sisältyvät velvoitteet asiakastietojen käsittelyyn tarkoitettujen järjestelmien tietoturvallisuudesta sekä vaatimukset koskien terveydenhuollon laitteita sekä velvoitteet häiriöiden ilmoittamisesta valvovalle viranomaiselle. Velvoitteiden voi katsoa sekä riskienhallinta- sekä häiriöraportointivelvoitteiden osalta täyttävän verkko- ja tietoturvadirektiivin 14 artiklan mukaiset keskeisten palvelujen tarjoajien verkko- ja tietojärjestelmien turvallisuutta koskevat vaatimukset.

Juomaveden toimittaminen ja jakelu

Verkko- ja tietoturvadirektiivin 5(2) artiklan a kohdan mukaisena yhteiskunnan toiminnan kannalta keskeisenä palveluna juomaveden toimittamista ja jakelua koskien voitaisiin pitää vesihuoltoa. Vesihuoltolaitokset huolehtivat vesihuoltolain mukaan yhdyskunnan vesihuollosta. Kaikkia vesihuoltolaitoksia voidaan pitää verkko- ja tietoturvadirektiivin 5(2) artiklan b kohdan mukaisesti riippuvaisina verkko- ja tietojärjestelmistä. Sen sijaan kaikkiin vesihuoltolaitoksiin kohdistuvilla poikkeamilla ei voisi olla 5(2) artiklan c kohdassa tarkoitettua merkittävää haitallista vaikutusta. Verkko- ja tietoturvadirektiivin 6 artiklan kriteereihin perustuen verkko- ja tietoturvadirektiivin mukaisina keskeisten palveluiden tarjoajina voitaisiin pitää vesihuoltolaitoksia, jotka toimittavat vettä vähintään 5000 kuutiometriä vuorokaudessa sekä vesihuoltolaitosta, joka toimittaa näille vettä. Tällaiseen palveluun kohdistuvilla tietoturvallisuuteen liittyvillä häiriöillä olisi aina verkko- ja tietoturvadirektiivin tarkoittama merkittävä vaikutus vesihuoltopalveluiden tarjontaan. Vettä vähintään 5000 kuutiometriä vuorokaudessa toimittavia vesihuoltolaitoksia on Suomessa arviolta noin 40 kappaletta ja näiden laitosten asiakkaat kattavat yli puolet Suomen väestöstä. Nämä vesihuoltolaitokset on lisäksi luokiteltu huoltovarmuuden kannalta kriittisiksi vesihuoltolaitoksiksi.

Juomaveden toimittamiseen ja jakeluun liittyvät vesihuoltolaitoksia koskevat turvallisuusriskien hallintavelvoitteet sisältyvät vesihuoltolakiin. Vesihuoltolain 15 a §:ään sisältyvä varautumisvelvoite sisältää velvoitteen varautua myös tietojärjestelmiin liittyviin riskeihin. Velvoitteiden voi katsoa riskienhallintavelvoitteiden osalta suoraan täyttävän verkko- ja tietoturvadirektiivin 14 artiklan mukaiset keskeisten palvelujen tarjoajien verkko- ja tietojärjestelmien turvallisuutta koskevat vaatimukset. Sen sijaan vesihuoltolakiin ei sisälly velvoitetta ilmoittaa järjestelmien tietoturvallisuuteen liittyvistä häiriöistä valvovalle viranomaiselle, joten lakiin olisi otettava tästä erillinen velvoite koskien vesihuoltolaitoksia, jotka toimittavat vettä vähintään 5000 kuutiometriä vuorokaudessa sekä vesihuoltolaitosta, joka toimittaa näille vettä.

Digitaalinen infrastruktuuri

Digitaalisen infrastruktuurin osalta verkko- ja tietoturvadirektiivin 5(2) artiklan a kohdan mukaisena mukaisena yhteiskunnan toiminnan kannalta keskeisenä palveluina olisi pidettävä aluetunnusrekisterin ylläpitämistä. Tietoyhteiskuntakaareen sisältyy velvoiteet aluetunnusrekisterin ylläpitäjälle huolehtia tietoturvasta. Viestintävirasto on lain mukaan fi-aluetunnusrekisteriä ylläpitävä viranomainen. Ahvenanmaan maakuntahallinto ylläpitää ax-aluetunnusrekisteriä. Tietoyhteiskuntakaaren velvoitteiden voi katsoa täyttävän verkko- ja tietoturvadirektiivin 14 artiklan mukaiset keskeisten palvelujen tarjoajien verkko- ja tietojärjestelmien turvallisuutta koskevat vaatimukset.

Digitaalisten palvelujen tarjoajat

Verkko- ja tietoturvadirektiivin mukaisten digitaalisten palveluiden tarjoajien (pilvipalvelu, hakukone, verkossa toimiva markkinapaikka) tietoturvariskienhallintaa tai tietoturvallisuuteen liittyvien häiriöiden ilmoittamista ei ole säännelty voimassa olevassa lainsäädännössä. Tämän vuoksi tulisi velvoitteet viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä merkittävistä järjestelmien tietoturvallisuuteen liittyvistä häiriöistä ilmoittamisesta Viestintävirastolle ottaa tietoyhteiskuntakaareen. Verkko- ja tietoturvadirektiivissä ei ole jätetty jäsenvaltioille vastaavaa palvelun keskeisyyttä koskevaa määritystehtävää koskien digitaalisten palveluiden tarjontaa vaan direktiivin velvoitteet koskevat kaikkia direktiivin soveltamisalaan kuuluvia palveluntarjoajia. Velvoitteiden soveltamisalasta tulisi kuitenkin sulkea verkko- ja tietoturvadirektiivin mukaisesti pienet ja mikroyritykset.

2.3.5 Riskienhallinta- ja raportointivelvoitteiden valvonta

Voimassa olevaan lainsäädäntöön sisältyy edellä kuvatulla tavalla turvallisuusriskienhallintaan sekä poikkeamien tai häiriöiden ilmoittamiseen liittyviä velvoitteita, joiden valvonnasta vastaa laissa säädetty toimivaltainen viranomainen. Valvontaviranomaisille on tyypillisesti säädetty myös valtuuksia valvontatehtävien hoitamiseen, kuten tiedonsaanti- ja tarkastusoikeuksia. Valvontaviranomaiset voivat myös antaa valvottavia sitovia päätöksiä. Näiden seikkojen johdosta olisi luontevaa, että viestintäverkkojen ja tietojärjestelmien turvallisuutta valvoisi sama viranomainen kuin muitakin palvelun tarjontaan liittyviä turvallisuusvelvoitteita. Myös verkko- ja tietoturvadirektiivin täytäntöönpanoa tukeva työryhmä on arviointinsa perusteella esittänyt, että direktiivin mukaisina toimivaltaisina viranomaisina toimisivat niin kutsutut sektorikohtaisen valvontaviranomaiset.

Sähkönjakelua koskevat verkko- ja tietoturvallisuutta koskevat vaatimukset ehdotettaisiin otettavan sähkömarkkinalakiin ja maakaasun jakelua koskevat vaatimukset maakaasunmarkkinalakiin. Sähkö- ja maakaasumarkkinalakeja valvoo sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain mukaan Energiavirasto ja se olisi näin luonteva taho myös tietoturvallisuutta koskevien velvoitteiden valvomiseksi.

Liikenteen osalta eri liikennemuotoja koskevat turvallisuuteen liittyvät valvontatehtävät on keskitetty pääasiallisesti Liikenteen turvallisuusvirastolle. Eräiden liikenteen palvelujen tarjoajien on lisäksi jo nykyään ilmoitettava Liikenteen turvallisuusvirastolle tietyistä liikenteen turvallisuutta vaarantavista poikkeamista tai häiriöistä. Liikenteen keskeisten palvelujen tietoturvallisuutta koskevat velvoitteet otettaisiin liikennemuotokohtaisiin erityislakeihin, joten toimivalta näiden velvoitteiden valvomiseksi olisi perusteltua säätää Liikenteen turvallisuusvirastolle.

Pankkialan osalta Finanssivalvonta valvoo voimassa olevan lainsäädännön nojalla operatiiviseen riskienhallintaan sisältyviä järjestelmien tietoturvallisuusvelvoitteita. Luottolaitosten on myös ilmoitettava tietoturvallisuuteen liittyvistä häiriöistä Finanssivalvonnalle.

Terveydenhuollon asiakastietojen sähköisestä käsittelyä sekä terveydenhuollon laiteiden laatuvaatimuksia valvoo Sosiaali- ja terveysalan lupa- ja valvontavirasto. Palvelun tarjoajien on myös ilmoitettava tietyistä tietoturvallisuuteen liittyvistä häiriöistä virastolle.

Juomaveden toimittamiseen ja jakeluun liittyvät vesihuoltolaitoksia koskevat turvallisuusriskienhallintavelvoitteet sisältyvät vesihuoltolakiin. Vesihuoltolain mukaisia valvovia viranomaisia ovat toimialoillaan elinkeino-, liikenne- ja ympäristökeskus sekä kunnan ympäristön-

suojeluviranomainen ja kunnan terveydensuojeluviranomainen.. Juomaveden toimittamisen ja jakelun toimialalla ei ole vastaavaa keskitettyä sektorikohtaista valvontaviranomaista kuin muilla direktiivin täytäntöönpanoon kuuluvilla toimialoilla. Juomaveden jakelun jatkuvuuden varmistamiseksi sekä viranomaisten valvontatehtävien tehokkaaksi suorittamiseksi olisi säädettävä tietoturvaan liittyvien häiriöiden ilmoittamisesta elinkeino-, liikenne- ja ympäristökeskukselle.

Edellä mainittujen valvovien viranomaisten toimivalta eri toimialoilla on riippuvaista niiden lakien, joissa toimivaltuuksista on säädetty, sisällöstä ja vaihtelee. Viranomaisella on toimivalta valvoa tietoturvallisuuteen liittyvien velvoitteiden noudattamista ja velvoittaa korjaamaan lain vastainen toiminta vain, mikäli toimivallasta on säädetty. Toimivallasta voidaan säätää yleisesti (esimerkiksi Energiavirasto valvoo sähkömarkkinalain mukaisien velvoitteiden noudattamista) tai erityisesti (tietyssä pykälässä säädettyjä velvoitteita valvoo tietty viranomainen). Myös viranomaisen oikeudesta tehostaa antamaansa päätöstä hallinnollisin seuraamuksin, kuten uhkasakoin, on säädettävä erikseen.

Riittävän toimivallan varmistamiseksi valvontaviranomaisten lakisääteiset tehtävät, viranomaisten tiedonsaantioikeuksia, tietojen käsittelyn edellytyksiä sekä hallinnollisia seuraamuksia koskeva sääntely kaipaavat tiettyjä tarkennuksia.

3 Esityksen tavoitteet ja keskeiset ehdotukset

3.1 Tavoitteet

Digitalisaatio on teollinen ja yhteiskunnallinen murros sekä globaali, kiihtyvällä vauhdilla etenevä megatrendi. Se mullistaa toimintatapoja kaikilla elämän osa-alueilla. Digitaalisten toimintatapojen käyttöönottoa voi kuitenkin jarruttaa se, ettei niitä kohtaan tunneta luottamusta. Näin digitalisaatiokehityksen tuomista hyödyistä ei pystytä täysimääräisesti hyötymään. Ehdotuksen tavoitteena onkin lisätä kansalaisten ja yritysten luottamusta digitaalisiin toimintatapoihin ja parantaa yhteiskunnan toiminnan sekä kansalaisten kannalta keskeisten palveluiden tietoturvallisuutta. Tämä on tärkeää tällaisten palveluiden ollessa yhä suuremmissa määrin riippuvaisia viestintäverkkojen ja tietojärjestelmien käytöstä.

Esityksessä ehdotettaisiin tietyille yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajille velvollisuutta huolehtia viestintäverkkoihin ja tietojärjestelmiin liittyvästä riskienhallinnasta. Tavoitteena olisi varmistua, että palvelun tarjoajat ottaisivat tietoturvallisuuteen liittyvän riskienhallinnan osaksi normaalia toimintansa turvallisuusriskienhallintaa.

Tietoturvallisuuteen liittyvät häiriöt voivat vaarantaa palvelun turvallisuuden taikka jatkuvuuden. Yhteiskunnan toiminnan kannalta keskeisille palveluille on jo voimassa olevassa lainsäädännössä säädetty velvoitteita, joilla palveluiden turvallinen tarjoaminen käyttäjille voidaan varmistaa. Toimivaltaiset viranomaiset valvovat näiden velvoitteiden noudattamista. Ehdotuksen tavoitteena on lisätä toimivaltaisen valvontaviranomaisen tietoa viestintäverkkoihin ja tietojärjestelmiin liittyvistä häiriöistä, jotka voivat vaarantaa palvelun laissa edelletyn laadun, turvallisuuden tason tai esimerkiksi häiriöttömyyden. Lisäksi ehdotuksen tavoitteena on mahdollistaa toimivaltaisten viranomaisten kyky käsitellä ja arvioida tällaisten tietoturvallisuuteen liittyvien häiriöiden merkitystä, jotta tarvittaviin korjaaviin toimenpiteisiin voitaisiin ryhtyä.

3.2 Toteuttamisvaihtoehdot

Valmistelun aikana on eri toteuttamisvaihtoehtoja arvioitu heijastamalla niitä hallitusohjelman sekä hallitusohjelman toimeenpano-ohjelman mukaisesti hyväksytyn tietoturvastrategian tavoitteisiin. Eri toteuttamisvaihtoehtoja arvioitiin verkko- ja tietoturvadirektiivin täytäntöönpanon tukemiseksi perustetussa työryhmässä.

Direktiivin täytäntöönpanon yhteydessä on arvioitu mahdollisuutta säätää kokonaan uusi verkko- ja tietoturvallisuutta koskeva erityislaki. Tätä vaihtoehtoa arvioitiin myös ministeriön asettamassa työryhmässä. Työryhmän työn tueksi selvitettiin millaisia tietoturvavelvoitteita tai muita riskienhallintaan sekä turvallisuuteen liittyviä velvoitteita verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvilla toimialoilla on tällä hetkellä voimassaolevan kansallisen lainsäädännön, EU-lainsäädännön sekä kansainvälisten velvoitteiden puitteissa. Selvityksen keskeisiä johtopäätöksiä olivat, että kotimainen tietoturvasääntely on fragmentoitunutta. Direktiivin soveltamisalaan kuuluville toimialoille on asetettu melko paljon turvallisuus- ja riskienhallintavelvoitteita, mutta myös näitä koskeva sääntely on hyvin hajanaista. Suurimmalla osalla soveltamisalaan kuuluvista toimialoista on säädetty joitakin riskienhallintaa tai tietoturvan tasoa koskevia velvoitteita. Turvallisuusvelvoitteet ovat kuitenkin useimmissa tapauksissa yksittäisiin toimintoihin liittyviä, eivät suoraan koko toimialaa tai toimijatyyppiä velvoittavia. Riskienhallintavelvoitteet on osin muotoiltu hyvin avoimiksi siten, ettei suoraan säännöksen sanamuodosta voida tulkita, voidaanko tietyn velvoitteen katsoa kattavan myös tietojärjestelmien turvaamisen. Ilmoitusvelvollisuuksia on asetettu lähes kaikilla toimialoilla, mutta tietoturvallisuuteen liittyvästä häiriöistä ilmoittamista koskevia velvoitteita on vain joillakin toimialoilla. Sektorikohtaiselle lainsäädännölle tehdyn selvityksen ja työryhmän arvion perusteella sekä kansalliselle täytäntöönpanolle asetetut tavoitteet huomioiden työryhmä on katsonut, että verkko- ja tietoturvadirektiivin mukaiset velvoitteet tulisi lähtökohtaisesti pyrkiä ottamaan kansallisesti osaksi sektorikohtaista lainsäädäntöä. Työryhmän näkemyksen mukaan direktiivin implementointi omaksi erityislaikseen ei täyttäisi samalla tavalla direktiivin täytäntöönpanolle asetettuja tavoitteita ja voisi sen sijaan johtaa päällekkäisiin velvoitteisiin ja raportointikäytäntöihin.

Edellä esitetyn lisäksi tietoturvallisuutta koskevan riskienhallinnan ei voida katsoa sillä tavoin eroavan muusta toimijan riskienhallinnasta, että siitä olisi ollut aiheellista säätää eri laissa. Useaa verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvaa toimialaa koskeva lainsäädäntö on koottu yhteen lakiin. Esimerkiksi sähkönjakelua koskevista velvoitteista säädetään pääasiallisesti sähkömarkkinalaissa ja vesihuollon järjestämisestä vesihuoltolaissa. Mikäli tietoturvaa koskevat velvoitteet olisi otettu erilliseen lakiin, olisi se ollut omiaan kasvattamaan riskiä päällekkäisen sääntelyn syntymisestä ja antamaan mielikuvaa tietoturvariskienhallinnasta erillisenä kokonaisuutena. Soveltamisalaan kuuluvan palveluntarjoajan näkökulmasta olisi selkeämpää, ettei turvallisuusriskien hallintaan liittyvien velvoitteiden valvontaa ja häiriöiden raportointia ole hajautettu useisiin lakeihin, joihin voisi syntyä päällekkäistä sääntelyä.

Toisena vaihtoehtona tarkasteltiin verkko- ja tietoturvallisuutta koskevien sääntöjen ottamista osaksi tietoyhteiskuntakaarta. Vaihtoehtoa ei kuitenkaan pidetty hyvänä, sillä direktiivin soveltamisalaan kuuluvien keskeisten palveluiden tarjoajien, kuten esimerkiksi sähkönjakeluverkon haltijan, voisi olla vaikea ymmärtää, että häntä koskevia velvoitteita sisältyisi tietoyhteiskuntakaareen. Sääntelyratkaisu olisi ollut myös poikkeava esimerkiksi finanssisektorilla jo omaksutusta ratkaisusta, jossa tietoturvallisuutta koskevat velvoitteet on sisällytetty toimialaa koskevaan erityissääntelyyn osana operatiivisten riskien hallintaa.

Edellä kuvatuin perustein pidettiin direktiivin täytäntöönpanon kannalta parhaana vaihtoehtona sisällyttää tietoturvallisuutta koskevat velvoitteet toimialakohtaiseen erityislainsäädäntöön.

