**HALLITUKSEN ESITYS EDUSKUNNALLE LAEIKSI EUROOPAN UNIONIN VERKKO- JA TIETOTURVADIREKTIIVIN TÄYTÄNTÖÖNPANOON LIITTYVIEN LAKIEN MUUTTAMISESTA**

**ESITYKSEN PÄÄASIALLINEN SISÄLTÖ**

Juha Sipilän hallituksen hallitusohjelman keskeisenä tavoitteena edistetään digitalisaatiota. Hallitusohjelman mukaan Suomen tavoitteena on ottaa tuottavuusloikka julkisissa palveluissa ja yksityisellä sektorilla tarttumalla digitalisaation mahdollisuuksiin. Digitaalisille palveluille ja uusille liiketoimintamalleille rakennetaan hallitusohjelman mukaan suotuisa toimintaympäristö. Osana tätä digitaalisen liiketoiminnan kasvuympäristön rakentamisen kärkihanketta edistetään uuden teknologian, digitalisaation ja uusien liiketoimintakonseptien käyttöönottoa lainsäädäntötoimin sekä varmistetaan tietoturva ja sen kilpailuetua kasvattavat mahdollisuudet.

Hallituksen toimintasuunnitelman mukaan hallituksen tavoitteena on parantaa sisäisen turvallisuuden edellyttämiä suorituskykyjä myös digitaalisen turvallisuuden alueella, koska digitaalinen yhteiskunta edellyttää, että turvallisuuden digitaalinen ulottuvuus on korkealla tasolla.

Tällä hallituksen 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.

Esityksessä ehdotetaan tietyille yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajille sekä eräiden digitaalisten palveluiden tarjoajille tietoturvariskienhallintaan ja tietoturvapoikkeamaraportointiin liittyviä velvoitteita. Lisäksi säädettäisiin näiden velvoitteiden valvonnasta, viranomaisten välisestä tietojen vaihdosta sekä yleisestä tietoturvallisuuteen liittyvästä viranomaistoiminnasta.

Yhteiskunnan toiminnan kannalta keskeisten palvelujen tietoturvallisuuden parantamiseksi tietoyhteiskuntakaareen (917/2014), ilmailulakiin (864/2014), rautatielakiin (304/2011), alusliikennepalvelulakiin (623/2005), eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annettuun lakiin (485/2004), liikenteenpalveluista annettuun lakiin (320/2017), sähkömarkkinalakiin (588/2013), maakaasumarkkinalakiin (xx) sekä vesihuoltolakiin (119/2001) lisättäisiin säännökset keskeisten palveluntarjoajien velvollisuudesta huolehtia viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä ilmoittaa merkittävistä 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 keskeisen 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 keskeisen sataman pitäjää. Sähkömarkkinalain velvoitteet koskisivat verkonhaltijaa. Maakaasumarkkinalain velvoitteet koskisivat siirtoverkonhaltijaa ja vesihuoltolain velvoitteet vesihuoltolaitosta, joka toimittaa vettä vähintään 5000 kuutiometriä vuorokaudessa.

Eri toimialojen toiminnan turvallisuuteen liittyvien velvoitteiden kokonaisvaltaisen ohjauksen ja valvonnan turvaamiseksi sekä päällekkäisten valvontatoimivaltojen ja hallinnollisen taakan välttämiseksi toimivalta valvoa riskienhallinta- ja poikkeamaraportointivelvoitteiden toteutumista olisi sektorikohtaisilla valvontaviranomaisilla. Tämä tarkoittaisi Viestintävirastoa, Liikenteen turvallisuusvirastoa, Energiavirastoa, Finanssivalvontaa sekä Sosiaali- ja terveysalan lupa- ja valvontavirastoa. Viranomaisten välisen yhteistyön turvaamiseksi ehdotettaisiin viranomaisten toimivaltuuksia koskevan lainsäädännön yhteyteen lisättäväksi säännökset valvovien viranomaisten yhteistyöstä sekä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi merkittävien salassa pidettävien tietojen vaihdosta.

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

Ehdotetulla lainsäädännöllä saatettaisiin osaksi kansallista lainsäädäntöä Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

SISÄLLYS

[YLEISPERUSTELUT 5](#_Toc490814473)

[1 Johdanto 5](#_Toc490814474)

[2 Nykytila 8](#_Toc490814475)

[2.1. Lainsäädäntö ja käytäntö 8](#_Toc490814476)

[2.2. Kansainvälinen kehitys sekä ulkomaiden ja EU:n lainsäädäntö 30](#_Toc490814477)

[2.3. Nykytilan arviointi 38](#_Toc490814478)

[3 Esityksen tavoitteet ja keskeiset ehdotukset 49](#_Toc490814479)

[3.1. Tavoitteet 49](#_Toc490814480)

[3.2. Toteuttamisvaihtoehdot 50](#_Toc490814481)

[3.3. Keskeiset ehdotukset 52](#_Toc490814482)

[4 Esityksen vaikutukset 53](#_Toc490814483)

[4.1. Taloudelliset vaikutukset 53](#_Toc490814484)

[4.2. Vaikutukset viranomaisen toimintaan 53](#_Toc490814485)

[4.3. Yhteiskunnalliset vaikutukset 53](#_Toc490814486)

[5 Asian valmistelu 53](#_Toc490814487)

[5.1. Valmisteluvaiheet ja -aineisto 53](#_Toc490814488)

[5.2. Lausunnot ja niiden huomioon ottaminen 54](#_Toc490814489)

[6 Riippuvuus muista esityksistä 54](#_Toc490814490)

[6.1. Esityksen suhde Ahvenanmaan itsehallintoon 55](#_Toc490814491)

[YKSITYISKOHTAISET PERUSTELUT 56](#_Toc490814492)

[1 Lakiehdotusten perustelut 56](#_Toc490814493)

[1.1. Laki tietoyhteiskuntakaaren muuttamisesta 56](#_Toc490814494)

[1.1. Laki ilmailulain muuttamisesta 58](#_Toc490814495)

[1.2. Laki rautatielain muuttamisesta 59](#_Toc490814496)

[1.3. Laki alusliikennepalvelulain muuttamisesta 60](#_Toc490814497)

[1.4. Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta 61](#_Toc490814498)

[1.5. Laki liikenteenpalveluista annetun lain muuttamisesta 61](#_Toc490814499)

[1.6. Laki sähkömarkkinalain muuttamisesta 62](#_Toc490814500)

[1.7. Laki maakaasumarkkinalain muuttamisesta 62](#_Toc490814501)

[1.8. Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta 63](#_Toc490814502)

[1.9. Laki vesihuoltolain muuttamisesta 63](#_Toc490814503)

[2 Voimaantulo 63](#_Toc490814504)

[3 Suhde perustuslakiin ja säätämisjärjestys 64](#_Toc490814505)

[LAKIEHDOTUKSET 66](#_Toc490814506)

# YLEISPERUSTELUT

## 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 kiristyshaittaohjelma -tapausten seurauksena yhä keskeisemmin esille. Haittaohjelmat ovat vaikeuttaneet esimerkiksi rautatiejärjestelmien, satamien, sairaaloiden sekä energiayhtiöiden toimintaa 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 Eurobarometri-tutkimuksen 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 syy-yhteyksien 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 huomioiden 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 hyväksyttiin 6 päivänä heinäkuuta 2015 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (jäljempänä verkko- ja tietoturvadirektiivi). Verkko- ja tietoturvadirektiivi on saatettava kansallisesti voimaan 9 päivänä toukokuuta 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.