Viestintäviraston erityisiin tehtäviin sisältyy yleisiä tietoturvallisuuden edistämiseen liittyviä tehtäviä. Lakiehdotuksen valmistelussa on arvioitu myös sitä, olisiko Viestintävirasto voinut toimia direktiivin tarkoittamana toimivaltaisena viranomaisilla kaikilla direktiivin soveltamisalan mukaisilla toimialueilla. Kuten edellä on kuitenkin selostettu, verkko- ja tietoturvadirektiivin soveltamisalalla on Suomessa jo useita valvontaviranomaisia, keskeisimpinä Energiavirasto, Finanssivalvonta, Liikenteen turvallisuusvirasto, Sosiaali- ja terveysalan lupa- ja valvontavirasto, elinkeino-, liikenne- ja ympäristökeskukset sekä Viestintävirasto. Tietoturvariskienhallinta velvoitteiden valvomiseksi ei Suomessa ole nimetty vain yhtä viranomaista, kuten Viestintävirastoa. Sen sijaan valvontaviranomaisilla on tyypillisesti toimivalta valvoa lainsäädännössä sille määritettyjä kokonaisuuksia. Esimerkiksi Finanssivalvonta valvoo sen valvottavien osalta operatiivisen riskinhallinnan velvoitteiden noudattamista. Näihin sisältyy myös tietojärjestelmille asetetut turvallisuusvaatimukset. Valvottavat tekevät myös mahdolliset tietoturvallisuuteen liittyvät häiriöilmoitukset Finanssivalvonnalle. Valvontaviranomaisille on tyypillisesti säädetty myös valtuuksia valvontatehtävien hoitamiseen, kuten tiedonsaanti- ja tarkastusoikeuksia. Valvontaviranomaiset voivat myös antaa valvottavia sitovia päätöksiä. Mikäli tietoturvariskienhallintaan liittyvät viranomaistehtävät keskitettäisiin jatkossa vain yhdelle viranomaiselle, se voisi aiheuttaa päällekkäisiä valvontatoimivaltuuksia sekä raportointivelvollisuuksia palvelun tarjoajille. Lisäksi palvelujen digitalisoituessa läpi yhteiskunnan jokaisen toimialan viranomaisen on kyettävä aiempaa paremmin ymmärtämään tietoturvallisuuden merkitys valvomassaan toiminnassa. Muutoin tietoturvasta voi tulla itseisarvo, eikä palveluiden turvallisuuden ja jatkuvuuden kannalta mitoitettu osa palveluiden tarjontaa ja valvontaa. Ongelmalliseksi voisi myös muodostua se, ettei aina ole selvää johtuuko palveluun kohdistuva häiriö esimerkiksi tietojärjestelmien turvallisuuteen vai onko kyseessä muuhun turvallisuuteen liittyvä häiriö. Häiriöillä saattaa todennäköisesti olla myös läheisiä liittymiä tietoturvallisuuden lisäksi esimerkiksi liikenteen osalta liikenteen turvallisuuteen. Tämän vuoksi toimivaltaisen viranomaisen tehtävät olisi tarkoituksen mukaista antaa niille viranomaisille, jotka jo voimassa olevan lainsäädännön perusteella valvovat toimialansa turvallisuusriskienhallintavelvoitteita.

Verkko- ja tietoturvadirektiivin mukaisen kansallisen yhteyspisteen osalta valmistelussa on arvioitu tehtävien säätämistä yhtäältä valtioneuvoston tilannekeskukselle ja toisaalta Viestintävirastolle. Valtioneuvoston ohjesäännön 12 §:n 7 kohdan mukaan valtioneuvoston kanslian toimialaan kuuluu valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus sekä häiriötilanteiden hallinnan yleinen yhteensovittaminen. Tämän johdosta keskitettynä yhteyspisteenä voisi toimia myös valtioneuvoston tilannekuvakeskus. Verkko- ja tietoturvadirektiivin täytäntöönpanoa tukevan työryhmän arvion mukaan keskitetyn yhteyspisteen tehtävien luonne on kuitenkin sillä tavoin operatiivinen ja sen toiminnalla on niin läheinen yhteys direktiivin mukaisen CSIRT-toimijan tehtäviin, että olisi luontevampaa, että Viestintävirasto toimisi direktiivin mukaisena keskitettynä yhteyspisteenä.

3.3 Keskeiset ehdotukset

Ilmailulakiin, rautatielakiin, alusliikennepalvelulakiin, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin, liikenteen palveluista annettuun lakiin, sähkömarkkinalakiin, maakaasumarkkinalakiin sekä vesihuoltolakiin lisättäisiin säännökset yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajien velvolli-

suudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä velvollisuudesta ilmoittaa tietoturvallisuuteen liittyvistä merkittävistä poikkeamista valvovalle viranomaiselle sekä tietyissä tapauksissa yleisölle. Laeissa ei määriteltäisi tarkemmin miten riskienhallinnasta olisi huolehdittava, vaan tältä osin toimijalla olisi mahdollisuus valita liiketoimintaansa, järjestelmiinsä ja muuhun riskienhallintaansa parhaiten sopivat menetelmät tietoturvariskien hallitsemiseksi.

Ilmailulain velvoitteet koskisivat lennonvarmistuspalvelun tarjoajaa sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjää. Rautatielain velvoitteet koskisivat valtion rataverkon haltijaa sekä liikenteenohjauspalveluita tarjoavaa yhtiötä. Alusliikennepalvelulain velvoitteet koskisivat alusliikennepalvelun tarjoajaa. Eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain velvoitteet koskisivat yhteiskunnan toiminnan kannalta merkittävän sataman pitäjää. Liikenteen palveluista annetun lain mukaiset velvoitteet koskisivat älykkään liikennejärjestelmän ylläpitäjää. Sähkömarkkinalain velvoitteet koskisivat verkonhaltijaa. Maakaasumarkkinalain velvoitteet koskisivat siirtoverkonhaltijaa ja vesihuoltolain velvoitteet vesihuoltolaitosta, joka toimittaa vettä tai ottaa vastaan jätevettä vähintään 5000 kuutiometriä vuorokaudessa. Vesihuoltolain sääntelyä täydennettäisiin samalla siten, että mainittujen laitosten olisi ilmoitettava viranomaiselle myös muista kuin tietoturvallisuuteen liittyvistä merkittävistä vesihuollon häiriötilanteista.

Tietoyhteiskuntakaareen otettaisiin vastaavat velvoitteet koskien eräitä digitaalisten palveluiden tarjoajia. Tietoyhteiskuntakaaren velvoitteet koskisivat verkossa toimivan markkinapaikan tarjoajaa, hakukonepalvelun tarjoajaa sekä pilvipalvelun tarjoajaa.

Lisäksi säädettäisiin valvovien viranomaisten oikeudesta tehdä tietoturvallisuuteen liittyvien velvoitteiden valvonnassa tarvittavaa yhteistyötä ja vaihtaa tarvittaessa salassa pidettäviä tietoja. Valvoville viranomaisille säädettäisiin myös velvoite ilmoittaa tarvittaessa tietoturvallisuuteen liittyvistä häiriöistä toisille EU:n jäsenvaltioille, mikäli häiriöllä on merkittävä vaikutus keskeisten palvelujen tarjoamiseen kyseisessä jäsenvaltiossa. Viestintävirastolle säädettäisiin velvollisuus tehdä tarvittaessa yhteistyötä muiden jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten, tietoturvaloukkauksiin reagoivien yksiköiden sekä EU:n verkko- ja tietoturvadirektiivin 10 artiklan mukaisen yhteistyöryhmän kanssa.

4 Esityksen vaikutukset

4.1 Taloudelliset vaikutukset

Esityksellä ei ole merkittäviä taloudellisia vaikutuksia verkko- ja tietoturvadirektiivissä ja tässä ehdotuksessa tarkoitetuille yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajille taikka digitaalisten palveluiden tarjoajille. Vaikka yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajille sekä digitaalisten palveluiden tarjoajille ehdotettavat tietoturvallisuuteen liittyvään riskienhallintaan sekä häiriöiden raportointiin liittyvät velvoitteet ovat uusia, sisältyy voimassa olevaan lainsäädäntöön jo ennestään samankaltaisia riskienhallintavelvoitteita. Lisäksi palvelun tarjoajalle on jätetty harkintavalta sen suhteen, millaisin konkreettisin toimenpitein se huolehtii riskien hallinnan toteuttamisesta. Tämä mahdollistaa uusien velvoitteiden mukaisten toimenpiteiden huomioimisen osana palvelun tarjoajan kokonaisvaltaista liiketoiminnan riskien hallintaa. Tietoturvallisuuteen liittyvien häiriöiden raportoinnista voi aiheuta palvelun tarjoajalle esimerkiksi tietojärjestelmiin liittyviä kustannuksia. Ottaen huomioon kuitenkin jo voimassa olevan lainsäädännön ilmoitusvelvollisuudet, ei nyt ehdotettavis-

ta uusista raportointivelvoitteista voida katsoa syntyvän merkittäviä taloudellisia vaikutuksia palvelun tarjoajille.

Tietoturvaloukkauksilla voi olla merkittäviä negatiivisia taloudellisia vaikutuksia. Suurimat vaikutukset seuraavat siitä, että yrityksen toiminta keskeytyy tai toiminnan kannalta tarpeellisia tietoja häviää. Ehdotettu velvollisuus huolehtia viestintäverkkojen ja tietojärjestelmien riskienhallinnasta parantaa palveluntarjoajien kykyä varautua tietoturvaloukkauksiin. Lisäksi velvoite ilmoittaa tietoturvaloukkauksista kasvattaa tietoturvaloukkauksiin liittyvää tietoa ja luo edellytyksiä esimerkiksi tietoturvallisuushaavoittuvuuksia koskevan tiedon tehokkaammalle jakamiselle toimijoiden yhteiseksi hyödyksi ja tietoturvallisuuden parantamiseksi.

4.2 Vaikutukset viranomaisen toimintaan

Esityksellä säädettäisiin tietoturvallisuuteen liittyviä valvontatehtäviä useille sektorikohtaisille valvontaviranomaisille. Digitaalisten palvelun tarjoajia koskevia velvoitteita valvoisi Viestintävirasto, liikennesektorin palveluiden tarjoajia koskevia velvoitteita Liikenteen turvallisuusvirasto, Finanssisektorin velvoitteita Finanssivalvonta, energiasektoria koskevia velvoitteita Energiavirasto sekä juomaveden toimittamista ja jakelua koskevia velvoitteita elinkeino-, liikenne- ja ympäristöministeriö. Viranomaisten tehtävänä olisi valvoa palvelun tarjoajien tietoturvallisuuteen liittyvää riskienhallintaa sekä vastaanottaa tietoturvahäiriöilmoituksia. Toimialakohtaiseen voimassaolevaan lainsäädäntöön sisältyy nykytilan kuvauksen yhteydessä esitetyllä tavalla nyt ehdotettuja riskienhallinta- ja raportointivelvoitteita muistuttavia velvoitteita, joiden valvonta on säädetty toimialakohtaisten valvontaviranomaisten tehtäväksi. Tästä syystä nyt ehdotettavista ehdotuksissa ei voida katsoa seuraavan merkittäviä resurssitarpeita tai kustannuksia valvoville viranomaisille vaan tehtävät pystyttäisiin hoitamaan lähtökohtaisesti nykyisten resurssien puitteissa.

Valvontatehtävien lisäksi ehdotuksella säädettäisiin Viestintävirastolle eräitä verkko- ja tietoturvadirektiivin mukaisia yleisiä tietoturvallisuuteen liittyviä tehtäviä, joita olisivat direktiivin mukaisena CSIRT-toimijana toimiminen direktiivin liitteen II ja III mukaisilla toimialoilla sekä direktiivin mukaisena keskitettynä yhteyspisteenä toimiminen. CSIRT-toimintoon liittyvät tehtävät vastaavat lähtökohtaisesti Viestintäviraston nykyisiä lakisääteisiä tehtäviä, eikä ehdotuksella laajennettaisi lakisääteisiä tehtäviä merkittävästi. Keskitetyn yhteyspisteen tehtävät olisivat uusia ja niihin kuuluisi yhteydenpito muiden EU:n jäsenvaltioiden kanssa sekä tiivistelmäraporttien toimittaminen direktiivin mukaiselle yhteistyöryhmälle. Tehtävistä aiheutuvat kustannukset eivät olisi merkittäviä, vaan tehtävät pystyttäisiin hoitamaan lähtökohtaisesti nykyisten resurssien puitteissa.

4.3 Yhteiskunnalliset vaikutukset

Esityksellä parannettaisiin yhteiskunnan toiminnan kannalta keskeisten palveluiden sekä eräiden digitaalisten palveluiden tietoturvallisuutta. Tietoturvallisuuden tason nouseminen olisi tärkeää yhteiskunnan toiminnan kannalta keskeisten palveluiden toiminnan jatkuvuuden varmistamiseksi, yhteiskunnan turvallisuuden parantamiseksi sekä erityisesti kansalaisten ja yritysten luottamuksen kasvattamiseksi digitaalisiin toimintatapoihin.

Esitetty velvollisuus huolehtia yhteiskunnan keskeisten palveluiden tietoturvariskienhallinnasta olisi omiaan parantamaan keskeisten palveluiden turvallisuutta ja kykyä varautua tietoturvallisuuteen liittyviin häiriöihin. Tällaisia häiriöitä ovat esimerkiksi tietomurrot, tietojenkalas-

telu ja muut tietoturvaloukkaukset, kuten laajamittaiset palvelunestohyökkäykset tai laajaalaisesti levitettävät kiristyshaittaohjelmat, jotka ovat vuosien 2016 ja 2017 aikana aiheuttaneet merkittäviä häiriöitä myös yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjontaan. Esimerkiksi toukokuussa 2017 Iso-Britanniassa kiristyshaittaohjelma levisi lukuisiin terveydenhuollon laitoksien (National Health Service) tietokoneisiin, minkä seurauksena tuhansia potilasaikoja ja operaatioita jouduttiin perumaan.

Esitetty ilmoitusvelvollisuus valvoville viranomaisille tietoturvallisuuteen liittyvistä häiriöistä parantaisi valvovien viranomaisten tietoturvallisuuden tilannekuvaa ja kasvattaisi tietoturvallisuuteen liittyvää osaamista eri toimialoilla. Viranomaisten tietoturvallisuuteen liittyvän osaamisen ja tilannekuvan parantuminen kasvattaisi koko yhteiskunnan tieturvallisuutta sekä sietokykyä tietoturvallisuuteen liittyviä häiriöitä kohtaan.

Ehdotetun lainsäädännön vaikutuksia yhteiskunnan toiminnan kannalta keskeisten palveluiden tietoturvallisuuteen arvioidaan liikenne- ja viestintäministeriön toimesta kahden vuoden kuluttua lainsäädännön voimaantulosta.

5 Asian valmistelu

5.1 Valmisteluvaiheet ja -aineisto

Liikenne- ja viestintäministeriö asetti verkko- ja tietoturvadirektiivin täytäntöönpanoa tukevan työryhmän lokakuussa 2016. Työryhmän tehtävänä oli tukea liikenne ja viestintäministeriötä direktiivin voimaansaattamisen valmistelussa, arvioida vaihtoehtoisia sääntelytapoja sekä edistää direktiivin edellyttämää yhteistyötä soveltamisalaan kuuluvien toimialojen välillä. Liikenne- ja viestintäministeriön lisäksi työryhmässä olivat edustettuina työ- ja elinkeinoministeriö, valtiovarainministeriö, sosiaali- ja terveysministeriö, Viestintävirasto, Liikenteen turvallisuusvirasto, Liikennevirasto, Huoltovarmuuskeskus, Finanssivalvonta, Energiavirasto, Sosiaali- ja terveysalan lupa- ja valvontavirasto, FiCom ry, Elinkeinoelämän keskusliitto EK, Teknologiateollisuus ry, Energiateollisuus ry sekä Finanssialan keskusliitto FK. Ympäristöministeriö ei nimennyt jäsentä työryhmään. Työryhmä kokoontui yhdeksän kertaa, joista viisi kertaa oli jaettu sektorikohtaisesti seuraavasti: liikennesektori, finanssisektori, terveydenhuoltosektori, energiasektori ja digisektori. Sektorikohtaisissa kokouksissa keskityttiin arvioimaan kunkin sektorin voimassa olevaa turvallisuusriskienhallinta lainsäädäntöä sekä verkko- ja tietoturvadirektiivin vaihtoehtoisia täytäntöönpanomalleja. Työryhmä ehdotti huhtikuussa 2016 julkaistussa loppuraportissaan (liikenne- ja viestintäministeriön julkaisuja 9/2017) yleisiä suuntaviivoja direktiivin täytäntöönpanolle.

Työryhmätapaamisten lisäksi valtiovarainministeriön, sosiaali- ja terveysministeriön, maa- ja metsätalousministeriön sekä työ- ja elinkeinoministeriön kanssa on käyty kahdenvälisiä keskusteluja. Ministeriöille on myös lähetetty toukokuussa 2017 toimenpidepyyntö koskien keskeisten palveluiden tarjoajien määrittelemistä ja viranomaisvalvonnan järjestämistä eri hallinnonaloilla.

Lisäksi liikenne- ja viestintäministeriössä järjestettiin sidosryhmille avoin kuulemistilaisuus koskien direktiivin täytäntöönpanoa joulukuussa 2016. Direktiivin valmistelua ja täytäntöönpanoa on myös käyty esittelemässä useissa sektorikohtaisissa tilaisuuksissa, valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmässä (VAHTI) sekä digitaalisen liiketoiminnan kasvu-

ympäristönrakentamiseen tähtäävän kärkihankkeen toimeenpanoa koordinoimaan elokuussa 2015 asetetussa työryhmässä.

EU-tason yhteistyötä valmistelun aikana muiden jäsenvaltioiden kanssa on tehty verkko- ja tietoturvadirektiivin mukaisen yhteistyöryhmän ja CSIRT-verkoston puitteissa.