## Nykytila

### Lainsäädäntö ja käytäntö

###### Yleistä

Tietoturvallisuutta koskevaa lainsäädäntöä ei ole Suomessa koottu yhteen lakiin vaan sitä sisältyy useisiin niin julkista hallintoa kuin erilaisten palveluiden tarjontaa koskeviin säädöksiin. Tietoturvariskienhallintaan liittyviä velvoitteita sisältyy hallinnon yleislakeihin (viranomaisten toiminnan julkisuudesta annettua laki, henkilötietolaki), yleiseen palveluntarjoajien turvallisuusvelvoitteita koskevaan lainsäädäntöön (esimerkiksi 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.

###### 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 liittyvässä 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 päivänä huhtikuuta 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.

###### 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 16 päivänä joulukuuta 2010 periaatepäätöksen yhteiskunnan turvallisuusstrategiaksi ja määritteli strategiassa yhteiskunnan elintärkeät toiminnot. Strategian mukaan suomalaisen yhteiskunnan elintärkeitä toimintoja ovat: valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky sekä henkinen kriisinkestävyys.

Strategian mukaan infrastruktuurin ylläpitämisellä tarkoitetaan niitä teknisiä rakenteita ja organisaatioita, jotka ovat välttämättömiä väestön elinmahdollisuuksille ja yhteiskunnan toimivuudelle. Tähän kokonaisuuteen kuuluvat julkisen talouden toimintaedellytysten, rahoitusmarkkinoiden ja vakuutusalan toiminnan turvaaminen, elintarvikehuollon toimintakyvyn turvaaminen, sähköisten tieto- ja viestintäjärjestelmien sekä kuljetusten turvaaminen, yhteiskunnan taloudellisten perustoimintojen ylläpitäminen, osaava työvoima, korkeatasoisen koulutus- ja tutkimusjärjestelmän ylläpitäminen sekä merkittävien ympäristömuutosten havaitseminen, rajoittaminen ja niihin sopeutuminen.

Lisäksi Valtioneuvosto on antanut huoltovarmuudesta annetun lain (1390/1992) 2 §:n mukaisesti päätöksen maan huoltovarmuuden tavoitteista 5 päivänä joulukuuta 2013 (VNp 857/2013). 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.

###### Yhteiskunnan toiminnan kannalta keskeisten 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.

**Digitaalinen infrastruktuuri**

Digitaalisen infrastruktuurin osalta verkko- ja tietoturvadirektiivissä ei ole määritelty tarkempia toiminnan osa-alueita, mutta toimijoiden tyyppeinä on mainittu internetin yhdysliikennepisteet (Internet exchange point, IXP), nimipalvelujen tarjoajat sekä aluetunnusrekisterit (direktiivin liite II). 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. Kyseisen 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 kohdistuvat 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 yhdysliikennepisteet 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 (621/1999) sekä sen nojalla annetun valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (tietoturva-asetus) (681/2010) 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 maakaasumarkkinalakiin 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. Maakaasumarkkinalain 3 luvun 1 §:n mukaan Maakaasumarkkinaviranomainen määrää maakaasuverkkoluvassa yhden siirtoverkonhaltijan vastaamaan muun muassa maakaasun siirtojärjestelmän teknisestä toimivuudesta ja käyttövarmuudesta (järjestelmävastuu). Järjestelmävastuussa oleva siirtoverkonhaltija voi asettaa järjestelmävastuun toteuttamiseksi tarpeellisia ehtoja maakaasun siirtojärjestelmän käyttämiselle.

*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 niin kutsutun EASA-asetuksen (Euroopan parlamentin ja neuvoston asetus yhteisistä siviili-ilmailua koskevista säännöistä ja Euroopan lentoturvallisuusviraston perustamisesta sekä neuvoston direktiivin 91/670/ETY, asetuksen (EY) N:o 1592/2002 ja direktiivin 2004/36/EY kumoamisesta ((EY) N:o 216/2008)) 8 artiklassa, asetuksen liitteissä IV (8 artiklassa tarkoitetut lentotoimintaa koskevat keskeiset vaatimukset) V a (lentopaikkoja 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 ja lennonvarmistuspalveluja sekä lennonjohtoa.

Euroopan parlamentin ja neuvoston niin kutsutussa poikkeama-asetuksessa (Euroopan parlamentin ja neuvoston asetus (EU) N:o 376/2014 poikkeamien ilmoittamisesta, analysoinnista ja seurannasta siviili-ilmailun alalla) 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. Ilmailulakiin sisältyy kuitenkin vain muutamia turvallisuuteen liittyviä vaatimuksia liittyen esimerkiksi lentokelpoisuuden ylläpitämiseen (33 ja 34 §), lentoaseman hyväksymistodistukseen (83 §), maahuolintapalvelujen tarjoamiseen (93 §) sekä varautumisessa 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 Euroopan parlamentin ja Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/798 rautateiden turvallisuudesta, komission asetus (EU) N:o 1078/2012 rautatieyritysten, turvallisuustodistuksen tai turvallisuusluvan saaneiden infrastruktuurin haltijoiden sekä kunnossapidosta vastaavien yksiköiden soveltamasta omavalvontaa koskevasta yhteisestä turvallisuusmenetelmästä sekä Komission asetus (EU) N:o 1077/2012 yhteisestä turvallisuusmenetelmästä kansallisten turvallisuusviranomaisten turvallisuustodistuksen tai turvallisuusluvan myöntämisen jälkeen harjoittamaa valvontaa varten. Kansallisesti rautateiden turvallisuudesta on säädetty rautatielailla, valtioneuvoston asetuksella ja Liikenteen turvallisuusvirastonmääräyksellä.

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 mukaanrautatieliikenteen 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 yleisesti on yhtiöiden (varustamot) osalta kansainvälisessä turvallisuusjohtamissäännöstössä (International Safety Management Code, ISM-säännöstö), joka perustuu SOLAS-yleissopimukseen. EU:n alueella säännöstö on toimeenpantu asetuksella (EY) N:o 336/2006 (Euroopan parlamentin ja neuvoston asetus (EY) N:o 336/2006

kansainvälisen turvallisuusjohtamissäännöstön täytäntöönpanosta yhteisössä ja neuvoston asetuksen (EY) N:o 3051/95 kumoamisesta) . 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. Alusturvallisuuden valvonnasta annetun lain (370/1995) 20 §:n mukaan valvontaviranomaiselle on tehtävä, mikäli mahdollista, kirjallinen ilmoitus alusturvallisuutta koskevan säännöksen tai määräyksen rikkomisesta.

Alusliikennepalvelu

Alusliikennepalvelulaissa 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 niin kutsutulla turvatoimiasetuksella (Euroopan parlamentin ja neuvoston asetus (EY) N:o 725/2004 alusten ja satamarakenteiden turvatoimien parantamisesta). Kansallisesti eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetussa laissasäädetään 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(ELY) -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. Lain III osan 2 luvun 6 §:ssä säädetään älykkäiden liikennejärjestelmien käyttöönotosta. Pykälän 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. Asetus mm. velvoittaa jäsenvaltiot nimeämään Euroopan laajuisen tieverkon osuudet, joilla on liikenne- ja turvallisuusolosuhteiden vuoksi otettava käyttöön liikenneturvallisuuteen liittyvä yleinen vähimmäistason liikennetietopalvelu.