5.2 Lausunnot ja niiden huomioon ottaminen

Ehdotus hallituksen esitykseksi on valmisteltu liikenne- ja viestintäministeriössä. Liikenne- ja viestintäministeriö on lähettänyt ehdotuksen lausunnoille lokakuussa 2017. Ehdotuksesta annettiin yhteensä 27 lausuntoa. Lausunnot saatiin oikeusministeriöltä, maa- ja metsätalousministeriöltä, sosiaali- ja terveysministeriöltä, työ- ja elinkeinoministeriötä, valtiovarainministeriöltä, sisäministeriöltä, Ahvenanmaan maakunnalta, Liikenteen turvallisuusvirastolta, Viestintävirastolta, Terveyden ja hyvinvoinnin laitokselta, Finanssivalvonnalta Sosiaali- ja terveysalan valvontavirastolta, Turvallisuuskomitean sihteeristöltä, Kuntaliitolta, Logistiikkayritysten liitolta, CSC-Tieteen tietotekniikan keskukselta, OP Ryhmältä, Suomen vesilaitosyhdistykseltä, Suomen Varustamoilta, Finanssiala ry:ltä, Finrail Oy:ltä, Tietoliikenteen ja tietotekniikan keskusliitolta, Elinkeinoelämän keskusliitolta, Suomen Satamaliitolta, Teknologiateollisuus ry:ltä, Tieto Oyj:ltä, Microsoft Oy:ltä sekä Nasdaq Helsinki Oy:ltä. Seitsemässä lausunnossa ei ollut varsinaista lausuttavaa.

Hallituksen esityksen ja verkko- ja tietoturvadirektiivin täytäntöönpanon yleisiin tavoitteisiin sekä valittuihin toteuttamisvaihtoehtoihin suhtauduttiin kaikissa lausunnoissa positiivisesti. Erityisen tyytyväisiä oltiin sektorikohtaiseen lähestymistapaan sekä siihen, että direktiivin kansallisessa täytäntöönpanossa on pyritty välttämään kansallista lisäsääntelyä. Lausunnoissa pidettiin myös hallituksen esityksessä määriteltyjä keskeisten palveluiden tarjoajia pääosin perustellusti rajattuina.

Lausunnoissa esitettiin joitakin yksittäisiä muutos- ja täydennysehdotuksia ehdotettuihin lakeihin sekä täydennyksiä perusteluihin. Ehdotukset koskivat erityisesti tietoyhteiskuntakaareen ehdotettua pilvipalvelun määritelmää, finanssialan keskeisten palveluiden tarjoajien määrittelemistä, viranomaisten oikeutta vaihtaa salassa pidettävää tietoa sekä juomaveden toimittamista ja jakelua koskevaa viranomaistoimintaa. Tarkempi lausuntopalaute on luettavissa liikenne- ja viestintäministeriön internetsivuilla julkaistussa lausuntoyhteenvedossa.

Lausuntopalautteen perusteella vesihuoltoa koskevaa ehdotettua sääntelyä on jatkovalmisteltu yhteistyössä maa- ja metsätalousministeriön, sosiaali- ja terveysministeriön, Sosiaali- ja terveysalan valvontaviraston sekä Vesilaitosyhdistyksen kanssa huomioiden lausunnoissa saadun palautteen. Myös ehdotuksia viranomaisten oikeudesta luovuttaa toisilleen salassa pidettävää tietoa on täydennetty. Lakiehdotuksien lisäksi esitysten perusteluja on tarvittavin määrin täydennetty saadun palautteen perusteella.

6 Riippuvuus muista esityksistä

Liikenne- ja viestintäministeriön hallinnonalan virastouudistus ja Liikenneviraston liikenteenohjaustehtävien yhtiöittäminen

Liikenne- ja viestintäministeriö on 25 päivänä huhtikuuta 2017 asettanut hankkeen, jossa valmistellaan hallituksen esitys eduskunnalle laeiksi Liikenne- ja X-virastoista ja niihin liittyväk-

si lainsäädännöksi sekä asetuksiksi ja hallituksen esitys eduskunnalle laiksi Liikenneviraston liikenteenohjaustoiminnon yhtiöittämisestä. Hankkeen tavoitteena on, että Liikenteen turvallisuusvirasto ja Viestintäviraston sekä Liikenneviraston tehtävät yhdistettäisiin yhdeksi virastoksi, kuitenkin niin, että Liikenneviraston liikenteenohjaustoiminto yhtiöitettäisiin valtion kokonaan omistamiksi erityistehtäväyhtiöiksi ja Liikennevirasto jatkaisi väyläverkosta vastaavana virastona.

Uudistuksen tavoitteena on parantaa hallinnonalan kykyä vastata asiakastarpeiden ja toimintaympäristön muutoksiin sekä kehittää ja vahvistaa hallinnonalan strategista ohjausta sekä saada synergiaetuja. Tavoitteena on myös parantaa edelleen hallinnon tuottavuutta ja vaikuttavuutta resurssien monipuolisemmalla ja tehokkaammalla käytöllä.

Liikenteenohjaustoimintojen yhtiöittämisen tavoitteena on lisäksi viranomaistehtävien selkeyttäminen sekä liikennealan sääntelyn sujuvoittaminen. Uudistuksella pyritään edesauttamaan liikenteeseen liittyvän tiedon hyödyntämistä yksityisellä sektorilla ja uuden liiketoiminnan syntymistä. Tavoitteena on, että liikenteen ohjauksella kerättävä tieto hyödyntää aiempaa tehokkaammin koko yhteiskuntaa.

6.1 Esityksen suhde Ahvenanmaan itsehallintoon

Ahvenanmaan itsehallintolain (1144/1991) 18 §:n 21 kohdan mukaan maakunnalla on lainsäädäntövalta koskien teitä ja kanavia, tieliikennettä, raideliikennettä, veneliikennettä sekä paikallisen meriliikenteen väyliä.

Ahvenanmaan itsehallintolain 18 §:n 22 kohdan mukaan maakunnalla on eräin rajoituksin lainsäädäntövaltaa asioissa, jotka koskevat elinkeinotoimintaa. Ahvenanmaan maakunnan toimivalta sähkö- ja energia-asioissa on maakunnan sähkölain (Ellag för landskapet Åland, ÅFS 1982:38) lainsäädäntövalvonnan yhteydessä johdettu aikaisemman Ahvenanmaan itsehallintolain (670/1951) 13 §:n 1 momentin 9 kohdasta, joka vastasi voimassa olevan Ahvenanmaan itsehallintolain elinkeinotoiminnasta säädettyä 18 §:n 22 kohtaa (HE 73/1990 vp s. 71). Itsehallintolaissa säädetystä valtakunnan ja maakunnan välisestä toimivallanjaosta johtuu, että sähkömarkkinalakia ei sovelleta Ahvenanmaan maakunnassa siltä osin kuin maakunnalla on lainsäädäntövalta sähkömarkkinoihin liittyvissä asioissa.

Ahvenanmaan itsehallintolain 27 §:n mukaan valtakunnalla on lainsäädäntövalta asioissa, jotka koskevat kauppamerenkulkua, ilmailua sekä valtion viranomaisten järjestysmuotoa ja toimintaa.

YKSITYISKOHTAISET PERUSTELUT

1 Lakiehdotusten perustelut

1.1 Laki tietoyhteiskuntakaaren muuttamisesta

247 a §. *Verkossa toimivan markkinapaikan, hakukonepalvelun sekä pilvipalvelun tarjoajan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.* Ehdotettu pykälä on uusi. Pykälässä säädettäisiin verkossa toimivan markkinapaikan tarjoajan, hakukonepalvelun tarjoajan sekä pilvipalvelun tarjoajan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Pykälän *1 momentin* mukaisella verkossa toimivalla markkinapaikalla tarkoitetaan verkko- ja tietoturvadirektiivin 4 artiklan 1 kohdan 17 alakohdan mukaista palvelua, jonka välityksellä käyttäjät voivat tehdä verkossa kauppa- tai palvelusopimuksia elinkeinonharjoittajien kanssa. Käyttäjät voivat olla Euroopan parlamentin ja neuvoston direktiivin 2013/11/EU 4 artiklan 1 kohdan a alakohdassa määriteltyjä kuluttajia tai kyseisen artiklan 1 kohdan b alakohdassa määriteltyjä elinkeinonharjoittajia. Palvelu voisi antaa mahdollisuuden tehdä sopimuksia elinkeinonharjoittajien kanssa omalla verkkosivustollaan tai muulla verkkosivustolla, joka käyttää verkossa toimivan markkinapaikan tarjoamia tietojenkäsittelypalveluja. Määritelmä ei kattaisi verkkopalveluja, joita käytetään vain välittäjänä kolmannen osapuolen palveluihin, joiden kautta sopimus voidaan lopulta tehdä. Määritelmä ei näin kata verkkopalveluja, joissa vertaillaan eri elinkeinonharjoittajien tiettyjen tuotteiden tai palvelujen hintoja ja sen jälkeen ohjataan käyttäjä valitun elinkeinonharjoittajan palveluun tuotteen ostamiseksi. Verkossa toimivan markkinapaikan tarjoamiin tietojenkäsittelypalveluihin voivat sisältyä maksutapahtumien käsittely, tietojen yhdistäminen tai käyttäjien profilointi. Verkossa toimivia markkinapaikkoja olisivat esimerkiksi sovelluskaupat, jotka toimivat kolmansien osapuolien tarjoamien sovellusten tai ohjelmistojen digitaalisen jakelun mahdollistavina verkkokauppoina, joko verkkosivuston tai sovelluksen kautta. Verkossa toimivia markkinapaikkoja eivät olisi yritykset, jotka myyvät suoraan kuluttajille tai elinkeinonharjoittajille tuotteita tai palveluitaan internetin välityksellä.

Hakukonepalvelulla tarkoitetaan verkko- ja tietoturvadirektiivin 4 artiklan 1 kohdan 18 alakohdan mukaista palvelua, joka etsii käyttäjän hakuun perustuen osumia määrittelemättömästä joukosta verkkosivustoja ja antaa käyttäjälle hakutuloksena linkkejä verkkosivustoille. Määrittelemättömällä joukolla verkkosivuja tarkoitettaisiin, että haku voidaan kohdistaa rajaamattomalle määrälle verkkosivustoja tai vaihtoehtoisesti kohdistaa esimerkiksi vain tietynkielisille verkkosivustoille, mutta haku ei kuitenkaan voisi rajoittua vain tietyn yksittäisen verkkosivuston sisältöön, riippumatta siitä, tarjoaako hakutoiminnon ulkoinen hakukone. Määritelmä ei myöskään kattaisi verkkopalveluja, joissa vertaillaan eri elinkeinonharjoittajien tiettyjen tuotteiden tai palvelujen hintoja ja sen jälkeen ohjataan käyttäjä valitun elinkeinonharjoittajan palveluun tuotteen ostamiseksi.

Pilvipalvelulla tarkoitetaan verkko- ja tietoturvadirektiivin 4 artiklan 1 kohdan 19 alakohdan mukaista palvelua, joka mahdollistaa verkon välityksellä pääsyn hajautettuihin tietoteknisiin resursseihin. Näihin tietoteknisiin resursseihin sisältyy verkkojen, palvelinten tai muun infrastruktuurin, tallentamisen, sovellusten ja palvelujen kaltaisia resursseja. Hajautetuilla resursseilla tarkoitettaisiin tietoteknisiä resursseja, joita pilvipalvelujen tarjoaja jakaa joustavasti resurssien maantieteellisestä sijainnista riippumatta kysynnän vaihtelujen mukaan, ja joita tarjo-

taan ja annetaan käyttöön kysynnän mukaan, jotta käytettävissä olevia resursseja voidaan lisätä ja vähentää nopeasti työtaakan mukaan. Lisäksi palveluita tarjotaan useille käyttäjille, joilla on yhteinen pääsy palveluun, mutta palvelussa käsittely kuitenkin tapahtuu erikseen kunkin käyttäjän osalta, vaikka palvelua tarjotaan samasta sähköisestä laitteistosta. Pilvipalvelu voi sisältää esimerkiksi ohjelmistojen hankkimista palveluna (Software as a Service), palvelimen tai tallennustilan hankkimista palveluna (Infrastructure as a Service) taikka sovelluskehitysalustojen tarjoamista palveluna (Platform as a Service).

Pykälän 1 momentin mukaiset tietojärjestelmät voivat koostua esimerkiksi tämän lain 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Pykälässä tarkoitettuja viestintäverkkoja ja tietojärjestelmiä olisivat ensisijaisesti yksityiset viestintäverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen, että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. Dokumentointi voitaisiin ottaa osaksi muita turvallisuusriskienhallintaa tai varautumista koskevia suunnitelmia

Pykälän *2 momentin* mukaan riskienhallinnassa on huomioitava järjestelmien ja tilojen turvallisuus, tietoturvaloukkausten ja häiriöiden käsittely, liiketoiminnan jatkuvuuden hallinta, seuranta, tarkastukset ja testaukset sekä kansainvälisten standardien noudattaminen. 2 momentin mukaisista parametreista on tarkemmin säädetty verkko- ja tietoturvadirektiivin nojalla annetussa komission täytäntöönpanoasetuksessa.

Pykälän *3 momentin* mukaan 1 momentissa tarkoitettua riskienhallintavelvoite ei koske verkko- ja tietoturvadirektiivin16 artiklan 11 kohdassa tarkoitettuja mikroyrityksiä tai pieniä yrityksiä. Rajauksen tarkoituksena olisi sulkea velvoitteiden piiristä pois komission suosituksessa mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä 2003/361/EY tarkoitetut mikroyritykset sekä pienet yritykset.

Ehdotetuilla säännöksillä pannaan täytäntöön verkko- ja tietoturvadirektiivin 16 artiklan 1 ja 2 kohta.

275 §. *Häiriöilmoitukset Viestintävirastolle.* Pykälä ehdotettaisiin muutettavan. Ehdotettu uusi *1 momentti* vastaisi voimassa olevan lain 1 momenttia muutoin, mutta momenttiin ehdotettaisiin lisättävän Viestintäviraston velvollisuus toimittaa komissiolle ja Euroopan verkko- ja tietoturvavirastolle tiivistelmäraportin häiriöilmoituksista. Velvoite vastaisi voimassa olevan lain 3 momentissa säädettyä.

Ehdotetussa uudessa *2 momentissa* säädettäisiin verkossa toimivan markkinapaikan tarjoajan, hakukonepalvelun tarjoajan sekä pilvipalvelun tarjoajan velvollisuudesta ilmoittaa sen palveluun kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä Viestintävirastolle. Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Määritelmä vastaisi verkko- ja tietoturvadirektiivin mukaista poikkeaman määritelmää. Häiriöön merkittävyyden arvioimiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys alueella, johon häiriö vaikuttaa, niin kuin on tarkemmin säädetty verkko- ja tietoturvadirektiivin nojalla annetussa Euroopan komission täytäntöönpanosäädöksessä.

Pykälän uudessa *3 momentissa* säädettäisiin Viestintäviraston oikeudesta velvoittaa palvelun tarjoaja tiedottamaan häiriöstä yleisölle tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. Viestintäviraston on ennen tiedottamista varattava palvelun tarjoajalle tilaisuus tulla kuulluksi. Viestintäviraston tulisi ensisijaisesti pyrkiä antamaan palvelun tarjoajalle mahdollisuus itse tiedottaa häiriöstä.

Ehdotettu uusi *4 momentti* vastaisi muutoin voimassa olevan lain 2 momenttia, mutta lisäksi siinä annettaisiin Viestintävirastolle toimivalta antaa määräyksiä myös uudessa 2 momentissa tarkoitettujen häiriöilmoituksien sisällöstä, muodosta ja toimittamisesta. Viestintävirastolle ei annettaisi toimivaltaa antaa määräyksiä siitä, milloin uudessa 2 momentissa tarkoitettu häiriö on merkittävä, sillä verkko- ja tietoturvadirektiivissä tämä toimivalta on annettu komissiolle.

Uudessa *5 momentissa* ehdotettaisiin velvoitetta Viestintävirastolle arvioida koskeeko uudessa 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltiota ja ilmoittaa tarvittaessa muille asiaan liittyville jäsenvaltioille. Tarkoituksena olisi varmistaa, että silloin kun häiriöllä on rajat ylittäviä vaikutuksia Euroopan unionissa ja Viestintävirasto katsoo, että häiriöstä olisi tarpeen kertoa toiselle jäsenvaltiolle, jäsenvaltiot, joita häiriö koskee, saisivat häiriöstä tiedon.

Ehdotetuilla säännöksillä pannaan täytäntöön verkko- ja tietoturvadirektiivin 16 artiklan 3 ja 4 sekä 6 ja 7 kohdat.

304 §. *Viestintäviraston erityiset tehtävät*. Pykälään tehtävien muutosten tarkoituksena olisi säätää Viestintäviraston tehtävistä, jotka liittyvät verkko- ja tietoturvadirektiivin 9 artiklan mukaisiin tehtäviin liittyen tietoturvaloukkauksiin reagoimiseen ja tutkimiseen. Viestintäviraston nykyiset tietoturvaloukkauksiin reagoimiseen ja tutkimiseen liittyvät tehtävät kattavat jo verkkopalveluihin, viestintäpalveluihin sekä lisäarvopalveluihin kohdistuvat tietoturvaloukkaukset. Ehdotetuilla muutoksilla Viestintäviraston tietoturvaloukkauksiin reagoimiseen ja tutkimiseen liittyviin tehtäviin lisättäisiin tietojärjestelmiin kohdistuvat tietoturvaloukkaukset. Pykälän mukaiset tietojärjestelmät voivat koostua esimerkiksi tämän lain 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Tietojärjestelmiin kohdistuviin tietoturvaloukkauksiin liittyvät teh-

tävät liittyisivät verkko- ja tietoturvadirektiivin 9 artiklassa tarkoitettuihin CSIRT-toimijan tehtäviin

308 §. *Yhteistyö eri viranomaisten kanssa.* Pykälään ehdotettaisiin lisättävän uusi 3 momentti, jossa säädettäisiin Viestintäviraston velvoitte*esta* toimia tarvittaessa yhteistyössä muiden jäsenvaltioiden verkko- ja tietoturvallisuuteen liittyvien eri viranomaisten kanssa. Yhteistyö muiden jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten kanssa voisi tarkoittaa esimerkiksi yhteistyötä silloin, kun valvottava toimija tarjoaa palveluita useammassa jäsenvaltiossa. Tietoturvaloukkauksiin reagoivilla yksiköillä tarkoitettaisiin verkko- ja tietoturvadirektiivin 9 artiklassa tarkoitettu CSIRT-toimijaa. Yhteistyö CSIRT-toimijoiden kanssa sisältäisi esimerkiksi osallistumisen verkko- ja tietoturvadirektiivin 12 artiklan mukaiseen CSIRT-verkostoon. Lisäksi säädettäisiin yhteistyöstä verkko- ja tietoturvadirektiivin mukaisen yhteistyöryhmän kanssa sekä velvoitteesta toimittaa yhteistyöryhmälle tiivistelmäraportti verko- ja tietoturvadirektiivin 14 ja 16 artiklan mukaisista häiriöilmoituksista.