**Pankkiala ja finanssimarkkinoiden infrastruktuuri**

Pankkialan ja finanssimarkkinoiden infrastruktuuria ei ole verkko- ja tietoturvadirektiivin liitteessä II jaettu tarkempiin osa-alueihin. 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. Näitä järjestelmiä koskevat vaatimukset, jotka ovat usein tiukempia kuin verkko- ja tietoturvadirektiivin nojalla säädetyt vaatimukset, on vahvistettu useissa unionin säädöksissä sekä kansallisessa lainsäädännössä. Velvoitteisiin sisältyy mm. säännöt oikeudesta harjoittaa luottolaitostoimintaa sekä luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta ja säännöt luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvaatimuksista, säännöt rahoitusvälineiden markkinoista, säännöt OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä, ja säännöt arvopaperikaupan selvitysjärjestelmän parantamisesta unionissa sekä arvopaperikeskuksista. Lisäksi poikkeamien ilmoittamista koskevat vaatimukset ovat osa rahoitusalan tavanomaista valvontakäytäntöä, ja ne sisältyvät usein valvontaohjeisiin.

*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 myös 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.

*Maksulaitokset*

Maksulaitoksien osalta maksulaitoslain (297/2010) 3 luvun 19 § sisältää velvoitteet toiminnan ja riskienhallinnan järjestämisestä sekä Finanssivalvonnan määräyksenantovaltuuden tarkempien määräysten antamisesta. Ulkoistamisesta annetut säännökset ovat 23§:ssä ja varautumisvelvollisuuteen liittyvät säännökset 41 a §:ssä. Myös maksulaitoksia velvoittaa Finanssivalvonnan määräys operatiivisen riskin hallinnasta rahoitussektorin valvottavissa sekä sen 6 luvun määräykset tietojärjestelmien tietoturvallisuudesta ja 9 luvun määräykset raportoinnista Finanssivalvonnalle.

*Säännelty markkina, monenkeskinen kaupankäyntijärjestelmä, organisoitu kaupankäyntijärjestelmä, sekä pörssi*

Säännellyn markkinan ylläpitäjän yleistä riskienhallintaa koskevaa sääntelyä on mm. laissa kaupankäynnistä rahoitusvälineillä (2 luku 17§). Samassa laissa on säädetty myös ulkoistamisen edellytyksistä (2 luku 19§). Finanssivalvonnalla on oikeus antaa tarkempia määräyksiä ja ohjeita (2 luku 44§) ja Finanssivalvonnanoperatiivisten riskien hallintaa koskevat määräykset ja ohjeet koskevat osittain myös pörssiä. Pörssiä velvoittaa operatiivista riskienhallintaa koskeva määräyksen 8/2014 6 luvun määräykset tietojärjestelmien tietoturvallisuudesta. Sen sijaan 9 luvun määräykset raportoinnista Finanssivalvonnalle koskevat pörssiä ainoastaan suosituksina. Ulkoistamista koskevat Finanssivalvonnan antamat määräykset ja ohjeet velvoittavat myös pörssiä. Pohjoismaissa toimivan Nasdaq-pörssin toimintaa on koordinoitu niin, että riskienhallintaa koskeva raportointi tehdään kaikille pohjoismaisille valvojille yhteisesti sovittujen kriteerien mukaisesti.

*Arvopaperikeskus*

Arvopaperikeskuksien osalta Euroopan parlamentin ja neuvoston asetus (EU) N:o 909/2014 arvopaperitoimituksen parantamisesta Euroopan unionissa sekä arvopaperikeskuksista ja direktiivien 98/26/EY ja 2014/65/EU sekä asetuksen (EU) N:o 236/2012 muuttamisesta (I-tason asetus) sisältää säännöksiä ulkoistamisesta ja operatiivisten riskien hallinnasta. Se velvoittaa myös raportoimaan operatiivisista toimintaan liittyvistä poikkeamista toimivaltaiselle viranomaiselle. II-tason asetus on edelleen valmisteluvaiheessa unionissa.. Asetus tulee todennäköisesti sisältämään tarkempaa sääntelyä mm. yleisesti riskienhallinnan järjestämisestä ja operatiivisista riskeistä sekä erityissäännöksiä muun muassa tietojärjestelmistä ja jatkuvuussuunnittelusta. Finanssivalvonnan operatiivista riskienhallintaa koskevan määräyksen (8/2014) 9 luvun määräykset raportoinnista Finanssivalvonnalle koskevat arvopaperikeskusta ainoastaan suosituksina.

**Terveydenhuoltoala**

Terveydenhuollon osalta 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 arkistointijärjestelmä 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.

Lain5 a luvussaon säädettysosiaali- 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 vaarantumiseen 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 tavoitteena on turvata sellainen vesihuolto, että kohtuullisin kustannuksin on saatavissa riittävästi moitteetonta talousvettä. 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. 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.

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 ryhtyä suunnitelman perusteella tarvittaviin toimenpiteisiin. Laitoksen tulee toimittaa suunnitelma valvonta- ja pelastusviranomaiselle ja kunnalle.

Talousveden turvallisuutta koskevat laatuvaatimukset perustuvat EU:n direktiiviin ihmisten käyttöön tarkoitetun veden laadusta (Euroopan parlamentin ja neuvoston direktiivi 2000/60/EY, annettu 23. päivänä lokakuuta 2000, yhteisön vesipolitiikan puitteista). Kansallisesti talousveden laatuvaatimuksista on säädetty terveydensuojelulain 17 §:ssä sekä laadun valvonnasta lain 20 §:ssä.

Sosiaali- ja terveysministeriö on antanut lain 20 §:n mukaan asetuksen talousveden laatuvaatimuksista ja valvontatutkimuksista (1352/2015). Asetuksessa säädetään talousveden laatuvaatimuksista ja -suosituksista ja niiden enimmäisarvoista sekä niistä poikkeamisesta. Asetuksessa säädetään lisäksi talousveden desinfioinnista ja säännöllisestä valvonnasta, valvontaa varten tarvittavista tutkimuksista, talousveden radioaktiivisista aineista aiheutuvan säteilyaltistuksen rajoittamisesta sekä erityistilanteisiin varautumista koskevien suunnitelmien sisällöstä ja laatimisesta.

###### 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. Suomen huoltovarmuuden kannalta kriittisiä toimialoja ovat tietoyhteiskuntasektorin lisäksi energiahuolto, rahoitushuolto, kuljetuslogistiikka, terveydenhuolto, elintarvikehuolto ja kriittinen teollisuustuotanto. Kaikkien näiden alojen toimivuus on eri tavoin riippuvainen tieto- ja viestintäjärjestelmien häiriöttömästä toiminnasta.

Kaikkein vakavimpien yhteiskunnan kriisien varalle on säädetty 1 päivänä maaliskuuta 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.

###### Muu keskeisten palvelujen tietoturvallisuuden sekä jatkuvuuden 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 Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (henkilötietodirektiivi). Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) korvaa henkilötietodirektiivin 25.5.2018 lähtien. Asetus on Suomessa suoraan sovellettava. Yleisen tietosuoja-asetuksen 32 artiklassa säädetään henkilötietojen käsittelyn turvallisuudesta. 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 teknisesti 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

###### 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 1 päivänä heinäkuuta 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.

*Onnettomuustutkintakeskus OTKES*

Turvallisuustutkintalaki (525/2011) määrittelee Onnettomuustutkintakeskuksen tehtävät ja toimivallan. Onnettomuustutkintakeskuksen tehtävänä on tutkia kaikki suuronnettomuudet ja suuronnettomuuden vaaratilanteet riippumatta niiden laadusta sekä ilmailu-, raideliikenne- ja vesiliikenneonnettomuudet ja niiden vaaratilanteet.

Onnettomuustutkintakeskus huolehtii turvallisuustutkinnan yleisestä järjestämisestä, suunnittelusta, ohjauksesta, tiedottamisesta ja valvonnasta, kouluttaa tutkijoiksi soveltuvia henkilöitä, pitää yllä valmiutta tutkinnan nopeaan käynnistämiseen, huolehtii turvallisuustutkinnan alaan liittyvästä kansainvälisestä yhteistyöstä sekä antaa turvallisuussuosituksia ja seuraa niiden toteutumista.

*Viestintävirasto*

Viestintäviraston tehtävät ja erityiset tehtävät on määritelty tietoyhteiskuntakaaressa ja eräissä muissa laeissa. Tietoyhteiskuntakaaren mukaan Viestintäviraston erityisiin tehtäviin kuuluu mm. 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 EU:n 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 tämän lain nojalla asetettujen säännösten ja määräysten noudattamista. Alusliikennepalvelulain 18 §:ssä säädetään VTS-viranomaisen velvollisuudesta ilmoittaa liikenteen turvallisuusvirastolle tietyistä merenkulun turvallisuuteen liittyvistä olennaisista seikoista ja luotsauslain [(940/2003)](http://www.finlex.fi/fi/laki/ajantasa/2003/20030940) 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 Euroopan komission antama asetus (EU) N:o 1077/2012 kansallisen viranomaisen suorittamasta valvonnasta turvallisuusluvan tai -todistuksen myöntämisen jälkeen.

Lisäksi Liikenteen turvallisuusvirasto valvoo tieverkon haltijoiden tieturvallisuusdirektiivin 2008/96/EY mukaisten johtamis- ja turvallisuudenhallintajärjestelmien toimivuutta ja infrastruktuurin hoitoa.

*Liikennevirasto*

Liikennevirastotoimii alusliikennepalvelulaissa tarkoitettuna VTS-viranomaisena. VTS-viranomaisen tehtävät on määritelty alusliikennepalvelulaissa. VTS-viranomaisen on esimerkiksi ilmoitettava 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.

*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*

Energiavirasto tehtävistä on säädetty sähkö- ja maakaasumarkkinoiden valvonnasta annetussa laissa (590/2013). Lain 2 §:n lakia sovelletaan niiden valvonta- ja seurantatehtävien hoitamiseen, jotka säädetään Energiaviraston tehtäviksi: mm. 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.

Energiaviraston virkamiehellä on lisäksi oikeus laissa tarkoitetun valvontatehtävän toteuttamiseksi toimittaa tarkastus valvottavaa toimintaa harjoittavan elinkeinonharjoittajan hallinnassa olevissa tiloissa. Tarkastusta toimittavalle virkamiehelle ja Energiaviraston valtuuttamalle muulle henkilölle on järjestettävä pääsy elinkeinonharjoittajan hallinnassa oleviin tiloihin sekä niihin sähkö- tai maakaasulaitteisiin ja -laitteistoihin, joilla voi olla merkitystä tässä laissa tarkoitettujen valvontatehtävien hoitamisessa. Tarkastusta toimittavalla virkamiehellä on oikeus tutkia elinkeinonharjoittajan asiakirjat ja data, joilla voi olla merkitystä tässä laissa tarkoitettujen valvontatehtävien hoitamisessa, ja ottaa niistä jäljennöksiä maksutta. Tarkastuksessa on noudatettava, mitä hallintolain (434/2003) 39 §:ssä säädetään.

Energiavirastolla on oikeus valvontatehtävän hoitamiseksi kutsua kuultavaksi elinkeinonharjoittajan edustaja, jos se on välttämätöntä tutkinnan kohteeseen liittyvien tietojen keräämistä varten. Kuulemiseen sovelletaan, mitä hallintolaissa säädetään asian suullisesta käsittelystä.

*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 terveydensuojeluviranomainen ja kunnan ympäristönsuojeluviranomainen.

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.

Lainsäädännössä laitokset on jaoteltu suuriin ja pieniin laitoksiin. Suuria laitoksia ovat ne, jotka toimittavat vettä vähintään 10 m3 päivässä tai vähintään 50 henkilön tarpeisiin. Kaikkein suurimpien talousvettä toimittavien laitosten – sellaisten, jotka toimittavat vettä vähintään 1000 m3 päivässä taikka vähintään 5000 käyttäjälle – veden laatutiedot toimitetaan Euroopan komissiolle.

Kuntien terveydensuojeluviranomaisten pitää toimittaa tällaisten laitosten valvontatutkimustulokset aluehallintoviranomaisille. 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. Muita ohjaukseen osallistuvia viranomaisia ovat sosiaali- ja terveysministeriö ja Terveyden ja hyvinvoinnin laitos.

*Viranomaisten välinen yhteistyö ja tiedonvaihto*

Verkko- ja tietoturvadirektiivi velvoittaa tietoturvallisuudesta vastaavien viranomaisten 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. Salassa pidettäviä tietoja voi kuitenkin luovuttaa mainittuja tehtäviä varten myös silloin, kun salassa pidettävien tietojen poistaminen niiden suuren määrän tai muun niihin verrattavan syyn vuoksi ei ilmeisesti ole tarkoituksenmukaista. 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.

*Hallinnolliset seuraamukset*

Hallintolain 67 §:n mukaan viranomainen voi tehostaa antamaansa kieltoa, velvoitetta tai vaatimusta uhkasakolla, teettämisuhalla taikka keskeyttämisuhalla tai muulla hallinnollisella seuraamuksella siten kuin erikseen säädetään.

[täydennetään]

### Kansainvälinen kehitys sekä ulkomaiden ja EU:n lainsäädäntö

###### EU:n lainsäädäntö

**Verkko- ja tietoturvadirektiivi**

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 samalla ehdotuksen verkko- ja tietoturvadirektiiviksi.

Direktiivin 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 keskeisille palveluntarjoajille sekä tietyille digitaalisten palveluiden tarjoajille.

Direktiivillä 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.

**Viranomaistehtävien määrittely**

Direktiivillä 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.

**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. Jäsen valtiot voivat antaa tämän tehtävän olemassa olevalle viranomaiselle tai olemassa oleville viranomaisille. 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 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 ei pitäisi saada suoraan ilmoituksia poikkeamista, elleivät ne toimi myös toimivaltaisena viranomaisena tai CSIRT-toimijana. Toimivaltaisen viranomaisen tai CSIRT-toimijan olisi kuitenkin voitava antaa keskitetylle yhteyspisteelle tehtäväksi toimittaa poikkeamia koskevia ilmoituksia muiden asiaan liittyvien jäsenvaltioiden keskitetyille yhteyspisteille. 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 myös 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:

1. poikkeamien seuranta kansallisella tasolla;
2. ennakkovaroitusten, varoitusten, ja tiedotusten antaminen sekä tiedon levittäminen riskeistä ja poikkeamista asiaankuuluville sidosryhmille;
3. poikkeamiin reagointi;
4. dynaamisen riskin ja poikkeamien analysointi sekä tilannetietoisuus;
5. 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. Palveluntarjoajat voidaan velvoittaa tekemään poikkeamailmoituksia myös CSIRT-toimijalle. CSIRT-toimija voidaan perustaa toimivaltaisen viranomaisen yhteyteen.