313 §. *Valvonta-asioiden käsittely Viestintävirastossa*. Pykälän 2 momentin 2 kohtaan lisättäisiin Viestintävirastolle oikeus jättää asia tutkimatta, jos asialla olisi 247 a §:ssä tarkoitettujen palveluiden riskinhallinnan kannalta vain vähäinen merkitys. Tarkoituksena olisi antaa Viestintävirastolle oikeus käsitellä tämän lain 275 §:n 2 momentissa tarkoitettu tietoturvallisuuteen liittyvää häiriötä koskeva ilmoitus lain 304 §:n 1 momentin 7 ja 10 alakohtien mukaisesti selvitys- ja tiedonvaihtoasiana, silloin kun asialla olisi säännöksessä tarkoitettujen palveluiden riskinhallinnan kannalta vain vähäinen merkitys. Valvontaan olisi ryhdyttävä vain, jos häiriöön voi liittyä sellainen 247 a §:ssä säädettyjen riskinhallintavelvoitteiden laiminlyönti, johon puuttuminen on kyseisen toimijan tai yleisesti vastaavien palveluiden tarjoajien riskinhallinnan kannalta olennainen.

318 §. *Tietojen luovuttaminen viranomaisesta*. Pykälään ehdotettaisiin lisättävän uusi 2 momentti, jossa säädettäisiin Viestintäviraston oikeudesta luovuttaa tietoja verkko- ja tietoturvadirektiivin kannalta keskeisille valvontaviranomaisille. Tarkoituksena olisi varmistaa, että verkko- ja tietoturvadirektiivin mukaisia velvoitteita valvovat eri viranomaiset pystyisivät vaihtamaan valvontatehtäviensä kannalta merkityksellistä tietoa. Vaihdettavat tiedot voisivat sisältää esimerkiksi tietoja tietoturvallisuuteen liittyvistä häiriöistä.

Ehdotetuilla säännöksillä pannaan täytäntöön verkko- ja tietoturvadirektiivin 10 artikla.

1.2 Laki ilmailulain muuttamisesta

128 a §. *Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta* . Ehdotettu pykälä on uusi. Pykälässä säädettäisiin lennonvarmistuspalvelun tarjoajan ja yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Valtioneuvoston asetuksella säädettäisiin tarkemmin, milloin pykälässä tarkoitettua lentoasemaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä.

Pykälän *1 momentin* mukaisilla viestintäverkoilla tarkoitettaisiin tietoyhteiskuntakaaren 3 §:n 39 kohdassa tarkoitettuja viestintäverkkoja. 1 momentin mukaiset tietojärjestelmät voivat koostua esimerkiksi tietoyhteiskuntakaaren 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Pykälässä tarkoitettuja viestintäverkkoja ja tietojärjestelmiä olisivat ensisijaisesti yksityiset viestin-

täverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. 1 momentin mukainen riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat ilmailun turvallisuuden kannalta merkittäviä. Ilmailun turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä tai joihin kohdistuvat häiriöt voisivat aiheuttaa ilmailun turvallisuudelle riskin.

Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen, että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. Dokumentointi voitaisiin ottaa osaksi muita turvallisuusriskienhallintaa tai varautumista koskevia suunnitelmia

Pykälän *2 momentissa* säädettäisiin palvelun tarjoajan velvoitteesta antaa Liikenteen turvallisuusvirastolle velvoitteiden noudattamisen valvonnan kannalta tarvittavat tiedot.

Pykälän *3 momentissa* säädettäisiin Liikenteen turvallisuusviraston toimivallasta valvoa 1 momentissa säädettyjä velvoitteita ja oikeudesta velvoittaa 1 momentissa tarkoitettu palvelun tarjoajan ryhtymään korjaaviin toimenpiteisiin ilmailun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi.

Pykälän *4 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta luovuttaa salassa pidettävää tietoa Viestintävirastolle, mikäli se olisi välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi. Tällaiset tiedot voisivat sisältää esimerkiksi tietoja tietoturvapoikkeamista.

Pykälän *5 momentin* asetuksenantovaltuuden mukaan valtioneuvoston asetuksella säädetään tarkemmin, milloin 1 momentissa tarkoitettua lentoaseman pitäjää on pidettävä yhteiskunnan toiminnan kannalta merkittävänä. Tarkoituksena olisi, että asetuksella voitaisiin tarkoituksen mukaisin raja-arvoin määritellä ne lentoasemat, joiden pitäjiin riskienhallintavelvoitetta sovellettaisiin, sillä kaikkia lentoasemanpitäjiä ei olisi tarkoituksen mukaista pitää verkko- ja tietoturvadirektiivin mukaisina keskeisten palveluiden tarjoajina. Arvioidessa sitä, onko toimija yhteiskunnan toiminnan kannalta merkittävä, olisi huomioitava verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaiset kriteerit.

Ehdotetuilla säännöksillä pannan täytäntöön verkko- ja tietoturvadirektiivin 10 artikla, 14 artiklan 1 ja 2 kohdat sekä 15 artiklan 1 ja3 kohta direktiivin liitteen II toimialan 2 osa-alueen a osalta.

128 b §. *Tietoturvapoikkeamien ilmoittaminen.* Ehdotettu pykälä on uusi. Pykälässä säädettäisiin 128 a §:ssä tarkoitetun toimijan velvollisuudesta ilmoittaa tietoturvallisuuteen liittyvästä merkittävästä poikkeamasta Liikenteen turvallisuusvirastolle.

Pykälän *1 momentissa* säädettäisiin velvoitteesta ilmoittaa Liikenteen turvallisuusvirastolle merkittävästä poikkeamasta. Poikkeamalla tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Määritelmä vastaisi verkko- ja tietoturvadirektiivin mukaista poikkeaman määritelmää. Merkittävänä olisi pidettävä poikkeamaa, joka voi muodostaa vastaavan merkittävän riskin ilmailun turvallisuudelle, mitä on tarkoitettu poikkeama-asetuksen 4 artiklassa. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, poikkeaman kesto sekä maantieteellinen levinneisyys.

Pykälän *2 momentti* säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 momentti.

Pykälän *3 momentissa* ehdotettaisiin velvoitetta Liikenteen turvallisuusvirastolle arvioida onko uudessa 2 momentissa tarkoitetulla poikkeamalla merkittävä vaikutus keskeisten palvelujen jatkuvuuteen toisessa Euroopan unionin jäsenvaltiossa ja ilmoittaa tarvittaessa muille asiaan liittyville jäsenvaltioille. Tarkoituksena olisi varmistaa, että silloin kun poikkeamalla on rajat ylittäviä vaikutuksia Euroopan unionissa ja Liikenteenturvallisuusvirasto katsoo, että poikkeama olisi tarpeen kertoa toiselle jäsenvaltiolle, jäsenvaltiot, joita poikkeama koskee, saisivat häiriöstä tiedon. Ilmoitus voitaisiin tehdä esimerkiksi silloin, kun poikkeama voisi muodostaa merkittävän riskin ilmailun turvallisuudelle toisessa jäsenvaltiossa. Liikenteen turvallisuusvirasto voi pyytää Viestintävirastoa välittämään ilmoituksen toisen jäsenvaltion verkko- ja tietoturvadirektiivin 8 artiklassa tarkoitetulle keskitetylle yhteyspisteelle.

Pykälän *4 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta antaa tarkempia määräyksiä pykälässä tarkoitettujen ilmoituksen sisällöstä, muodosta ja toimittamisesta. Määräyksessä voitaisiin tarkemmin määrätä esimerkiksi siitä milloin 1 momentissa tarkoitettua poikkeamaa olisi pidettävä merkittävänä sekä siitä missä muodossa tiedot olisi annettava.

Ehdotetuilla säännöksillä pannan täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 3–6 kohdat direktiivin liitteen II toimialan 2 osa-alueen a osalta.

1.3 Laki rautatielain muuttamisesta

41 a §. *Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen.* Ehdotettu pykälä on uusi. Pykälässä säädettäisiin valtion rataverkon haltijan ja liikenteenohjauspalveluja tarjoavan yrityksen velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä velvollisuudesta ilmoittaa Liikenteen turvallisuusvirastolle merkittävästä järjestelmiensä tietoturvallisuuteen liittyvästä häiriöstä.

Pykälän *1 momentin* mukaisilla viestintäverkoilla tarkoitettaisiin tietoyhteiskuntakaaren 3 §:n 39 kohdassa tarkoitettuja viestintäverkkoja. 1 momentin mukaiset tietojärjestelmät voivat koostua esimerkiksi tietoyhteiskuntakaaren 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Pykälässä tarkoitettuja viestintäverkkoja ja tietojärjestelmiä olisivat ensisijaisesti yksityiset viestintäverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. 1 momentin mukainen riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat rautatieliikenteen turvallisuuden kannalta merkittäviä. Rautatieliikenteen turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä tai joihin kohdistuvat häiriöt voisivat aiheuttaa riskin rautatiejärjestelmän turvallisuudelle.

Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen, että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. Dokumentointi voitaisiin ottaa osaksi muita turvallisuusriskienhallintaa tai varautumista koskevia suunnitelmia

Pykälän *2 momentissa* säädettäisiin velvoitteesta ilmoittaa tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Liikenteen turvallisuusvirastolle. Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Määritelmä vastaisi verkko- ja tietoturvadirektiivin mukaista poikkeaman määritelmää. Merkittävänä olisi pidettävä häiriötä, joka voisi aiheuttaa rautatiejärjestelmälle vastaavan merkittävän turvallisuusriskin kuin on tarkoitettu rautatielain 39 §:n 2 momentissa. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys.

Pykälän *3 momentti* säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 momentti.

Pykälän *4 momentissa* ehdotettaisiin velvoitetta Liikenteen turvallisuusvirastolle arvioida onko 2 momentissa tarkoitetulla häiriöllä merkittävä vaikutus keskeisten palvelujen jatkuvuuteen toisessa Euroopan unionin jäsenvaltiossa ja ilmoittaa tarvittaessa muille asiaan liittyville jä-

senvaltioille. Tarkoituksena olisi varmistaa, että silloin kun häiriöllä on rajat ylittäviä vaikutuksia Euroopan unionissa ja Liikenteenturvallisuusvirasto katsoo, että häiriöstä olisi tarpeen kertoa toiselle jäsenvaltiolle, jäsenvaltiot, joita häiriö koskee, saisivat häiriöstä tiedon. Ilmoitus voitaisiin tehdä esimerkiksi silloin, kun häiriö voisi muodostaa merkittävän riskin rautatiejärjestelmän turvallisuudelle toisessa jäsenvaltiossa. Liikenteen turvallisuusvirasto voi pyytää Viestintävirastoa välittämään ilmoituksen toisen jäsenvaltion verkko- ja tietoturvadirektiivin 8 artiklassa tarkoitetulle keskitetylle yhteyspisteelle.

Pykälän *5 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta luovuttaa salassa pidettävää tietoa Viestintävirastolle, mikäli se olisi välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi. Tällaiset tiedot voisivat sisältää esimerkiksi tietoja tietoturvallisuuteen liittyvistä häiriöistä.

Pykälän *6 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta antaa tarkempia määräyksiä pykälässä tarkoitettujen ilmoituksen sisällöstä, muodosta ja toimittamisesta. Määräyksessä voitaisiin tarkemmin määrätä esimerkiksi siitä milloin 2 momentissa tarkoitettua tietoturvallisuuteen liittyvää häiriötä olisi pidettävä merkittävänä sekä siitä missä muodossa tiedot olisi annettava.

Ehdotetuilla säännöksillä pannaan täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 1–6 kohdat sekä 10 artikla direktiivin liitteen II toimialan 2 osa-alueen b osalta.

1.4 Laki alusliikennepalvelulain muuttamisesta

16 §. *Alusliikennepalvelun ylläpito.* Pykälään ehdotettaisiin lisättävän uusi *5 momentti*, jossa säädettäisiin alusliikennepalvelun tarjoajan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Pykälän 5 *momentin* mukaisilla viestintäverkoilla tarkoitettaisiin tietoyhteiskuntakaaren 3 §:n 39 kohdassa tarkoitettuja viestintäverkkoja. 1 momentin mukaiset tietojärjestelmät voivat koostua esimerkiksi tietoyhteiskuntakaaren 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Pykälässä tarkoitettuja viestintäverkkoja ja tietojärjestelmiä olisivat ensisijaisesti yksityiset viestintäverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. 5 momentin mukainen riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat merenkulun turvallisuuden kannalta merkittäviä. Merenkulun turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä tai joihin kohdistuvat häiriöt voisivat aiheuttaa riskin merenkulun turvallisuudelle. Velvoite kohdistuisi VTS-viranomaisen tehtäviin, jotka liittyvät liikenteenohjaamisen operatiiviseen toimintaan.

Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatimi-

nen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen, että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. Dokumentointi voitaisiin ottaa osaksi muita turvallisuusriskienhallintaa tai varautumista koskevia suunnitelmia

Ehdotetuilla säännöksillä yhdessä eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin ehdotettujen kanssa pannan täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 1 ja 2 kohdat direktiivin liitteen II toimialan 2 osa-alueen c osalta.

18 a §. *Velvollisuus ilmoittaa tietoturvallisuuteen liittyvistä häiriöistä.* Ehdotettu pykälä on uusi. Pykälässä säädettäisiin tietoturvallisuuteen liittyvien häiriöiden ilmoittamisesta sekä Liikenteen turvallisuusviraston oikeudesta antaa ilmoituksia koskevia määräyksiä.

Pykälän *1 momentissa* säädettäisiin velvoitteesta ilmoittaa tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Liikenteen turvallisuusvirastolle. Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Määritelmä vastaisi verkko- ja tietoturvadirektiivin mukaista poikkeaman määritelmää. Merkittävänä olisi pidettävä häiriötä, joka voisi merkittävästi vaikuttaa merenkulun turvallisuuteen. Häiriön merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys.

Pykälän *2 momentti* säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 momentti.

Pykälän *3 momentissa* ehdotettaisiin velvoitetta Liikenteen turvallisuusvirastolle arvioida onko 2 momentissa tarkoitetulla häiriöllä merkittävä vaikutus keskeisten palvelujen jatkuvuuteen toisessa Euroopan unionin jäsenvaltiossa ja ilmoittaa tarvittaessa muille asiaan liittyville jäsenvaltioille. Tarkoituksena olisi varmistaa, että silloin kun häiriöllä on rajat ylittäviä vaikutuksia Euroopan unionissa ja Liikenteenturvallisuusvirasto katsoo, että häiriöstä olisi tarpeen kertoa toiselle jäsenvaltiolle, jäsenvaltiot, joita häiriö koskee, saisivat häiriöstä tiedon. Ilmoitus voitaisiin tehdä esimerkiksi silloin, kun häiriö voisi merkittävästi vaikuttaa merenkulun turvallisuuteen toisessa jäsenvaltiossa. Liikenteen turvallisuusvirasto voi pyytää Viestintävirastoa välittämään ilmoituksen toisen jäsenvaltion verkko- ja tietoturvadirektiivin 8 artiklassa tarkoitetulle keskitetylle yhteyspisteelle.

Pykälän *4 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta antaa tarkempia määräyksiä pykälässä tarkoitettujen ilmoituksen sisällöstä, muodosta ja toimittamisesta. Määräyksessä voitaisiin tarkemmin määrätä esimerkiksi siitä milloin 1 momentissa tarkoitettua tie-

toturvallisuuteen liittyvää häiriötä olisi pidettävä merkittävänä sekä siitä missä muodossa tiedot olisi annettava.

Pykälän *5 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta luovuttaa salassa pidettävää tietoa Viestintävirastolle, mikäli se olisi välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi. Tällaiset tiedot voisivat sisältää esimerkiksi tietoja tietoturvallisuuteen liittyvistä häiriöistä

Ehdotetuilla säännöksillä yhdessä eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin ehdotettujen kanssa pannan täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 3–6 kohdat sekä 10 artikla direktiivin liitteen II toimialan 2 osa-alueen c osalta.

28 §. *Valvonta.* Pykälään ehdotettaisiin lisättävän uusi *4 momentti*, jossa säädettäisiin 16 §:n 5 momentissa tarkoitetun riskienhallinnan valvonnasta. Liikenteen turvallisuusvirasto voisi velvoittaa VTS-viranomaisen ryhtymään korjaaviin toimenpiteisiin merenkulun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi. Merkittävällä riskillä tarkoitettaisiin ehdotetun 18 a §:n 1 momenttia vastaavaa merkittävää vaikutusta. Lisäksi säädettäisiin Liikenteen turvallisuusviraston mahdollisuudesta antaa velvoitteen tehosteeksi uhkasakko.

Ehdotetuilla säännöksillä yhdessä eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin ehdotettujen kanssa pannan täytäntöön verkko- ja tietoturvadirektiivin direktiivin 15 artiklan 1 ja 3 kohdat sekä 21 artikla direktiivin liitteen II toimialan 2 osa-alueen c osalta.

1.5 Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta

7 e §. *Satamanpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen*. Ehdotettu pykälä on uusi. Pykälässä säädettäisiin yhteiskunnan toiminnan kannalta keskeisen sataman pitäjän velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Pykälän *1 momentin* mukaisilla viestintäverkoilla tarkoitettaisiin tietoyhteiskuntakaaren 3 §:n 39 kohdassa tarkoitettuja viestintäverkkoja. 1 momentin mukaiset tietojärjestelmät voivat koostua esimerkiksi tietoyhteiskuntakaaren 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Pykälässä tarkoitettuja viestintäverkkoja ja tietojärjestelmiä olisivat ensisijaisesti yksityiset viestintäverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. 1 momentin mukainen riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat merenkulun turvallisuuden kannalta merkittäviä. Merenkulun turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä tai joihin kohdistuvat häiriöt voisivat aiheuttaa riskin merenkulun turvallisuudelle.

Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden

kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen, että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. Dokumentointi voitaisiin ottaa osaksi muita turvallisuusriskienhallintaa tai varautumista koskevia suunnitelmia

Pykälän *2 momentissa* säädettäisiin Liikenteen turvallisuusviraston toimivallasta valvoa 1 momentissa säädettyjä velvoitteita ja oikeudesta velvoittaa 1 momentissa tarkoitettu palvelun tarjoajan ryhtymään korjaaviin toimenpiteisiin merenkulun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi. Velvoitteen tehostamiseksi Liikenteen turvallisuusvirasto voisi asettaa uhkasakon.

Pykälän *3 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta luovuttaa salassa pidettävää tietoa Viestintävirastolle, mikäli se olisi välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi. Tällaiset tiedot voisivat sisältää esimerkiksi tietoja tietoturvapoikkeamista.

Pykälän *4 momentin* asetuksenantovaltuuden mukaan valtioneuvoston asetuksella säädetään tarkemmin, milloin 1 momentissa tarkoitettua satamaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä. Tarkoituksena olisi, että asetuksella voitaisiin tarkoituksenmukaisin raja-arvoin määritellä ne satamat, joidenka pitäjiin riskienhallintavelvoitetta sovellettaisiin, sillä kaikkia satamanpitäjiä ei olisi tarkoituksenmukaista pitää verkko- ja tietoturvadirektiivin mukaisin keskeisten palveluiden tarjoajina. Arvioidessa sitä, onko toimija yhteiskunnan toiminnan kannalta merkittävä, olisi huomioitava verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaiset kriteerit.

Ehdotetuilla säännöksillä yhdessä alusliikennepalvelulakiin ehdotettujen muutosten kanssa pannan täytäntöön verkko- ja tietoturvadirektiivin 10 artikla, 14 artiklan 1 ja 2 kohdat, 15 artiklan 3 kohta sekä 21 artikla direktiivin liitteen II toimialan 2 osa-alueen c osalta.

7 f §. *Tietoturvallisuuteen liittyvistä häiriöistä ilmoittaminen*. Ehdotettu pykälä on uusi. Pykälän *1 momentissa* säädettäisiin velvoitteesta ilmoittaa tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Liikenteen turvallisuusvirastolle. Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Määritelmä vastaisi verkko- ja tietoturvadirektiivin mukaista poikkeaman määritelmää. Merkittävänä olisi pidettävä häiriötä, joka voisi merkittävästi vaikuttaa merenkulun turvallisuuteen. Poikkeaman merkittävyyden määrittämiseksi olisi otettava

huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, poikkeaman kesto sekä maantieteellinen levinneisyys.

Pykälän *2 momentti* säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 momentti.

Pykälän *3 momentissa* ehdotettaisiin velvoitetta Liikenteen turvallisuusvirastolle arvioida onko 2 momentissa tarkoitetulla häiriöllä merkittävä vaikutus keskeisten palvelujen jatkuvuuteen toisessa Euroopan unionin jäsenvaltiossa ja ilmoittaa tarvittaessa muille asiaan liittyville jäsenvaltioille. Tarkoituksena olisi varmistaa, että silloin kun häiriöllä on rajat ylittäviä vaikutuksia Euroopan unionissa ja Liikenteenturvallisuusvirasto katsoo, että häiriöstä olisi tarpeen kertoa toiselle jäsenvaltiolle, jäsenvaltiot, joita häiriö koskee, saisivat häiriöstä tiedon. Ilmoitus voitaisiin tehdä esimerkiksi silloin, kun häiriö voisi merkittävästi vaikuttaa merenkulun turvallisuuteen toisessa jäsenvaltiossa. Liikenteen turvallisuusvirasto voi pyytää Viestintävirastoa välittämään ilmoituksen toisen jäsenvaltion verkko- ja tietoturvadirektiivin 8 artiklassa tarkoitetulle keskitetylle yhteyspisteelle.

Pykälän *4 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta antaa tarkempia määräyksiä pykälässä tarkoitettujen ilmoituksen sisällöstä, muodosta ja toimittamisesta. Määräyksessä voitaisiin tarkemmin määrätä esimerkiksi siitä milloin 1 momentissa tarkoitettua tietoturvallisuuteen liittyvää häiriötä olisi pidettävä merkittävänä sekä siitä missä muodossa tiedot olisi annettava.

Ehdotetuilla säännöksillä yhdessä alusliikennepalvelulakiin ehdotettujen muutosten kanssa pannan täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 3–6 kohdat direktiivin liitteen II toimialan 2 osa-alueen c osalta.

1.6 Laki liikenteenpalveluista annetun lain muuttamisesta

III OSA. PALVELUT

2 luku. Tietojen ja tietojärjestelmien yhteentoimivuus

7 §. *Älykkään liikennejärjestelmän ylläpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen.* Ehdotettu pykälä on uusi. Pykälässä säädettäisiin älykkään liikennejärjestelmän ylläpitäjän velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä velvollisuudesta ilmoittaa järjestelmiensä tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Liikenteen turvallisuusvirastolle. Älykkäillä liikennejärjestelmillä tarkoitetaan lain 2 luvun 6 §:ssä ja tieliikenteen älykkäiden liikennejärjestelmien käyttöönoton sekä tieliikenteen ja muiden liikennemuotojen rajapintojen puitteista annetun Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU 4 artiklan 1 kohdassa tarkoitettuja järjestelmiä.

Pykälän *1 momentin* mukaisilla viestintäverkoilla tarkoitettaisiin tietoyhteiskuntakaaren 3 §:n 39 kohdassa tarkoitettuja viestintäverkkoja. 1 momentin mukaiset tietojärjestelmät voivat koostua esimerkiksi tietoyhteiskuntakaaren 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Pykälässä tarkoitettuja viestintäverkkoja ja tietojärjestelmiä olisivat ensisijaisesti yksityiset viestin-

täverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Riskienhallintavelvoite koskisi vain viestintäverkkoja ja tietojärjestelmiä, jotka olisivat älykkään liikennejärjestelmän turvallisuudelle merkittäviä. Älykkään liikennejärjestelmän turvallisuuden kannalta merkittävinä olisi ainakin pidettävä järjestelmiä, jotka ovat palvelun tarjonnan jatkuvuuden kannalta keskeisiä.

Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen, että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. Dokumentointi voitaisiin ottaa osaksi muita turvallisuusriskienhallintaa tai varautumista koskevia suunnitelmia

Pykälän *2 momentissa* säädettäisiin velvoitteesta ilmoittaa tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Liikenteen turvallisuusvirastolle. Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Määritelmä vastaisi verkko- ja tietoturvadirektiivin mukaista poikkeaman määritelmää. Merkittävänä olisi pidettävä häiriötä joka voi muodostaa älykkään liikennejärjestelmän turvallisuudelle merkittävän riskin. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys.

Pykälän *3 momentti* säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 momentti.

Pykälän *4 momentissa* ehdotettaisiin velvoitetta Liikenteen turvallisuusvirastolle arvioida onko 2 momentissa tarkoitetulla häiriöllä merkittävä vaikutus keskeisten palvelujen jatkuvuuteen toisessa Euroopan unionin jäsenvaltiossa ja ilmoittaa tarvittaessa muille asiaan liittyville jäsenvaltioille. Tarkoituksena olisi varmistaa, että silloin kun häiriöllä on rajat ylittäviä vaikutuksia Euroopan unionissa ja Liikenteenturvallisuusvirasto katsoo, että häiriöstä olisi tarpeen kertoa toiselle jäsenvaltiolle, jäsenvaltiot, joita häiriö koskee, saisivat häiriöstä tiedon. Ilmoitus voitaisiin tehdä esimerkiksi silloin, kun häiriö voisi merkittävästi vaikuttaa älykkään liikennejärjestelmän turvallisuuden toisessa jäsenvaltiossa. Liikenteen turvallisuusvirasto voi pyytää Viestintävirastoa välittämään ilmoituksen toisen jäsenvaltion verkko- ja tietoturvadirektiivin 8 artiklassa tarkoitetulle keskitetylle yhteyspisteelle.

Pykälän *5 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta luovuttaa salassa pidettävää tietoa Viestintävirastolle, mikäli se olisi välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi. Tällaiset tiedot voisivat sisältää esimerkiksi tietoja tietoturvallisuuteen liittyvistä häiriöistä.

Pykälän *6 momentissa* säädettäisiin Liikenteen turvallisuusviraston oikeudesta antaa tarkempia määräyksiä pykälässä tarkoitettujen ilmoituksen sisällöstä, muodosta ja toimittamisesta. Määräyksessä voitaisiin tarkemmin määrätä esimerkiksi siitä milloin 2 momentissa tarkoitettua tietoturvallisuuteen liittyvää häiriötä olisi pidettävä merkittävänä sekä siitä missä muodossa tiedot olisi annettava.

Ehdotetuilla säännöksillä pannaan täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 1–6 kohdat sekä 10 artikla direktiivin liitteen II toimialan 2 osa-alueen d osalta.

1.7 Laki sähkömarkkinalain muuttamisesta

29 a §. *Verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen* . Ehdotettu pykälä on uusi. Pykälässä säädettäisiin verkonhaltijan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä velvollisuudesta ilmoittaa järjestelmiensä tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Energiavirastolle. Pykälän säännöksiä sovellettaisiin kaikkiin verkonhaltijoihin lukuun ottamatta suljetun jakeluverkon haltijoita.

Pykälän *1 momentin* mukaisilla viestintäverkoilla tarkoitettaisiin tietoyhteiskuntakaaren 3 §:n 39 kohdassa tarkoitettuja viestintäverkkoja. 1 momentin mukaiset tietojärjestelmät voivat koostua esimerkiksi tietoyhteiskuntakaaren 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Pykälässä tarkoitettuja viestintäverkkoja ja tietojärjestelmiä olisivat ensisijaisesti yksityiset viestintäverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Pykälän 1 momentin mukainen riskienhallintavelvoite kohdistuisi sellaisiin tietojärjestelmiin ja viestintäverkkoihin, jotka olisivat merkityksellisiä sähkönjakelun jatkuvuuden kannalta.

Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen,

että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. Dokumentointi voitaisiin ottaa osaksi muita turvallisuusriskienhallintaa tai varautumista koskevia suunnitelmia, kuten esimerkiksi osaksi 28 §:ssä tarkoitettua varautumissuunnitelmaa.

Pykälän *2 momentissa* säädettäisiin velvoitteesta ilmoittaa merkittävästä tietoturvallisuuteen liittyvästä häiriöstä Energiavirastolle. Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Määritelmä vastaisi verkko- ja tietoturvadirektiivin mukaista poikkeaman määritelmää. Merkittävänä olisi pidettävä häiriötä, jonka seurauksena sähkönjakelu voi keskeytyä jakeluverkossa merkittävässä laajuudessa. Ilmoituskynnys, silloin kun häiriön seurauksena sähkönjakelu voi keskeytyä merkittävässä laajuudessa, vastaisi sähkömarkkinalain 59 §:n ilmoituskynnystä. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys.

Pykälän *3 momentti* säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 momentti.

Pykälän *4 momentissa* ehdotettaisiin velvoitetta Energiavirastolle arvioida onko 2 momentissa tarkoitetulla häiriöllä merkittävä vaikutus keskeisten palvelujen jatkuvuuteen toisessa Euroopan unionin jäsenvaltiossa ja ilmoittaa tarvittaessa muille asiaan liittyville jäsenvaltioille. Tarkoituksena olisi varmistaa, että silloin kun häiriöllä on rajat ylittäviä vaikutuksia Euroopan unionissa ja Energiavirasto katsoo, että häiriöstä olisi tarpeen kertoa toiselle jäsenvaltiolle, jäsenvaltiot, joita häiriö koskee, saisivat häiriöstä tiedon. Ilmoitus voitaisiin tehdä esimerkiksi silloin, kun häiriö voisi merkittävästi vaikuttaa sähkönjakelun jatkuvuuteen toisessa jäsenvaltiossa. Energiavirasto voi pyytää Viestintävirastoa välittämään ilmoituksen toisen jäsenvaltion verkko- ja tietoturvadirektiivin 8 artiklassa tarkoitetulle keskitetylle yhteyspisteelle.

Pykälän *5 momentissa* säädettäisiin Energiaviraston oikeudesta antaa tarkempia määräyksiä pykälässä tarkoitettujen ilmoituksen sisällöstä, muodosta ja toimittamisesta. Määräyksessä voitaisiin tarkemmin määrätä esimerkiksi siitä milloin 2 momentissa tarkoitettua tietoturvallisuuteen liittyvää häiriötä olisi pidettävä merkittävänä sekä siitä missä muodossa tiedot olisi annettava.

Ehdotetuilla säännöksillä pannaan täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 1–6 kohdat direktiivin liitteen II toimialan 1 osa-alueen a osalta.

62 §. *Suljettua jakeluverkkoa koskevat erityissäännökset*. Pykälään ehdotettaisiin lisättävän, ettei suljettuun jakeluverkkoon ja suljetun jakeluverkonhaltijaan sovelleta ehdotettua 29 a §:ää. Velvoitetta huolehtia tietoturvasta ei tulisi soveltaa suljetun jakeluverkonhaltijaan, sillä sähkönjakelua suljetussa jakeluverossa ei olisi pidettävä verkko- ja tietoturvadirektiivin tarkoittamalla tavalla keskeisenä palveluna.

1.8 Laki maakaasumarkkinalain muuttamisesta

34 a §. *Siirtoverkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen.* Ehdotettu pykälä on uusi. Pykälässä säädettäisiin siirtoverkonhaltijan velvollisuudesta huolehtia käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä velvollisuudesta ilmoittaa järjestelmiensä tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Energiavirastolle.

Pykälän *1 momentin* mukaisilla viestintäverkoilla tarkoitettaisiin tietoyhteiskuntakaaren 3 §:n 39kohdassa tarkoitettuja viestintäverkkoja. 1 momentin mukaiset tietojärjestelmät voivat koostua esimerkiksi tietoyhteiskuntakaaren 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. Pykälässä tarkoitettuja viestintäverkkoja ja tietojärjestelmiä olisivat ensisijaisesti yksityiset viestintäverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Pykälän 1 momentin mukainen riskienhallintavelvoite kohdistuisi sellaisiin tietojärjestelmiin ja viestintäverkkoihin, jotka olisivat merkityksellisiä maakaasunsiirron jatkuvuuden kannalta.

Riskienhallinnalla tarkoitettaisiin asianmukaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistettaisiin viestintäverkkojen ja tietojärjestelmien kyky suojautua tietyllä varmuudella toimilta, jotka vaarantavat tallennettujen tai siirrettyjen tai käsiteltyjen tietojen taikka muiden kyseisissä järjestelmissä tarjottujen tai niiden välityksellä saatavilla olevien palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnan tulisi sisältää asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan palvelujen tarjoamisessa käytettyjen järjestelmien tietoturvallisuuteen liittyvien häiriöiden vaikutus palvelujen jatkuvuuteen. Riskienhallintaan kuuluvia toimenpiteitä voisivat olla esimerkiksi turvallisuussuunnitelmien laatiminen, testaaminen käytännössä tai auditoiminen, tiedon suojaus- ja salaustuotteiden käyttö sekä tiettyjen tunnettujen tietoturvallisuusstandardien, kuten ISO/IEC 27001:2013 -standardin, noudattaminen. Riskillä tarkoitettaisiin mitä tahansa kohtuullisesti tunnistettavissa olevaa tilannetta tai tapahtumaa, joka saattaa vaikuttaa haitallisesti viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Riskienhallinnan tulisi olla todennettavassa muodossa. Dokumentoinnin tavoite on edistää riskien johdonmukaista hallintaa ja toimijan tietoisia ratkaisuja siitä, miten riskien hallitsemiseen tarvittavat toimet mitoitetaan. Dokumentointi mahdollistaisi myös sen, että viranomainen voi tarvittaessa jälkikäteen arvioida pykälän velvoitteiden noudattamista. Dokumentointi voisi tarkoittaa esimerkiksi kirjallisessa muodossa laadittavien riskiarvioiden, turvallisuusohjeiden tai toimintasuunnitelmien laadintaa taikka todistuksia turvallisuustarkastusten suorittamisesta. Dokumentointi voitaisiin ottaa osaksi muita turvallisuusriskienhallintaa tai varautumista koskevia suunnitelmia

Pykälän *2 momentissa* säädettäisiin velvoitteesta ilmoittaa Energiavirastolle merkittävästä tietoturvallisuuteen liittyvästä häiriöstä Energiavirastolle. Tietoturvallisuuteen liittyvällä häiriöllä tarkoitettaisiin mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti kyseessä olevien järjestelmien turvallisuuteen. Määritelmä vastaisi verkko- ja tietoturvadirektiivin mukaista poikkeaman määritelmää. Merkittävänä olisi pidettävä häiriötä, jonka seurauksena maakaasun siirto voi keskeytyä siirtoverkossa merkittävässä laajuudessa. Häiriön merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, häiriön kesto sekä maantieteellinen levinneisyys.

Pykälän *3 momentti* säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 momentti.

Pykälän *4 momentissa* ehdotettaisiin velvoitetta Energiavirastolle arvioida onko 2 momentissa tarkoitetulla häiriöllä merkittävä vaikutus keskeisten palvelujen jatkuvuuteen toisessa Euroopan unionin jäsenvaltiossa ja ilmoittaa tarvittaessa muille asiaan liittyville jäsenvaltioille. Tarkoituksena olisi varmistaa, että silloin kun häiriöllä on rajat ylittäviä vaikutuksia Euroopan unionissa ja Energiavirasto katsoo, että häiriöstä olisi tarpeen kertoa toiselle jäsenvaltiolle, jäsenvaltiot, joita häiriö koskee, saisivat häiriöstä tiedon. Ilmoitus voitaisiin tehdä esimerkiksi silloin, kun häiriö voisi merkittävästi vaikuttaa maakaasunjakelun jatkuvuuteen toisessa jäsenvaltiossa. Energiavirasto voi pyytää Viestintävirastoa välittämään ilmoituksen toisen jäsenvaltion verkko- ja tietoturvadirektiivin 8 artiklassa tarkoitetulle keskitetylle yhteyspisteelle.

Pykälän *5 momentissa* säädettäisiin Energiaviraston oikeudesta antaa tarkempia määräyksiä pykälässä tarkoitettujen ilmoituksen sisällöstä, muodosta ja toimittamisesta. Määräyksessä voitaisiin tarkemmin määrätä esimerkiksi siitä milloin 2 momentissa tarkoitettua tietoturvallisuuteen liittyvää häiriötä olisi pidettävä merkittävänä sekä siitä missä muodossa tiedot olisi annettava.

Ehdotetuilla säännöksillä pannaan täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 1–6 kohdat direktiivin liitteen II toimialan 1 osa-alueen c osalta.