**EU-tason yhteistyö**

Lisäksi direktiivissä 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 palveluntarjoajien määritteleminen**

Jäsenvaltiot velvoitetaan määrittämään 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)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr1-L_2016194FI.01002701-E0001) 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)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr2-L_2016194FI.01002701-E0002) 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)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr3-L_2016194FI.01002701-E0003) 3 artiklan 4 kohdassa |

 |
|

|  |  |
| --- | --- |
| — | Lentoaseman pitäjät, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2009/12/EY[(4)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr4-L_2016194FI.01002701-E0004) 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)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr5-L_2016194FI.01002701-E0005) 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)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr6-L_2016194FI.01002701-E0006) 2 artiklan 1 kohdassa |

 |
|

|  |  |
| --- | --- |
| b) | Rautatieliikenne |

 |

|  |  |
| --- | --- |
| — | Rataverkon haltijat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2012/34/EU[(7)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr7-L_2016194FI.01002701-E0007) 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)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr8-L_2016194FI.01002701-E0008) liitteessä I, lukuun ottamatta noiden yhtiöiden liikennöimiä yksittäisiä aluksia |

 |
|

|  |  |
| --- | --- |
| — | Euroopan parlamentin ja neuvoston direktiivin 2005/65/EY[(9)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr9-L_2016194FI.01002701-E0009) 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)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr10-L_2016194FI.01002701-E0010) 3 artiklan o alakohdassa määriteltyjen alusliikennepalvelujen tarjoajat |

 |
|

|  |  |
| --- | --- |
| d) | Tieliikenne |

 |

|  |  |
| --- | --- |
| — | Tieviranomaiset, sellaisina kuin ne määritellään komission delegoidun asetuksen (EU) 2015/962[(11)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr11-L_2016194FI.01002701-E0011) 2 artiklan 12 kohdassa, jotka vastaavat liikenteenhallinnasta |

 |
|

|  |  |
| --- | --- |
| — | Euroopan parlamentin ja neuvoston direktiivin 2010/40/EU[(12)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr12-L_2016194FI.01002701-E0012) 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)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr13-L_2016194FI.01002701-E0013) 4 artiklan 1 kohdassa |
|

|  |  |
| --- | --- |
| 4. | Finanssimarkkinoiden infrastruktuurit |

 |   |

|  |  |
| --- | --- |
| — | Euroopan parlamentin ja neuvoston direktiivin 2014/65/EU[(14)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr14-L_2016194FI.01002701-E0014) 4 artiklan 24 kohdassa määriteltyjen kauppapaikkojen ylläpitäjät |

 |
|

|  |  |
| --- | --- |
| — | Keskusvastapuolet, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012[(15)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr15-L_2016194FI.01002701-E0015) 2 artiklan 1 kohdassa |

 |
|

|  |  |
| --- | --- |
| 5. | Terveydenhuoltoala |

 | Terveydenhuoltolaitokset (mukaan lukien sairaalat ja yksityisklinikat) | Terveydenhuollon tarjoajat, sellaisina kuin ne määritellään Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU[(16)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr16-L_2016194FI.01002701-E0016) 3 artiklan g alakohdassa |
|

|  |  |
| --- | --- |
| 6. | Juomaveden toimittaminen ja jakelu |

 |   | Neuvoston direktiivin 98/83/EY[(17)](http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=FI#ntr17-L_2016194FI.01002701-E0017) 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 ja/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. Luetteloa on käytettävä viitekohtana määritettäessä keskeisten palvelujen tarjoajia. Luettelon tarkoituksena on määrittää direktiivissä tarkoitettujen toimialojen keskeisten palvelujen tyypit erottaen ne näin muista kuin keskeisistä toiminnoista, joista tietyn toimialan toimija saattaa olla vastuussa.

Jäsenvaltion on myös määriteltävä, mihin toimijoihin sovelletaan verkko- ja tietojärjestelmien turvallisuutta koskevia velvollisuuksia. Direktiivin mukaan tämä voitaisiin tehdä esimerkiksi hyväksymällä luettelo, jossa luetellaan kaikki keskeisten palvelujen tarjoajat tai hyväksymällä toimenpiteitä, joiden avulla palvelun tarjoajat voitaisiin määrittää.

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.”[[1]](#footnote-1)*

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.

**Turvallisuusriskienhallintavelvoitteet**

*Keskeiset palveluntarjoajat*

Direktiivin mukaan keskeiset palvelun tarjoajat tulee kansallisilla säädöksillä velvoittaa tekemään riskienhallintatoimenpiteitä ja ilmoittamaan poikkeamista viranomaiselle. Direktiivin mukaan jäsenvaltioiden on huolehdittava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset ja oikeasuhtaiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä keskeisten palvelujen tarjoajat käyttävät toiminnoissaan. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen. 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 tekniset ja organisatoriset toimenpiteet 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 ne verkko- ja tietojärjestelmiensä ylläpidosta sisäisesti vai ulkoistavatko ne sen.

*Digitaalisten palveluiden tarjoajat*

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. Koska keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien välillä on perustavanlaatuisia eroja, kun otetaan huomioon erityisesti edellisten suora yhteys fyysiseen infrastruktuuriin ja jälkimmäisten rajat ylittävä luonne, on tarve yhdenmukaisille säännöille keskeisempää digitaalisten palveluntarjoajien osalta.

Keskeisten palvelujen tarjoajien osalta jäsenvaltioiden olisi voitava määrittää asiaankuuluvat palvelujen tarjoajat ja määrätä vaatimuksia, jotka ovat tiukempia kuin tässä direktiivissä säädetyt. Sen sijaan digitaalisen palvelun tarjoajia ei olisi määritettävä, koska direktiiviä on 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 viivytystä toimivaltaiselle viranomaiselle tai CSIRT-toimijalle poikkeamista, joilla on merkittävä vaikutus niiden tarjoamien keskeisten palvelujen jatkuvuuteen. Poikkeamalla tarkoitetaan direktiivissä mitä tahansa tapahtumaa, joka tosiasiassa vaikuttaa haitallisesti verkko- ja tietojärjestelmien turvallisuuteen. Ilmoituksiin on sisällytettävä tiedot, joiden perusteella toimivaltainen viranomainen tai CSIRT-toimija voi määrittää poikkeaman mahdollisen rajat ylittävän vaikutuksen. Ilmoittaminen ei lisää ilmoituksen tekevän osapuolen vastuuta.

Lisäksi jäsenvaltioiden tulee velvoittaa digitaalisten palveluiden tarjoajat ilmoittamaan kansallisille viranomaisille kaikista poikkeamista, joilla on merkittävä vaikutus sellaisen 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. Direktiivin 16 artiklassa on määritelty tarkemmin miten on arvioitava, onko poikkeamalla merkittävä vaikutus.

###### Kansainvälinen kehitys

Tietoturvallisuus on useissa valtioissa ja kansainvälisessä yhteistyössä nostettu viime vuosina keskeisempään poliittiseen asemaan. Kyberturvallisuusstrategioita on laadittu esimerkiksi lähes kaikissa EU-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 (Bundesnetzagentur). 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 yleistä 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 implementointia koskevan lakiehdotuksensa 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. Poikkeamien ilmoittamisesta Ruotsin suojelupoliisille tai puolustusvoimille säädettäisiin erikseen. Lisäksi MSB:lle ehdotetaan verkko- ja tietoturvadirektiivin mukaisen keskitetyn 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 valtion 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/hankkeeseen sekä suojata kriittistä infrastruktuuria ja tutkia voimassa olevan sääntelyn käyttö kyberturvallisuuden edistämiseksi.

### Nykytilan arviointi

###### 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 implementoidaan verkko- ja tietoturvadirektiivin 7 artikla.

###### 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. Viestintäviraston toiminta täyttävät jo käytännössä nykyisellään direktiivin artiklassa 9 ja direktiivin liitteessä I luetellut 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, yhteistyön 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/CERT-toimijoihin.

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

Valtioneuvoston ohjesäännön 12 §:n 7 kohdan mukaan valtioneuvoston kanslian toimialaan kuuluu valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus sekä häiriötilanteiden hallinnan yleinen yhteensovittaminen. Tämän johdosta olisi mahdollista, että keskitettynä yhteyspisteenä voisi toimia valtioneuvoston tilannekuvakeskus.

Keskitetyn yhteyspisteen toiminnan voi kuitenkin katsoa olevan läheisellä tavoin sidoksissa direktiivissä tarkoitettuun operatiivisen tason toimintaan, erityisesti CSIRT-toimintaan. Yhteyspisteen tarkoitus on tukea jäsenvaltioiden viranomaisten, CSIRT-toimijoiden sekä direktiivillä perustettujen jäsenvaltioiden välisen yhteistyöryhmän ja CSIRT-verkoston toimintaa. Tämän johdosta keskitetyn yhteyspisteen olisi tarkoituksenmukaista toimia CSIRT-toimijan yhteydessä Viestintävirastossa.

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

###### 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 ja/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.

Direktiivin johdanto-osan mukaan keskeisten palveluiden tarjoajat voidaan määritellä hyväksymällä luettelo keskeisistä palvelun 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.

Verkko- ja tietoturvadirektiivin mukaan keskeisten palvelun tarjoajien on tarjottava palvelua, joka on yhteiskunnan toiminnan kannalta keskeistä. 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.

Lisäksi direktiivin mukaan keskeisen palvelun on oltava riippuvaista verkko- ja tietojärjestelmistä. Riippuvaisuus liittyy läheisesti siihen, miten palvelun tarjoaminen on järjestetty. Lähtökohtaisesti voidaan olettaa, että suuri osa palveluista on nykyään tavalla tai toisella riippuvaisia verkko- ja tietojärjestelmien käytöstä.

Direktiivissä säädetään myös, että palveluun kohdistuvalla poikkeamalla tulisi myös olla merkittäviä haitallisia vaikutuksia palvelun tarjoamiseen. 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 toimiala- ja palvelukohtaisesti.

Liikenne- ja viestintäministeriö asetti työryhmän tukemaan verkko- ja tietoturvadirektiivin kansallisessa täytäntöönpanossa. Työryhmä on esittänyt loppuraportissaan, että direktiivin mukaiset keskeisten palveluiden tarjoajat määriteltäisiin lain tasolla. Toimialakohtainen keskeisten palvelun tarjoajien määrittäminen perustuu toimivaltaisten ministeriöiden tekemään analyysiin.

**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 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 katsottava olevan aina keskeistä palvelua sen asiakkaille riippumatta sähkönjakeluverkon koosta.

Sähkönjakelu on riippuvaista verkko- ja tietojärjestelmistä. Sähkönjakeluun kohdistuvalla poikkeamalla voisi olla myös merkittäviä haitallisia vaikutuksia sähkönjakeluun, sillä sähkönjakelun jatkuvuus on välttämätöntä yhteiskunnan kriittisten toimintojen ylläpitämiseksi ja yhteiskunnan toiminnan kannalta keskeisten palveluiden järjestämiseksi. Sähkönjakeluun liittyvällä häiriöllä voi olla merkittäviä vaikutuksia jakeluverkon koosta riippumatta.

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.

Sähkönjakelun osalta keskeisiä palveluita voidaan katsoa olevan

1. siirtopalvelu kantaverkossa ja järjestelmävastaavan kantaverkonhaltijan tarjoamat järjestelmäpalvelut
2. sähkönjakelu jakeluverkossa, ei kuitenkaan sähkönjakelu suljetussa jakeluverkossa
3. sähkönjakelu suurjännitteisessä jakeluverkossa, johon on liitetty jakeluverkko, ei kuitenkaan sähkönjakelu suljetussa jakeluverkossa

Keskeisinä palveluntarjoajina voitaisiin siis sähkön osa-alueella pitää järjestelmävastaavaa kantaverkonhaltijaa ja mahdollisia muita kantaverkonhaltijoita, kaikkia jakeluverkonhaltijoita niiden koosta riippumatta sekä sellaisia suurjännitteisen jakeluverkon haltijoita, joiden verkkoon on liitetty jakeluverkkoa pois lukien kuitenkin suljetut jakeluverkot.

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.

Kaasun osa-alueella keskeisiä palveluita Suomessa ovat maakaasumarkkinalain mukainen siirtopalvelu siirtoverkossa ja järjestelmävastaavan siirtoverkonhaltijan tarjoamat järjestelmäpalvelut. Maakaasun osalta keskeisten palveluiden tarjoajina voitaisiin siis pitää järjestelmävastaavaa siirtoverkonhaltijaa ja mahdollisia muita siirtoverkonhaltijoita.

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

**Liikenne**

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

*Liikenteenohjaus*

Liikenteenohjaus on liikennejärjestelmän toimivuuden kannalta keskeistä ja vaikuttaa välittömästi koko liikennejärjestelmän turvallisuuteen. Häiriöt liikenteenohjauksessa voisivat johtaa välittömästi liikenneturvallisuuden vaarantumiseen taikka liikenteen keskeytymiseen.

Liikenteenohjauksen rooli tieliikenteen osalta eroaa vaikutuksiltaan osittain muista liikennemuodoista. Liikennettä ohjataan merkittävissä määrin liikennesäännöillä ja sellaisilla liikenteenohjauslaitteilla, jotka eivät ole riippuvaisia verkko- ja tietojärjestelmistä (tiemerkinnät, liikennemerkit).

Liikenteenohjauksen merkitys tullee tulevaisuudessa edelleen korostumaan liikenteen älykkään automaation yleistyessä. Liikenteenohjaus on myös merkittävällä tavalla riippuvaista verkko- ja tietojärjestelmistä. Lisäksi liikenteenohjaustoiminnot ovat keskitetysti riippuvaista pienestä joukosta toimijoita. Liikenteenohjauspalveluita olisikin pidettävä keskeisinä palveluina ilmailun, rautatieliikenteen ja vesiliikenteen osalta.

­­ *Lentoliikenne*

Ilmailun osalta keskeisinä palveluina voitaisiin pitää liikenteenohjauksen osalta lennonvarmistuspalveluita. 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), joka on aloittanut toimintansa 1 päivänä huhtikuuta 2017, ja se on korvannut Finavia Oyj:n lennonvarmistusliiketoiminnan. 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.

*Rautatieliikenne*

Rautatieliikenteen osalta keskeisenä palveluna voitaisiin pitää liikenteen ohjausta. Rautatielain 36 §:n mukaan rataverkonhaltija vastaa hallinnoimansa rataverkon liikenteenohjauksesta ja huolehtii liikenteenohjauspalvelun tasapuolisuudesta. Rataverkon haltija voi järjestää liikenteenohjauspalvelut itse tai hankkia ne julkisilta tai yksityisiltä palvelujen tuottajilta. Keskeisten palveluiden tarjoajina voitaisiin pitää rataverkonhaltijoiden lisäksi liikenteenohjauspalveluita tarjoavia yrityksiä.