1.9 Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 27 ja 28 §:n muuttamisesta

27 §. *Viranomaisten valvontayhteistyö.* Pykälää ehdotettaisiin muutettavan niin, että siinä säädettäisiin Energiaviraston oikeudesta tehdä valvontayhteistyötä Viestintäviraston kanssa. Valvontayhteistyön tekeminen voisi olla tarpeen tietoturvallisuuteen liittyvien velvoitteiden valvomiseksi. Lisäksi viittaukset Energiamarkkinavirastoon korvattaisiin viittauksilla Energiavirastoon. Säännöksellä pannaan täytäntöön verkko- ja tietoturvadirektiivin 10 artiklan 1 kohta direktiivin liitteen II toimialan 1 osalta.

28 §. *Energiaviraston oikeus luovuttaa tietoja toiselle viranomaiselle.* Pykälää ehdotettaisiin muutettavan niin, että siinä säädettäisiin Energiaviraston oikeudesta luovuttaa salassa pidettäviä tietoja Viestintävirastolle. Tietojen luovuttaminen voisi olla välttämätöntä tietoturvallisuuteen liittyvien velvoitteiden valvomiseksi. Lisäksi viittaukset Energiamarkkinavirastoon korvattaisiin viittauksilla Energiavirastoon. Säännöksellä pannaan täytäntöön verkko- ja tietoturvadirektiivin 10 artiklan 2 ja 3 kohta direktiivin liitteen II toimialan 1 osalta.

1.10 Laki vesihuoltolain muuttamisesta

15 b §. *Vesihuollon häiriötilanteesta ilmoittaminen.* Lakiin lisättäisiin uusi pykälä vesihuoltolaitoksen sekä elinkeino-, liikenne- ja ympäristökeskuksen velvollisuudesta ilmoittaa merkittävistä vesihuollon häiriöistä. Ehdotetuilla säännöksillä pantaisiin myös täytäntöön verkko- ja tietoturvadirektiivin 14 artiklan 3–6 kohdat direktiivin liitteen II toimialan 6 osalta.

Voimassa olevan vesihuoltolain 15 a §:n mukaan vesihuoltolaitos vastaa verkostoihinsa liitettyjen kiinteistöjen vesihuoltopalvelujen saatavuudesta myös häiriötilanteissa. Palveluiden turvaamiseksi vesihuoltolaitoksen on laadittava ja pidettävä ajan tasalla suunnitelma häiriötilanteisiin varautumisesta ja ryhdyttävä sen perusteella tarvittaviin toimenpiteisiin. Elinkeino-, liikenne- ja ympäristökeskus sekä kunnan ympäristönsuojeluviranomainen ja terveydensuojelu-

viranomainen valvovat, että laitos täyttää suunnitteluvelvoitteensa, Laitoksilla ei kuitenkaan ole vesihuoltolain mukaan velvollisuutta ilmoittaa häiriötilanteista valvontaviranomaisille.

Vesihuoltolaitoksen on nykyisin ilmoitettava eräistä vesihuollon häiriötilanteista ympäristönsuojelua tai terveydensuojelua koskevan lainsäädännön perusteella. Häiriöiden ilmoittamisesta säädetään nykyisin eri tavoin eri laeissa, ja joistakin vesihuollon häiriöistä kuten katkoksista talousveden jakelussa tai jätevesien johtamisessa ilmoitusvelvollisuudesta ei ole säädetty lainkaan. Alueellisen tilannekuvan muodostamiseksi, vesihuollon haavoittuvuuksien tunnistamiseksi ja riskienhallinnan parantamiseksi on siksi tarpeen, että laitokset ilmoittaisivat kaikentyyppisistä merkittävistä vesihuollon häiriötilanteista ja että ilmoitukset tehtäisiin myös kootusti yhdelle alueelliselle viranomaiselle.

Pykälän *1 momentissa* säädettäisiin tämän vuoksi, että vesihuoltolaitoksen olisi ilmoitettava vesihuollon merkittävistä häiriötilanteista elinkeino-, liikenne- ja ympäristökeskukselle häiriön syystä ja ilmenemistavasta riippumatta. Velvollisuus koskisi laitoksia, jotka toimittavat vettä vähintään 5 000 kuutiometriä vuorokaudessa. Tällaisia laitoksia on Suomessa noin 40 kappaletta, ja niiden asiakasmäärä kattaa yli puolet Suomen väestöstä. Tämän kokoluokan laitokset on myös luokiteltu huoltovarmuuden kannalta kriittisiksi vesihuoltolaitoksiksi. Sellaisilla laitoksilla, jotka käsittelevät myös oman verkostonsa ulkopuolisia jätevesiä, ilmoitusvelvollisuuden tulisi tarvittaessa määräytyä vastaan otetun jätevesimäärän perusteella laitoksen toimittaman talousveden määrästä riippumatta. Ilmoitusvelvollisuus säädettäisiin tämän vuoksi koskemaan myös vesihuoltolaitoksia, jota ottavat vastaan jätevettä vähintään 5 000 kuutiometriä vuorokaudessa.

Ilmoitus olisi tehtävä vain vesihuollon merkittävistä häiriötilanteista. Häiriön merkittävyyden arvioinnissa huomioon otettavista seikoista voitaisiin säätää tarkemmin pykälän 4 momentissa tarkoitetulla maa- ja metsätalousministeriön asetuksella.

Pykälän *1 momentin* mukaan elinkeino-, liikenne- ja ympäristökeskus voisi velvoittaa laitoksen tiedottamaan häiriötilanteesta. Häiriöstä ja sen vaatimista toimenpiteistä olisi yleensä riittävää tiedottaa asiakkaille ja viranomaisille laitoksen vesihuoltolain mukaisella toiminta-alueella sekä laitoksen mahdollisille asiakkaille toiminta-alueen ulkopuolella. Tiedottamisen sisältö ja laajuus olisivat kuitenkin tapauskohtaisesti elinkeino-, liikenne- ja ympäristökeskuksen harkittavissa. Elinkeino-, liikenne- ja ympäristökeskus voisi myös katsoa tarkoituksenmukaiseksi huolehtia tiedottamisesta osittain tai kokonaan itse.

Pykälän *2 momentin* mukaan vesihuoltolaitokselle 1 momentissa tarkoitettu ilmoittamisvelvollisuus ja tiedottamisvelvollisuus koskisivat myös vesihuoltolaitokselle vettä toimittavia tai vesihuoltolaitoksen jätevesiä vastaanottavia laitoksia.

Pykälän *3 momentin* mukaan elinkeino-, liikenne- ja ympäristökeskuksen olisi toimitettava ilmoitus vesihuollon merkittävästä häiriöstä tiedoksi maa- ja metsätalousministeriölle, Tieto välittyisi näin tarvittaessa myös valtioneuvoston tilannekuvakeskukseen. Elinkeino-, liikenne- ja ympäristökeskuksen olisi lisäksi arvioitava häiriön mahdolliset vaikutukset toisessa EU:n jäsenvaltiossa ja ilmoitettava häiriöstä tarvittaessa jäsenvaltion asianomaiselle viranomaiselle. Ilmoitus voitaisiin tehdä esimerkiksi silloin, kun häiriö voisi merkittävästi vaikuttaa talousveden jakelun jatkuvuuteen toisessa jäsenvaltiossa.

Pykälän *1 ja 3 momentin* mukaan vesihuoltolaitoksen ja elinkeino-, liikenne- ja ympäristökeskuksen olisi ilmoitettava vesihuollon merkittävistä häiriötilanteista niiden aiheutumisen syystä riippumatta. Ilmoittamisvelvollisuus koskisi siten myös verkko- ja tietoturvadirektiivissä tarkoitettua laitoksen tietojärjestelmiin tai sen käyttämiin viestintäverkkoihin kohdistuvaa merkittävää tietoturvallisuuteen liittyvää häiriötä, jonka seurauksena talousveden jakelu voisi keskeytyä merkittävässä laajuudessa tai talousveden laatuvaatimusten täyttäminen voisi merkittävästi vaarantua. Laitoksen tietojärjestelmiä ja viestintäverkkoja voisivat olla yksityiset viestintäverkot ja tietojärjestelmät, joita hallinnoi palveluntarjoajan oma tietotekninen henkilöstö tai joiden tietoturvahallinto on ulkoistettu. Tietojärjestelmät voivat koostua esimerkiksi tietoyhteiskuntakaaren 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään.

Verkko-ja tietoturvadirektiivin täytäntöönpanon osalta pykälän 3 momentti säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 momentti. Jos kyse olisi direktiivissä tarkoitetusta tietoturvahäiriöstä, elinkeino-, liikenne- ja ympäristökeskus voi pyytää Viestintävirastoa välittämään ilmoituksen toisen jäsenvaltion verkko- ja tietoturvadirektiivin 8 artiklassa tarkoitetulle keskitetylle yhteyspisteelle.

Pykälän *4 momentin* mukaan maa- ja metsätalousministeriö voisi antaa tarkempia säännöksiä siitä, milloin 1 momentissa tarkoitettua vesihuollon häiriötä olisi pidettävä merkittävänä Asetuksella voitaisiin säätää tarkemmin myös 1 momentissa tarkoitettujen ilmoitusten sisällöstä, muodosta ja toimittamisesta.

35 §. *Salassapitovelvollisuus.* Pykälän *2 momenttia* muutettaisiin niin, että lain mukaista tehtävää suorittava saisi luovuttaa salassa pidettäviä tietoja myös Viestintävirastolle silloin, kun se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi. Tällaiset tiedot voisivat sisältää esimerkiksi tietoja sellaisista 15 b §:ssä tarkoitetuista vesihuollon häiriöistä, jotka liittyisivät tietoturvallisuuteen. Ehdotetulla säännöksellä pannaan täytäntöön verkko- ja tietoturvadirektiivin 10 artikla direktiivin liitteen II toimialan 6 osalta.

1.11 Laki finanssivalvonnasta annetun lain muuttamisesta

50 n §. *Toiminta verkko- ja tietoturvadirektiivissä tarkoitettuna toimivaltaisena viranomaisena.* Pykälässä säädettäisiin siitä, että Finanssivalvonta toimii verkko- ja tietoturvadirektiivin 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena direktiivin liitteen II toimialojen 3 ja 4 osalta. Säännös on selkeyttävä, sillä verkko- ja tietoturvadirektiivin mukaisten valvontatehtävien voi katsoa jo kuuluvan Finanssivalvonnan voimassa olevan lainsäädännön mukaisiin tehtäviin.

52 a §.*Yhteistyö ja tietojenvaihto verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa.* Pykälässä säädettäisiin Finanssivalvonnalle velvoite tehdä yhteistyötä viestintäviraston ja muiden tarpeellisten viranomaisten kanssa verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa sekä oikeus vaihtaa salassa pidettävää tietoa tätä tarkoitusta varten. Viestintäviraston lisäksi muita tarpeellisia viranomaisia voisivat olla verkko- ja tietoturvadirektiivin mukaiset toimivaltaiset viranomaiset muilla direktiivin liitteen II mukaisilla toimialoilla (liikenteen osalta Liikenteen turvallisuusvirasto, energian osalta Energiavirasto, terveydenhuollon osalta sosiaali- ja terveysalan lupa- ja valvontavirasto sekä juomavedenjakelun osalta elinkeino-, liikenne- ja ympäristökeskus), muut ministeriöt sekä muiden Euroopan unionin jäsenvaltioiden toimivaltaiset viranomaiset. Tällaiset tiedot voisivat sisältää esimerkiksi tietoja tie-

toturvallisuuteen liittyvistä häiriöistä. Ehdotetulla säännöksellä pannaan täytäntöön verkko- ja tietoturvadirektiivin 10 artikla direktiivin liitteen II toimialojen 3 ja 4 osalta.

2 Voimaantulo

Lait ehdotetaan tulemaan voimaan 1 päivänä toukokuuta 2018.

3 Suhde perustuslakiin ja säätämisjärjestys

Yksityisyyden suoja. Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Saman momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan käytännön mukaan lainsäätäjän liikkuma-alaa rajoittaa tämän säännöksen lisäksi myös se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Esityksellä ei heikennetä yksityisyydensuojaa. Sekä Euroopan ihmisoikeustuomioistuin että Euroopan unionin tuomioistuin ovat Euroopan ihmisoikeussopimuksen 8 artiklaa sekä Euroopan unionin perusoikeuskirjan 7 ja 8 artiklaa koskevassa oikeuskäytännössään katsoneet, että oikeus yksityiselämän kunnioittamiseen henkilötietojen käsittelyssä koskee kaikenlaisia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevia tietoja. Henkilötiedon käsite on laaja ja myös valvontaviranomaiselle tehtävät tietoturvaan liittyviä häiriöitä koskevat ilmoitukset voivat mahdollisesti sisältää joissakin tapauksissa henkilötietoja. Pääsääntöisesti näin ei voida katsoa kuitenkaan olevan. Lisäksi on huomioitava, että yksityiselämän ja henkilötietojen suojan kannalta lähtökohtana on, että oikeushenkilöt eivät kuulu näiden oikeuksien soveltamisalaan. Mikäli häiriöilmoitukset sisältävät henkilötietoja, on näitä käsiteltävä henkilötietojen käsittelyä koskevan lainsäädännön mukaisesti. Henkilötietojen käsittelylle tulee olla henkilötietolain mukainen käsittelyperuste. Henkilötietolain mukaan henkilötietoja saa käsitellä, jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta. Sähköisen viestinnän välitystietoja voidaan käsitellä vain tietoyhteiskuntakaaressa säädetyn mukaisesti.

Valtuudet. Perustuslain 80 §:n 1 momentin mukaan valtioneuvosto voi antaa asetuksia perustuslaissa tai muussa laissa säädetyn valtuuden nojalla. Lailla on kuitenkin säädettävä yksilön oikeuksien ja velvollisuuksien perusteista sekä asioista, jotka perustuslain mukaan muuten kuuluvat lain alaan. Valtuuden säätämiseen laissa on perustuslakivaliokunnan käytännössä kohdistettu vaatimuksia sääntelyn täsmällisyydestä ja tarkkarajaisuudesta (esim. PeVL 33/2004 vp, s. 4—6, PeVL 38/2013 vp, s. 3–4, PeVL 11/2016 vp, s. 2–3, PeVL 26/2017 vp, s. 26–28 PeVL 47/2001 vp , s. 2–3, PeVL).

Perustuslain 80 §:n 2 momentin mukaan muu viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä määrätyistä asioista, jos siihen on sääntelyn kohteeseen liittyviä erityisiä syitä eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella. Valtuuden tulee olla soveltamisalaltaan täsmällisesti rajattu. Lisäksi perustuslaista johtuu, että valtuuden kattamat asiat on määriteltävä tarkasti laissa. Valtuutuksen säätämiseen laissa on perustuslakivaliokunnan lausuntokäytännössä kohdistettu vaatimuksia sääntelyn täsmällisyydestä ja tarkkuudesta 16/2002 vp, s. 2, PeVL 19/2002 vp s. 5, PeVL 1/2004 vp, s. 2 ja PeVL 17/2010 vp, s. 2. Perustuslakiuudistuksen yhteydessä mainittiin esimerkkeinä viranomaisen norminantovallasta tekninen ja vähäisiä yksityiskohtia koskeva sääntely, johon ei liity merkittävää harkintavallan käyttöä (HE 1/1998 vp, s. 133/II; ks. myös PeVL 16/2002 vp, s. 2/I ja PeVL 19/2002 vp, s. 5/I).

Esityksessä ehdotetaan, että valtioneuvoston asetuksella voitaisiin antaa tarkemmat säännökset siitä, milloin lentoasemaa tai satamaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä (ilmailulain muuttamisesta annetun lain 128 §:n 5 momentti ja eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta annetun lain 7 e §:n 6 momentti). Asetuksella täsmennettäisiin sitä, mitä lentoasemia tai satamia olisi pidettävä yhteiskunnan toiminnan kannalta merkittävinä. Perustelujen mukaan arvioidessa sitä, onko toimija yhteiskunnan toiminnan kannalta merkittävä, olisi huomioitava verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaiset kriteerit. Täsmennyksistä säätäminen asetuksen tasolla on perusteltua, koska muutoin sääntely laintasolla muodostuisi tarpeettoman yksityiskohtaiseksi ja tapauksittaiseksi. Asetuksella ei annettaisi yleisiä oikeussääntöjä lain alaan kuuluvista asioista eikä säädettäisi yksilön oikeuksien ja velvollisuuksien perusteista. Asetuksenantovaltuus on myös sijoitettu perustuslakivaliokunnan edellyttämällä tavalla perussäännöksen yhteyteen.

Ehdotetuilla laeilla annettaisiin uusia määräyksenantovaltuuksia seuraavasti: Viestintävirastolle tietoyhteiskuntakaaren muuttamisesta annetun lain 275 §:n 4 momentissa, Liikenteen turvallisuusvirastolle ilmailulain muuttamisesta annetun lain 128 b §:n 4 momentissa, rautatielain muuttamisesta annetun lain 41 a §:n 6 momentissa, alusliikennepalvelulain muuttamisesta annetun lain 18 a §:n 5 momentissa, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta annetun lain 7 f §:n 4 momentissa, liikenteen palveluista annetun lain muuttamisesta annetun lain 7 §:n 6 momentissa, Energiavirastolle sähkömarkkinalain muuttamisesta annetun lain 29 a §:n 5 momentissa ja maakaasumarkkinalain 34 a §:n 4 momentissa sekä asetuksenanto valtuus maa- ja metsätalousministeriölle vesihuoltolain muuttamisesta annetun lain 15 b §:n 3 momentissa.

Valtuutussäännökset on sijoitettu ja asiallisesti kytketty säänneltävää asiaa koskeviin pykäliin. Määräyksissä määriteltäisiin esimerkiksi tietoturvallisuuteen liittyviä häiriöitä koskevien ilmoituksien sisältöön liittyvät muodolliset ja tekniset seikat sekä ilmoitusten tarkempi tekotapa. Valtuudet koskisivat teknisluonteisia ja vähäisiä yksityiskohtia koskevaa sääntelyä, johon ei liity merkittävää harkintavallan käyttöä.

Edellä kerrotuin perustein esityksessä ehdotettavat valtuudet ovat soveltamisalaltaan täsmällisiä ja tarkkarajaisia, eikä niiden katsota olevan ristiriidassa perustuslain kanssa.

Edellä kerrotuilla perusteilla esitetään, että lakiehdotukset voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä.

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

Lakiehdotukset

1.

Laki

tietoyhteiskuntakaaren muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan tietoyhteiskuntakaaren (917/2014) 275 §, 304 §:n 1 momentin 7 ja 10 kohta sekä 313 §:n 2 momentin 2 kohta sekä

lisätään lakiin uusi 247 a §, 308 §:ään, sellaisena kuin se on osaksi laissa 456/2016, uusi 3 momentti sekä 318 §:ään, sellaisena kuin se on osaksi laissa 456/2016, uusi 2 momentti, jolloin nykyinen 2–4 momentti siirtyvät 3–5 momentiksi, seuraavasti:

247 a §

Verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta

Verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Riskienhallinnassa on huomioitava:

1) järjestelmien ja tilojen turvallisuus;
2) tietoturvauhkien ja häiriöiden käsittely;
3) liiketoiminnan jatkuvuuden hallinta;
4) seuranta, tarkastukset ja testaukset;
5) kansainvälisten standardien noudattaminen.

Edellä 1 momentissa tarkoitettu riskienhallintavelvoite ei koske toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun Euroopan parlamentin ja neuvoston direktiivin(EU) 2016/1148, jäljempänä *verkko- ja tietoturvadirektiivi*, 16 artiklan 11 kohdassa tarkoitettuja mikroyrityksiä tai pieniä yrityksiä.

275 §

Häiriöilmoitukset Viestintävirastolle

Teleyrityksen on ilmoitettava viipymättä Viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Teleyrityksen on ilmoitettava myös ilman aiheetonta viivästystä häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään. Viestintävirasto toimittaa komissiolle ja Euroopan unionin verkko- ja tietoturvavirastolle vuosittain tiivistelmäraportin ilmoituksista.

Edellä 247 a §:ssä tarkoitetun verkossa toimivan markkinapaikan tarjoajan, hakukonepalvelun tarjoajan sekä pilvipalvelun tarjoajan on ilmoitettava viipymättä Viestintävirastolle sen palveluun kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.

Jos häiriöistä ilmoittaminen on yleisen edun mukaista, Viestintävirasto voi velvoittaa teleyrityksen tai palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä 1 ja 2 momentissa tarkoitettujen ilmoitusten sisällöstä, muodosta ja toimittamisesta.

Viestintäviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

304 §

Viestintäviraston erityiset tehtävät

Sen lisäksi, mitä muualla tässä laissa säädetään, Viestintäviraston tehtävänä on:

— —

7) kerätä tietoa verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista;

— —

10) selvittää verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvia tietoturvaloukkauksia ja niiden uhkia;

— —

308 §

Yhteistyö eri viranomaisten kanssa

— —

Viestintäviraston on toimittava yhteistyössä muiden Euroopan unionin jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten, tietoturvaloukkauksiin reagoivien yksiköiden sekä verkko- ja tietoturvadirektiivin 11 artiklassa tarkoitetun yhteistyöryhmän kanssa. Viestintävirasto toimittaa yhteistyöryhmälle vuosittain verkko- ja tietoturvadirektiivin 10 artiklan 3 kohdan mukaisen tiivistelmäraportin.

313 §

Valvonta-asioiden käsittely Viestintävirastossa

— —

Viestintävirasto voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen. Viestintävirasto voi jättää asian tutkimatta, jos:

— —

2) asialla on epäillystä virheestä tai laiminlyönnistä huolimatta viestintämarkkinoiden toimivuuden, viestintäpalvelujen luotettavuuden tai sähköisen viestinnän häiriöttömyyden turvaamisen ja palveluja käyttävien edun taikka 247 a §:ssä tarkoitettujen palveluiden riskinhallinnan kannalta vain vähäinen merkitys; tai

— —

318 §

Tietojen luovuttaminen viranomaisesta

— —

Viestintävirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Liikenteen turvallisuusvirastolle, Energiavirastolle, Finanssivalvonnalle, Sosiaali- ja terveysalan lupa- ja valvontavirastolle sekä elinkeino-, liikenne- ja ympäristökeskukselle, jos se on näille säädettyjen tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämätöntä.

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

2.

Laki

ilmailulain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään ilmailulakiin (864/2014) uusi 128 a ja 128 b § seuraavasti:

11 luku

Ilmailuonnettomuudet, ilmailun etsintä- ja pelastuspalvelu, vaaratilanteet ja poikkeamat

128 a §

Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta

Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Liikenteen turvallisuusviraston on arvioitava 1 momentissa tarkoitetun riskienhallinnan vaikutuksia ilmailun turvallisuuteen. Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on annettava Liikenteen turvallisuusvirastolle arvioinnin kannalta tarpeelliset tiedot. Virasto voi velvoittaa lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän ryhtymään korjaaviin toimenpiteisiin ilmailun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi.

Liikenteen turvallisuusvirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa 2 momentissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Valtioneuvoston asetuksella säädetään, milloin lentoasemaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä.

128 b §

Tietoturvapoikkeamista ilmoittaminen

Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä poikkeamasta.

Jos poikkeamasta ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenteen turvallisuusviraston on arvioitava koskeeko 1 momentissa tarkoitettu poikkeama muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu poikkeama on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Tämä laki tulee voimaan päivänä kuuta 20 .

3.

Laki

rautatielain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään rautatielakiin (304/2011) uusi 41 a § seuraavasti:

6 luku

Turvallisuus

41 a §

Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen

Valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.

Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenteen turvallisuusviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteen turvallisuusvirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä pykälässä säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 2 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksensisällöstä, muodosta ja toimittamisesta.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

4.

Laki

alusliikennepalvelulain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään alusliikennepalvelulain (623/2005) 16 §:ään uusi 5 momentti, lakiin uusi 18 a § sekä 28 §:ään, sellaisena kuin se on osaksi laissa (1307/2009), uusi 4 momentti seuraavasti:

16 §

Alusliikennepalvelun ylläpito

— —

VTS-viranomaisen on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

18 a §

Tietoturvaan liittyvistä häiriöistä ilmoittaminen

VTS-viranomaisen on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.

Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenteen turvallisuusviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Liikenteen turvallisuusvirastolla on salassapitosäännösten ja muiden tietojenluovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä pykälässä säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

28 §

Valvonta

— —

Liikenteen turvallisuusviraston on arvioitava 16 §:n 5 momentissa tarkoitetun riskienhallinnan vaikutuksia merenkulun turvallisuuteen. Liikenteen turvallisuusvirasto voi velvoittaa ryhtymään korjaaviin toimenpiteisiin merenkulun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi. Velvoitteen tehosteeksi voidaan asettaa uhkasakko. Uhkasakosta säädetään uhkasakkolaissa (1113/1190).

Tämä laki tulee voimaan päivänä kuuta 20 .

5.

Laki

eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin (485/2004) uusi 7 e ja 7 f § seuraavasti:

2 a luku

Satamien turvatoimet

7 e §

Satamanpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta

Yhteiskunnan toiminnan kannalta merkittävän satamanpitäjä on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Liikenteen turvallisuusviraston on arvioitava 1 momentissa tarkoitetun riskienhallinnan vaikutuksia merenkulun turvallisuuteen. Virasto voi velvoittaa 1 momentissa tarkoitetun satamanpitäjän ryhtymään korjaaviin toimenpiteisiin merenkulun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi. Velvoitteen tehosteeksi voidaan asettaa uhkasakko. Uhkasakosta säädetään uhkasakkolaissa (1113/1190).

Liikenteen turvallisuusvirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa 2 momentissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Valtioneuvoston asetuksella säädetään, milloin 1 momentissa tarkoitettua satamaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä.

7 f §

Tietoturvallisuuteen liittyvistä häiriöistä ilmoittaminen

Yhteiskunnan toiminnan kannalta merkittävän satamanpitäjän on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.

Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenteen turvallisuusviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

6.

Laki

liikenteen palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään liikenteen palveluista annetun lain (320/2017) III osan 2 lukuun uusi 7 § seuraavasti:

7 §

Älykkään liikennejärjestelmän ylläpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen

Älykkään liikennejärjestelmän ylläpitäjän on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Älykkään liikennejärjestelmän ylläpitäjän on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.

Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenteen turvallisuusviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteen turvallisuusvirastolla on salassapitosäännösten tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä pykälässä säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

7.

Laki

sähkömarkkinalain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sähkömarkkinalain (588/2013) 62 §:n 1 momentti, sellaisena kuin se on laissa 590/2017, sekä

lisätään lakiin uusi 29 a § seuraavasti:

29 a §

Verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen

Verkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Verkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena sähkönjakelu voi keskeytyä jakeluverkossa merkittävässä laajuudessa.

Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa palvelun tarjoajan tiedottamaan yleisölle asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Energiaviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille jäsenvaltioille.

Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä] ilmoituksen sisällöstä, muodosta ja toimittamisesta.

62 §

Suljettua jakeluverkkoa koskevat erityissäännökset

Suljettuun jakeluverkkoon ja suljetun jakeluverkonhaltijaan ei sovelleta 23 eikä 26 a §:ää, 27 §:n 3 momenttia, 28, 29, 29 a, 50—53, 53 a, 54—57, 57 a, 58 eikä 59 §:ää.

— —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

8.

Laki

maakaasumarkkinalain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään maakaasumarkkinalakiin (587/2017) uusi 34 a § seuraavasti:

34 a §

Siirtoverkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen

Siirtoverkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Siirtoverkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena maakaasun siirto voi keskeytyä siirtoverkossa merkittävässä laajuudessa.

Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa siirtoverkonhaltijan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Energiaviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille jäsenvaltioille.

Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Tämä laki tulee voimaan päivänä kuuta 20 .

9.

Laki

sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 27 ja 28 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 27 § sekä 28 §:n otsikko, 1 momentin johdantokappale ja 1 kohta sekä 2 ja 3 momentti seuraavasti:

27 §

Viranomaisten valvontayhteistyö

Energiavirastolla on oikeus toimivaltaansa kuuluvissa asioissa tehdä valvontayhteistyötä Finanssivalvonnan, Kilpailu- ja kuluttajaviraston, Viestintäviraston, kuluttaja-asiamiehen, energia-alan sääntelyviranomaisten yhteistyöviraston, toisen ETA-valtion sääntelyviranomaisen ja Euroopan komission kanssa sekä antaa pyynnöstä virka-apua näiden suorittaessa sähkö- tai maakaasualan yritykseen liittyvää valvonta- tai tarkastustehtävää.

28 §

Energiaviraston oikeus luovuttaa tietoja toiselle viranomaiselle

Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Energiavirastolla on oikeus luovuttaa salassapitosäännösten estämättä tietoja:

1) Finanssivalvonnalle, Kilpailu- ja kuluttajavirastolle ja kuluttaja-asiamiehelle niiden tehtävien hoitamista varten sekä Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi;

— —

Energiavirastolla on oikeus luovuttaa vain sellaisia tietoja, jotka ovat tarpeen asianomaisen viranomaisen tehtävien suorittamiseksi, ja jos tietoja luovutetaan ulkomaan viranomaiselle tai kansainväliselle toimielimelle, edellyttäen, että niitä koskee kyseisten tietojen osalta vastaava salassapitovelvollisuus kuin Energiavirastoa.

Energiavirasto ei saa luovuttaa toisen valtion viranomaiselta tai kansainväliseltä toimielimeltä saatuja salassa pidettäviä tietoja edelleen, ellei tiedon antanut viranomainen ole antanut siihen nimenomaista suostumusta. Näitä tietoja voidaan käyttää ainoastaan tämän lain mukaisten tehtävien hoitamiseen tai niihin tarkoituksiin, joita varten suostumus on annettu.

Tämä laki tulee voimaan päivänä kuuta 20 .

10.

Laki

vesihuoltolain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan vesihuoltolain (119/2001) 35 §:n 2 momentti ja
lisätään lakiin uusi 15 b § seuraavasti:

15 b §

Vesihuollon häiriötilanteista ilmoittaminen

Vesihuoltolaitoksen, joka toimittaa vettä tai ottaa vastaan jätevettä vähintään 5 000 kuutiometriä vuorokaudessa, on ilmoitettava viipymättä elinkeino-, liikenne- ja ympäristökeskukselle merkittävästä häiriöstä vesihuollossa. Ilmoituksen saatuaan elinkeino-, liikenne- ja ympäristökeskus voi velvoittaa vesihuoltolaitoksen tiedottamaan asiasta tai vesihuoltolaitosta kuultuaan tiedottaa asiasta itse.

Mitä 1 momentissa säädetään vesihuoltolaitoksesta, koskee myös laitosta, joka toimittaa vettä vesihuoltolaitokselle tai ottaa vastaan jätevettä vesihuoltolaitokselta.

Elinkeino-, liikenne- ja ympäristökeskus toimittaa 1 momentissa tarkoitetun ilmoituksen tiedoksi maa- ja metsätalousministeriölle. Elinkeino-, liikenne- ja ympäristökeskuksen on lisäksi arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltiota, ja ilmoitettava häiriöstä tarvittaessa jäsenvaltion asianomaiselle viranomaiselle.

Maa- ja metsätalousministeriö voi antaa asetuksella tarkempia säännöksiä siitä, milloin 1 momentissa tarkoitettua vesihuollon häiriötä on pidettävä merkittävänä, sekä momentissa tarkoitetun ilmoituksen sisällöstä, muodosta ja toimittamisesta.

35 §

Salassapitovelvollisuus

— —

Viranomaisten toiminnan julkisuudesta annetussa laissa säädetyn salassapitovelvollisuuden estämättä saa tämän lain mukaisia tehtäviä suoritettaessa saatuja tietoja yksityisen tai yhteisön taloudellisesta asemasta, liike- tai ammattisalaisuudesta taikka yksityisen henkilökohtaisista oloista luovuttaa:

1) valvontaviranomaiselle tämän lain mukaisten tehtävien suorittamista varten;
2) rikoksen selvittämiseksi syyttäjä- ja poliisiviranomaiselle;
3) Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

11.

Laki

Finanssivalvonnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään finanssivalvonnasta annettuun lakiin (878/2008) uusi 50 n ja 52 a § seuraavasti:

50 n §

Toiminta verkko- ja tietoturvadirektiivissä tarkoitettuna toimivaltaisena viranomaisena

Finanssivalvonta toimii yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148, jäljempänä *verkko- ja tietoturvadirektiivi*, 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena direktiivin liitteen II toimialojen 3 ja 4 osalta.

52 a §

Yhteistyö ja tietojenvaihto verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa

Finanssivalvonnan on tehtävä yhteistyötä verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa Viestintäviraston ja muiden tarpeellisten viranomaisten kanssa. Finanssivalvonnalla on tätä tarkoitusta varten oikeus salassapitosäännösten estämättä vaihtaa tietoja Viestintäviraston ja muiden tarpeellisten viranomaisten kanssa.

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä 19 päivänä joulukuuta 2017

Pääministeri

Juha Sipilä

Liikenne- ja viestintäministeri Anne Berner

Rinnakkaistekstit

1.

Laki

tietoyhteiskuntakaaren muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan tietoyhteiskuntakaaren (917/2014) 275 §, 304 §:n 1 momentin 7 ja 10 kohta sekä 313 §:n 2 momentin 2 kohta sekä
lisätään lakiin uusi 247 a §, 308 §:ään, sellaisena kuin se on osaksi laissa 456/2016, uusi 3 momentti sekä 318 §:ään, sellaisena kuin se on osaksi laissa 456/2016, uusi 2 momentti, jolloin nykyinen 2–4 momentti siirtyvät 3–5 momentiksi**,** seuraavasti:

Voimassa oleva laki	Ehdotus
	247 a §
uusi	*Verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta*
	Verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Riskienhallinnassa on huomioitava: *1) järjestelmien ja tilojen turvallisuus;* *2) tietoturvauhkien ja häiriöiden käsittely;* *3) liiketoiminnan jatkuvuuden hallinta;* *4) seuranta, tarkastukset ja testaukset;* *5) kansainvälisten standardien noudattaminen.* *Edellä 1 momentissa tarkoitettu riskienhallintavelvoite ei koske toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148, jäljempänä verkko- ja tietoturvadirektiivi, 16 artiklan 11 kohdassa tarkoitettuja mikroyrityksiä tai pieniä yrityksiä.*

275 §

Häiriöilmoitukset Viestintävirastolle

Teleyrityksen on ilmoitettava viipymättä Viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Teleyrityksen on ilmoitettava myös ilman aiheetonta viivästystä häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään. Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Viestintävirasto voi velvoittaa teleyrityksen tiedottamaan asiasta.

Viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä sekä määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Viestintävirasto toimittaa komissiolle ja Euroopan verkko- ja tietoturvavirastolle vuosittain tiivistelmäraportin 1 momentin mukaisista ilmoituksista.

275 §

Häiriöilmoitukset Viestintävirastolle

Teleyrityksen on ilmoitettava viipymättä Viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Teleyrityksen on ilmoitettava myös ilman aiheetonta viivästystä häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään. *Viestintävirasto toimittaa komissiolle ja Euroopan unionin verkko- ja tietoturvavirastolle vuosittain tiivistelmäraportin ilmoituksista.*

Edellä 247 a §:ssä tarkoitetun verkossa toimivan markkinapaikan tarjoajan, hakukonepalvelun tarjoajan sekä pilvipalvelun tarjoajan on ilmoitettava viipymättä Viestintävirastolle *sen palveluun kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.*

Jos häiriöistä ilmoittaminen on yleisen edun mukaista, Viestintävirasto voi velvoittaa teleyrityksen tai palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Viestintävirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä 1 ja 2 momentissa tarkoitettujen ilmoitusten sisällöstä, muodosta ja toimittamisesta.

Viestintäviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

304 §	304 §
Viestintäviraston erityiset tehtävät	*Viestintäviraston erityiset tehtävät*
Sen lisäksi, mitä muualla tässä laissa säädetään, Viestintäviraston tehtävänä on:	Sen lisäksi, mitä muualla tässä laissa säädetään, Viestintäviraston tehtävänä on:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
7) kerätä tietoa verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista;	7) kerätä tietoa verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin *sekä tietojärjestelmiin* kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista;
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
10) selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia;	10) selvittää verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin *sekä tietojärjestelmiin* kohdistuvia tietoturvaloukkauksia ja niiden uhkia;
	308 §
uusi	*Yhteistyö eri viranomaisten kanssa*
	— — — — — — — — — — — — — — — —
	Viestintäviraston on toimittava yhteistyössä muiden Euroopan unionin jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten, tietoturvaloukkauksiin reagoivien yksiköiden sekä verkko- ja tietoturvadirektiivin 11 artiklassa tarkoitetun yhteistyöryhmän kanssa. Viestintävirasto toimittaa yhteistyöryhmälle vuosittain verkko- ja tietoturvadirektiivin 10 artiklan 3 kohdan mukaisen tiivistelmäraportin.
313 §	313 §
Valvonta-asioiden käsittely Viestintävirastossa	*Valvonta-asioiden käsittely Viestintävirastossa*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Viestintävirasto voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen. Viestintävirasto voi jättää asian tutkimatta, jos:	Viestintävirasto voi asettaa tässä laissa säädetyt valvontatehtävänsä tärkeysjärjestykseen. Viestintävirasto voi jättää asian tutkimatta, jos:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

2) asialla on epäillystä virheestä tai laiminlyönnistä huolimatta viestintämarkkinoiden toimivuuden, viestintäpalvelujen luotettavuuden tai sähköisen viestinnän häiriöttömyyden turvaamisen ja palveluja käyttävien edun kannalta vain vähäinen merkitys; tai	2) asialla on epäillystä virheestä tai laiminlyönnistä huolimatta viestintämarkkinoiden toimivuuden, viestintäpalvelujen luotettavuuden tai sähköisen viestinnän häiriöttömyyden turvaamisen ja palveluja käyttävien edun *taikka 247 a §:ssä tarkoitettujen palveluiden riskinhallinnan kannalta* vain vähäinen merkitys; tai
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	318 §
	Tietojen luovuttaminen viranomaisesta
	— — — — — — — — — — — — — — — —
uusi	*Viestintävirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Liikenteen turvallisuusvirastolle, Energiavirastolle, Finanssivalvonnalle, Sosiaali- ja terveysalan lupa- ja valvontavirastolle sekä elinkeino-, liikenne- ja ympäristökeskukselle, jos se on näille säädettyjen tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämätöntä.*
	— — — — — — — — — — — — — — — —
	————
	Tämä laki tulee voimaan päivänä kuuta 20 ————

2.

Laki

ilmailulain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään ilmailulakiin (864/2014) uusi 128 a ja 128 b § seuraavasti:

Voimassa oleva laki	Ehdotus
	11 luku
	Ilmailuonnettomuudet, ilmailun etsintä- ja pelastuspalvelu, vaaratilanteet ja poikkeamat
	128 a §
uusi	*Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta*
	Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.
	Liikenteen turvallisuusviraston on arvioitava 1 momentissa tarkoitetun riskienhallinnan vaikutuksia ilmailun turvallisuuteen. Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on annettava Liikenteen turvallisuusvirastolle arvioinnin kannalta tarpeelliset tiedot. Virasto voi velvoittaa lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän ryhtymään korjaaviin toimenpiteisiin ilmailun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi.
	Liikenteen turvallisuusvirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oike-

us luovuttaa 2 momentissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Valtioneuvoston asetuksella säädetään, milloin lentoasemaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä.

128 b §

Tietoturvapoikkeamista ilmoittaminen

uusi

Lennonvarmistuspalvelun tarjoajan sekä yhteiskunnan toiminnan kannalta merkittävän lentoaseman pitäjän on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä poikkeamasta.

Jos poikkeamasta ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenteen turvallisuusviraston on arvioitava koskeeko 1 momentissa tarkoitettu poikkeama muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu poikkeama on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

———

Tämä laki tulee voimaan päivänä kuuta 20

———

3.

Laki

rautatielain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään rautatielakiin (304/2011) uusi 41 a § seuraavasti:

Voimassa oleva laki	Ehdotus
	6 luku
	Turvallisuus
	41 a §
uusi	*Velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen*
	Valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.
	Valtion rataverkon haltijan sekä liikenteenohjauspalvelun tarjoajan on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.
	Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.
	Liikenteen turvallisuusviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.
	Liikenteen turvallisuusvirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä pykälässä säädettyjen teh-

täviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 2 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksensisällöstä, muodosta ja toimittamisesta.

Tämä laki tulee voimaan päivänä kuuta 20

4.

Laki

alusliikennepalvelulain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään alusliikennepalvelulain (623/2005) 16 §:ään uusi 5 momentti, lakiin uusi 18 a § sekä 28 §:ään, sellaisena kuin se on osaksi laissa (1307/2009), uusi 4 momentti seuraavasti:

Voimassaoleva laki	Ehdotus
	16 §
	Alusliikennepalvelun ylläpito
uusi	— — — — — — — — — — — — — — —
	VTS-viranomaisen on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.
	18 a §
	Tietoturvaan liittyvistä häiriöistä ilmoittaminen
uusi	*VTS-viranomaisen on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.*
	Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.
	Liikenteen turvallisuusviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.
	Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.
	Liikenteen turvallisuusvirastolla on salas-

sapitosäännösten ja muiden tietojenluovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä pykälässä säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

28 §

Valvonta

— — — — — — — — — — — — — — — —

uusi

Liikenteen turvallisuusviraston on arvioitava 16 §:n 5 momentissa tarkoitetun riskienhallinnan vaikutuksia merenkulun turvallisuuteen. Liikenteen turvallisuusvirasto voi velvoittaa ryhtymään korjaaviin toimenpiteisiin merenkulun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi. Velvoitteen tehosteeksi voidaan asettaa uhkasakko. Uhkasakosta säädetään uhkasakkolaissa (1113/1190).

———

Tämä laki tulee voimaan päivänä kuuta 20

———

5.

Laki

eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin (485/2004) uusi 7 e ja 7 f § seuraavasti:

Voimassa oleva laki	Ehdotus
	2 a luku
	Satamien turvatoimet
	7 e §
uusi	*Satamanpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta*
	Yhteiskunnan toiminnan kannalta merkittävän satamanpitäjä on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.
	Liikenteen turvallisuusviraston on arvioitava 1 momentissa tarkoitetun riskienhallinnan vaikutuksia merenkulun turvallisuuteen. Virasto voi velvoittaa 1 momentissa tarkoitetun satamanpitäjän ryhtymään korjaaviin toimenpiteisiin merenkulun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi. Velvoitteen tehosteeksi voidaan asettaa uhkasakko. Uhkasakosta säädetään uhkasakkolaissa (1113/1190).
	Liikenteen turvallisuusvirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa 2 momentissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Valtioneuvoston asetuksella säädetään, milloin 1 momentissa tarkoitettua satamaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä.

7 f §

Tietoturvallisuuteen liittyvistä häiriöistä ilmoittaminen

uusi

Yhteiskunnan toiminnan kannalta merkittävän satamanpitäjän on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.

Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

Liikenteen turvallisuusviraston on arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Tämä laki tulee voimaan päivänä kuuta 20

6.

Laki

liikenteen palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään liikenteen palveluista annetun lain (320/2017) III osan 2 lukuun uusi 7 § seuraavasti:

Voimassa oleva laki	Ehdotus
	7 §
uusi	*Älykkään liikennejärjestelmän ylläpitäjän velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen*
	Älykkään liikennejärjestelmän ylläpitäjän on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. *Älykkään liikennejärjestelmän ylläpitäjän on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä.* *Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Liikenteen turvallisuusvirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.* *Liikenteen turvallisuusviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.* *Liikenteen turvallisuusvirastolla on salassapitosäännösten tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä pykälässä säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Viestintävirastolle, jos se on*

välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

Liikenteen turvallisuusvirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Tämä laki tulee voimaan päivänä kuuta 20

7.

Laki

sähkömarkkinalain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan sähkömarkkinalain (588/2013) 62 §:n 1 momentti, sellaisena kuin se on laissa 590/2017, sekä
lisätään lakiin uusi 29 a § seuraavasti:

Voimassa oleva laki	Ehdotus
	29 a §
	Verkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen
	Verkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.
	Verkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena sähkönjakelu voi keskeytyä jakeluverkossa merkittävässä laajuudessa.
	Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa palvelun tarjoajan tiedottamaan yleisölle asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.
	Energiaviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille jäsenvaltioille.
	Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä] ilmoituksen sisällöstä, muodosta ja toimittamisesta.
	Mitä 1 ja 2 momentissa säädetään, ei sovelleta suurjännitteisen jakeluverkon haltijaan, jonka sähköverkkoon ei ole liitetty jakeluverkkoa.

62 §	62 §
Suljettua jakeluverkkoa koskevat erityissäännökset	*Suljettua jakeluverkkoa koskevat erityissäännökset*
Suljettuun jakeluverkkoon ja suljetun jakeluverkon haltijaan ei sovelleta 23 eikä 26 a §:ää, 27 §:n 3 momenttia, 28, 29, 50–53, 53 a, 54–57, 57a, 58 eikä 59 §:ää.	Suljettuun jakeluverkkoon ja suljetun jakeluverkonhaltijaan ei sovelleta 23 eikä 26 a §:ää, 27 §:n 3 momenttia, 28, 29, *29 a,* 50—53, 53 a, 54—57, 57 a, 58 eikä 59 §:ää.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
	Tämä laki tulee voimaan päivänä kuuta 20

8.

Laki

maakaasumarkkinalain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään maakaasumarkkinalakiin (587/2017) uusi 34 a § seuraavasti:

Voimassa oleva laki	Ehdotus
	34 a §
uusi	*Siirtoverkonhaltijan velvollisuus huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta ja tietoturvallisuuteen liittyvästä häiriöstä ilmoittaminen*
	Siirtoverkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. *Siirtoverkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen käyttämiin viestintäverkkoihin tai tietojärjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena maakaasun siirto voi keskeytyä siirtoverkossa merkittävässä laajuudessa.* *Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa siirtoverkonhaltijan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.* *Energiaviraston on arvioitava, koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltioita ja ilmoitettava tarvittaessa muille jäsenvaltioille.* *Energiavirasto voi antaa tarkempia määräyksiä siitä, milloin 1 momentissa tarkoitettu häiriö on merkittävä, sekä ilmoituksen sisällöstä, muodosta ja toimittamisesta.*
	————
	Tämä laki tulee voimaan päivänä kuuta 20
	————

9.

Laki

sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 27 ja 28 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 27 § sekä 28 §:n otsikko, 1 momentin johdantokappale ja 1 kohta sekä 2 ja 3 momentti seuraavasti:

Voimassa oleva laki	Ehdotus
27 §	27 §
Viranomaisten valvontayhteistyö	*Viranomaisten valvontayhteistyö*
Energiamarkkinavirastolla on oikeus toimivaltaansa kuuluvissa asioissa tehdä valvontayhteistyötä Finanssivalvonnan, Kilpailu- ja kuluttajaviraston, kuluttaja-asiamiehen, energia-alan sääntelyviranomaisten yhteistyöviraston, toisen ETA-valtion sääntelyviranomaisen ja Euroopan komission kanssa sekä antaa pyynnöstä virka-apua näiden suorittaessa sähkö- tai maakaasualan yritykseen liittyvää valvonta- tai tarkastustehtävää.	*Energiavirastolla* on oikeus toimivaltaansa kuuluvissa asioissa tehdä valvontayhteistyötä Finanssivalvonnan, Kilpailu- ja kuluttajaviraston, *Viestintäviraston,* kuluttaja-asiamiehen, energia-alan sääntelyviranomaisten yhteistyöviraston, toisen ETA-valtion sääntelyviranomaisen ja Euroopan komission kanssa sekä antaa pyynnöstä virka-apua näiden suorittaessa sähkö- tai maakaasualan yritykseen liittyvää valvonta- tai tarkastustehtävää.
28 §	28 §
Energiamarkkinaviraston oikeus luovuttaa tietoja toiselle viranomaiselle	***Energiaviraston** oikeus luovuttaa tietoja toiselle viranomaiselle*
Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Energiamarkkinavirastolla on oikeus luovuttaa salassapitosäännösten estämättä tietoja: 1) Finanssivalvonnalle, Kilpailu- ja kuluttajavirastolle sekä kuluttaja-asiamiehelle niiden tehtävien hoitamista varten;	Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, *Energiavirastolla* on oikeus luovuttaa salassapitosäännösten estämättä tietoja: 1) Finanssivalvonnalle, Kilpailu- ja kuluttajavirastolle ja kuluttaja-asiamiehelle niiden tehtävien hoitamista varten *sekä Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi*;
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Energiamarkkinavirastolla on oikeus luovuttaa vain sellaisia tietoja, jotka ovat tarpeen asianomaisen viranomaisen tehtävien suorittamiseksi, ja jos tietoja luovutetaan ulkomaan	*Energiavirastolla* on oikeus luovuttaa vain sellaisia tietoja, jotka ovat tarpeen asianomaisen viranomaisen tehtävien suorittamiseksi, ja jos tietoja luovutetaan ulkomaan vi-

viranomaiselle tai kansainväliselle toimielimelle, edellyttäen että niitä koskee kyseisten tietojen osalta vastaava salassapitovelvollisuus kuin Energiamarkkinavirastoa.

Energiamarkkinavirasto ei saa luovuttaa toisen valtion viranomaiselta tai kansainväliseltä toimielimeltä saatuja salassa pidettäviä tietoja edelleen, ellei tiedon antanut viranomainen ole antanut siihen nimenomaista suostumusta. Näitä tietoja voidaan käyttää ainoastaan tämän lain mukaisten tehtävien hoitamiseen tai niihin tarkoituksiin, joita varten suostumus on annettu.

ranomaiselle tai kansainväliselle toimielimelle, edellyttäen, että niitä koskee kyseisten tietojen osalta vastaava salassapitovelvollisuus kuin *Energiavirastoa.*

Energiavirasto ei saa luovuttaa toisen valtion viranomaiselta tai kansainväliseltä toimielimeltä saatuja salassa pidettäviä tietoja edelleen, ellei tiedon antanut viranomainen ole antanut siihen nimenomaista suostumusta. Näitä tietoja voidaan käyttää ainoastaan tämän lain mukaisten tehtävien hoitamiseen tai niihin tarkoituksiin, joita varten suostumus on annettu.

Tämä laki tulee voimaan päivänä kuuta 20

10.

Laki

vesihuoltolain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan vesihuoltolain (119/2001) 35 §:n 2 momentti ja
lisätään lakiin uusi 15 b § seuraavasti:

Voimassa oleva laki	Ehdotus
	15 b §
	Vesihuollon häiriötilanteista ilmoittaminen
uusi	*Vesihuoltolaitoksen, joka toimittaa vettä tai ottaa vastaan jätevettä vähintään 5 000 kuutiometriä vuorokaudessa, on ilmoitettava viipymättä elinkeino-, liikenne- ja ympäristökeskukselle merkittävästä häiriöstä vesihuollossa. Ilmoituksen saatuaan elinkeino-, liikenne- ja ympäristökeskus voi velvoittaa vesihuoltolaitoksen tiedottamaan asiasta tai vesihuoltolaitosta kuultuaan tiedottaa asiasta itse.* *Mitä 1 momentissa säädetään vesihuoltolaitoksesta, koskee myös laitosta, joka toimittaa vettä vesihuoltolaitokselle tai ottaa vastaan jätevettä vesihuoltolaitokselta.* *Elinkeino-, liikenne- ja ympäristökeskus toimittaa 1 momentissa tarkoitetun ilmoituksen tiedoksi maa- ja metsätalousministeriölle. Elinkeino-, liikenne- ja ympäristökeskuksen on lisäksi arvioitava, koskeeko 1 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltiota, ja ilmoitettava häiriöstä tarvittaessa jäsenvaltion asianomaiselle viranomaiselle.* *Maa- ja metsätalousministeriö voi antaa asetuksella tarkempia säännöksiä siitä, milloin 1 momentissa tarkoitettua vesihuollon häiriötä on pidettävä merkittävänä, sekä momentissa tarkoitetun ilmoituksen sisällöstä, muodosta ja toimittamisesta.*

35 §	35 §
Salassapitovelvollisuus	*Salassapitovelvollisuus*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Viranomaisten toiminnan julkisuudesta annetussa laissa säädetyn salassapitovelvollisuuden estämättä saa tämän lain mukaisia tehtäviä suoritettaessa saatuja tietoja yksityisen tai yhteisön taloudellisesta asemasta, liike- tai ammattisalaisuudesta taikka yksityisen henkilökohtaisista oloista luovuttaa:	Viranomaisten toiminnan julkisuudesta annetussa laissa säädetyn salassapitovelvollisuuden estämättä saa tämän lain mukaisia tehtäviä suoritettaessa saatuja tietoja yksityisen tai yhteisön taloudellisesta asemasta, liike- tai ammattisalaisuudesta taikka yksityisen henkilökohtaisista oloista luovuttaa:
1) valvontaviranomaiselle tämän lain mukaisten tehtävien suorittamista varten;	1) valvontaviranomaiselle tämän lain mukaisten tehtävien suorittamista varten;
2) rikoksen selvittämiseksi syyttäjä- ja poliisiviranomaiselle;	2) rikoksen selvittämiseksi syyttäjä- ja poliisiviranomaiselle;
	3) Viestintävirastolle, jos se on välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.
	————
	Tämä laki tulee voimaan päivänä kuuta 20
	————

11.

Laki

Finanssivalvonnasta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään finanssivalvonnasta annettuun lakiin (878/2008) uusi 50 n ja 52 a § seuraavasti:

Voimassa oleva laki	Ehdotus
	50 n §
	Toiminta verkko- ja tietoturvadirektiivissä tarkoitettuna toimivaltaisena viranomaisena
uusi	*Finanssivalvonta toimii yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/1148, jäljempänä verkko- ja tietoturvadirektiivi, 8 artiklan 1 kohdassa tarkoitettuna toimivaltaisena viranomaisena direktiivin liitteen II toimialojen 3 ja 4 osalta.*
	52 a §
	Yhteistyö ja tietojenvaihto verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa
uusi	*Finanssivalvonnan on tehtävä yhteistyötä verkko- ja tietoturvadirektiivin mukaisten tehtävien hoitamisessa Viestintäviraston ja muiden tarpeellisten viranomaisten kanssa. Finanssivalvonnalla on tätä tarkoitusta varten oikeus salassapitosäännösten estämättä vaihtaa tietoja Viestintäviraston ja muiden tarpeellisten viranomaisten kanssa.*
	————
	Tämä laki tulee voimaan päivänä kuuta 20
	————