Liikenneviraston rautatieliikenteen ohjausyksikkö (rataliikennekeskus) vastaa rautatieliikenteen ohjauksen operatiivisen toiminnan valvonnasta ja koordinoinnista. Itse operatiivinen rautatieliikenteen ohjaus on ostettu Finrail Oy:ltä.

*Vesiliikenne*

Vesiliikenteenohjauksen osalta keskeisenä palveluna voitaisiin pitää alusliikennepalvelua. Alusliikennepalvelulain mukaan alusliikennepalvelulla (Vessel Traffic Service, VTS) tarkoitetaan alusliikenteen valvontaa ja ohjausta, jolla on valmiudet toimia vuorovaikutuksessa liikenteen kanssa ja reagoida muuttuviin liikennetilanteisiin. Lain mukaan VTS-viranomaisella tarkoitetaan Liikennevirastoa.

*Keskeisen liikenneinfrastruktuurin ylläpitäminen*

Useiden liikennepalvelujen tarjoaminen on riippuvaista keskeisestä liikenneinfrastruktuurista (lentoasemat, satamat, rautatiet, tieverkosto) eikä liikennepalveluja ole usein välttämättä mahdollista tarjota vaihtoehtoisella tavalla, mikäli keskeinen infrastruktuuri olisi poissa käytöstä.

Lentoliikenteen alueella keskeisenä palveluna voitaisiin pitää lentoasemien keskeisten toimintojen hallintaa. Lentoaseman pitäjät vastaavat lentoasemien hallinnasta.

 *Lentoasemat*

Lentoasemat ovat Suomessa merkittävässä asemassa matkustajaliikenteessä ja lentomatkustajien määrä kasvaa. 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. Helsinki-Vantaan osuus sekä lentomatkustajista sekä tavaraliikenteestä on ylivoimaisesti suurin.

Lentoaseman pitäjiä Suomessa ovat Finavia Oyj, Mikkelin kaupunki sekä Seinäjoen lentoasema Oy.

Suomen ulkomaankaupan kuljetuksia oli vuonna 2014 noin 109 miljoonaa tonnia. Tästä merikuljetuksia oli 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.

 *Satamat*

Suomessa on 72 kansainvälistä liikennettä välittävää satamapaikkaa, joiden koko ja toiminta vaihtelee. Kymmenen suurinta satamaa käsittelee noin 80 prosenttia merikuljetusten kokonaisvolyymista. Suomen suurimmat satamat tavaramäärällä mitattuna ovat Kilpilahti (Sköldvik), HaminaKotka ja Helsinki. Tärkeimmät vientisatamat ovat HaminaKotka (metsäteollisuus, kemikaalit ja transito), Sköldvik (öljysatama), Kokkola (malmit ja rikasteet), Helsinki (yleissatama) ja Rauma (metsäteollisuus). Tuonnissa merkittävimmät ovat Sköldvik (öljysatama), Helsinki, HaminaKotka, Raahe (terästeollisuus) ja Naantali (öljysatama).

Eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain mukaan satamanpitäjällä tarkoitetaan sitä, joka ylläpitää satamaa tai satamarakennetta.

Kaikkia lentoaseman tai satamien pitäjiä ei olisi kuitenkaan pidettävä suoraan verkko- ja tietoturvadirektiivin tarkoittamina keskeisten palveluiden tarjoajina. Velvoitteiden kohdistamista tulisi etenkin arvioida verkko- ja tietoturvadirektiivin 6 artiklan kriteerien valossa. Velvoitteiden kohdistaminen verkko- ja tietoturvadirektiivin tarkoittamiin keskeisten palveluiden tarjoajiin voitaisiin tehdä valtioneuvoston asetuksella.

*Rautatiet*

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. Rautatiet ovat näin keskeisiä niin henkilö- kuin tavarakuljetuksessa.

Valtion rataverkonhaltijalla tarkoitetaan rautatielain mukaan Liikennevirastoa. Myös yksityisraide voi mahdollisesti olla merkittävä yhteiskunnan toiminnan kannalta, mikäli se johtaa esimerkiksi teollisuuden kannalta merkittävälle alueelle. Kaikki yksityisraiteet eivät kuitenkaan ole samalla tavoin keskeisiä. Lainsäädännön tasolla voisi olla vaikeaa tai mahdotonta määritellä, mitkä yksityisraiteet olisivat keskeisimpiä. Tästä johtuen keskeisten palvelun tarjoajina tulisi pitää vain valtion rataverkon haltijaa.

 *Tieliikenne*

Tieliikenteen alueella infrastuktuurin osalta keskeisenä verkko- ja tietojärjestelmistä riippuvaisina palveluina voitaisiin pitää ITS-järjestelmien ylläpitäjiä. Fyysisen tieverkon ylläpitämistä ei voida direktiivin tarkoittamalla tavalla pitää riippuvaisena verkko- ja tietojärjestelmistä sillä tavoin, että tähän palveluun kohdistuvilla poikkeamilla olisi verkko- ja tietoturvadirektiivissä tarkoitettuja merkittäviä haitallisia vaikutuksia palvelun tarjoamiseen.

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 voitanee 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. Aineisto mahdollistaa erilaisten reitinsuunnittelu-, navigointi-, matkailu- ja liikennetelemaattisten palveluiden kehittämisen ja tuotteistamisen.

Digitraffic on Liikenneviraston palvelu, jonka kautta on saatavissa ajantasaista liikennetietoa Suomen tieverkolta ja rautatieliikenteestä. Digitraffic käsitti aluksi vain tieliikenteen liikenne- ja olosuhdetietoja. Nykyisin palvelu tarjoaa myös rautatieliikenteen ja vesiliikenteen tietoja.

*Liikennepalvelut*

Liikenteen osalta liikennepalveluiden tarjoaminen (lentoliikenteen harjoittajat, varustamot, rautatieliikenteen harjoittajat) ei oleva vastaavalla tavalla keskeistä. Liikennepalveluissa on usein kilpailevaa tarjontaa sekä vaihtoehtoisia tapoja järjestää palvelu. Joidenkin liikennemuotojen osalta kotimaisten palveluiden tarjoaminen on kuitenkin keskittynyt käytännössä vain yhdelle toimijalle (lentoliikenne ja raideliikenne). Tästä huolimatta on liikenteen palvelujen kansainvälisen luonteen kannalta katsottava, että liikennepalvelujen tarjoajien osalta tietoturvallisuutta voidaan tulevaisuudessa kehittää kohdennetummin ja harmonisoidummin osana kulkumuotokohtaisten kansainvälisten sopimusvelvoitteiden ja EU-säädösten valmistelua. Näin voitaisiin välttää erilaisesta kansallisesta sääntelystä mahdollisesti aiheutuvat kilpailuedellytyksiin kohdistuvat häiriöt.

**Pankkiala ja finanssimarkkinoiden infrastruktuurit**

Pankkialan ja finanssimarkkinoiden infrastruktuurin osalta ei verkko- ja tietoturvadirektiivin liitteessä ole määritelty osa-alueita.

Useat rahoitusalan yritykset tuottavat yhteiskunnan elintärkeiden toimintojen kannalta kriittisiä palveluita, joiden toiminnan jatkuvuuden turvaaminen on tärkeää kaikissa olosuhteissa. Yhteiskunnan toiminnan kannalta keskeisinä toimintoina olisi pidettävä luottolaitoslain mukaista luottolaitostoimintaa, maksulaitoslain mukaista maksupalvelun tarjontaa, arvo-osuusjärjestelmästä ja selvitystoiminnasta annetun lain mukaisten arvopaperikeskuksen tehtävien hoitamista sekä kaupankäynnistä rahoitusvälineillä annetun lain mukaisen pörssitoiminnan harjoittamista. Näiden kaikkien palveluiden tarjoaminen on riippuvaista verkko- ja tietojärjestelmistä.

**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.

Terveydenhuollon palvelut on monin osin verkko- ja tietojärjestelmistä riippuvaista. Yhteiskunnan kannalta merkittävimmät haitalliset vaikutukset voisivat olla sellaisiin järjestelmiin kohdistuvilla tietoturvallisuuteen liittyvillä häiriöillä, joissa käsitellään potilaiden asiakastietoja tai jotka sisältyvät terveydenhuollossa käytettäviin laitteisiin.

**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. Verkko- ja tietoturvadirektiivin 5 ja 6 artiklan mukaisten kriteerien valossa keskeisten palveluiden tarjoajina voitaisiin pitää vesihuoltolaitoksia, jotka toimittavat vettä vähintään 5000 käyttäjälle, sillä tällaiseen palveluun kohdistuvilla tietoturvallisuuteen liittyvillä häiriöillä olisi aina verkko- ja tietoturvadirektiivin tarkoittama merkittävä vaikutus vesihuoltopalveluiden tarjontaan.

**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, ml. internetin yhdysliikennepisteet ainakin niiltä osin, kun niitä käytetään yleisten viestintäverkkojen yhteenliittämiseen sekä nimipalvelun tarjoaminen silloin, kun se liittyy internetyhteyspalvelun tarjontaan.

Yhdysliikennepisteisiin voivat kytkeytyä muutkin kuin yleiset viestintäverkot ja näin tyypillisesti tapahtuukin. Esimerkiksi suuret sisällönvälittäjät voivat käyttää yhdysliikennepisteitä. Toisaalta yleisten viestintäverkkojen liikennettä vaihdetaan paljon myös yhdysliikennepisteiden n ulkopuolella. Suomalaiset toimijat vaihtavat liikennettä myös Suomen ulkopuolella, esimerkiksi ruotsalaisessa yhdysliikennepisteessä. Suomen markkinoilla on ennestään kaksi yhdysliikennepisteen tarjoajaa ja kolmas on käynnistämässä toimintaa.

Vaikka teleyrityksiä voitaisiin pitää digitaalisen infrastruktuurin alueella yhteiskunnan toiminnan kannalta keskeisinä, ne on direktiivin mukaan suljettu sen velvoitteiden soveltamisalan ulkopuolelle. Lisäksi teleyrityksiä koskevasta tietoturvariskienhallinnasta ja velvollisuudesta ilmoittaa häiriöistä säädetään jo nykyisin tietoyhteiskuntakaaressa.

Teleyritysten lisäksi aluetunnusrekisterin ylläpitoa voidaan pitää digitaalisen infrastruktuurin kannalta keskeisenä. Suomessa keskeistä on aluetunnusrekisterin ylläpito fi-maatunnuksen ja ax-maakuntatunnuksen osalta.

###### Palveluntarjoajien toimintaan liittyvät tietoturvallisuusriskienhallinta- ja häiriöraportointivaatimukset

###### *Energia*

Vaikka sähkömarkkinalakiin ja kaasumarkkinalakiin sisältyy joitakin riskienhallintavelvoitteita, ei varsinaisia velvoitteita verkko- ja tietojärjestelmiin kohdistuvien riskien hallitsemiseksi ole säädetty. Häiriöistä ilmoittamisesta ei myöskään ole sähkömarkkinalaissa säädetty, muutoin kuin käyttäjille lain 59 §:ssä tarkoitetuissa tapauksissa. Tämän vuoksi sähkömarkkinalakiin olisi otettava säännökset velvoittamaan keskeisten palveluiden tarjoajia huolehtimaan verkko- ja tietojärjestelmiensä turvallisuudesta sekä ilmoittamaan merkittävistä järjestelmien tietoturvallisuuteen liittyvistä häiriöistä Energiavirastolle.

###### *Liikenne*

Vaikka liikenteen osalta riskienhallintaan liittyvään lainsäädäntöön voisi sinänsä katsoa sisältyvän myös verkko- ja tietojärjestelmien turvallisuuden, ei verkko- ja tietoturvallisuuteen liittyviä velvoitteita varsinaisesti sisälly liikenteen keskeisiä palveluita koskevaan lainsäädäntöön. Tietoturvallisuuden vaarantuessa vaaratilanteita voisi aiheutua myös liikenteen turvallisuuteen tai keskeisten palvelujen jatkuvuuteen. Tämän vuoksi tulisi velvoitteet tietoturvallisuudesta huolehtimisesta 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 (hätäkeskuslaitos e-call palvelun ylläpitäjänä sekä Liikennevirasto Digiroad ja Digitraffic- palveluiden ylläpitäjänä) koskien liikennekaareen.

###### *Pankkiala ja finanssimarkkinoiden infrastruktuurit*

Luottolaitoslaissa ja maksulaitoslaissa säädetään molemmissa kattavasti operatiiviseen riskienhallintaan liittyvistä velvoitteista, joita täydentää Finanssivalvonnan antama määräys operatiivisten riskien hallinnasta. Velvoitteiden voi katsoa sekä riskienhallinta- sekä poikkeamanraportointivelvoitteiden osalta täyttävän verkko- ja tietoturvadirektiivin vaatimukset.

Pörssin ja arvopaperikeskuksen osalta lakisääteisten ja Finanssivalvonnan operatiiviseen riskienhallintaa koskevan määräykseen sisältyvien riskienhallintavelvoitteiden voidaan katsoa olevan verkko- ja tietoturvadirektiivin velvoitteiden valossa riittävät, mutta velvoite ilmoittaa tietoturvallisuuteen liittyvistä häiriöistä tulisi säätää erikseen.

###### *Terveydenhuoltoala*

Terveydenhuollon osalta voimassa olevaan lainsäädäntöön sisältyy velvoitteet asiakastietojen käsittelyyn tarkoitettujen järjestelmien tietoturvallisuudesta sekä vaatimukset koskien terveydenhuollon laitteita. Velvoitteiden lisäksi on säädetty tietoturvallisuuteen liittyvien häiriöiden ilmoituksista valvovalle viranomaiselle. Voimassa oleva lainsäädäntö täyttää sellaisenaan verkko- ja tietoturvadirektiivin 14 artiklassa asetetut turvallisuusvaatimukset ja poikkeamien ilmoittamisvaatimukset.

###### *Juomaveden toimittaminen ja jakelu*

Juomaveden toimittamiseen ja jakeluun liittyvät vesihuoltolaitoksia koskevat turvallisuusriskienhallintavelvoitteet sisältyvät vesihuoltolakiin. Vesihuoltolaitoslakiin sisältyvän varautumisvelvoitteen voi katsoa sisältävän velvoitteen varautua myös tietoturvariskeihin. Sen sijaan vesihuoltolakiin ei sisälly velvoitetta ilmoittaa järjestelmien tietoturvallisuuteen liittyvistä häiriöistä valvovalle viranomaiselle, joten lakiin olisi otettava tästä erillinen velvoite.

###### *Digitaalinen infrastruktuuri*

Teleyrityksiä koskevat sähköisen viestinnän laatuvaatimukset sekä velvoitteet ilmoittaa tietoturvallisuuteen liittyvistä häiriöistä sisältyvät tietoyhteiskuntakaareen. Tietoyhteiskuntakaareen sisältyy myös velvoite aluetunnusrekisterin ylläpitäjälle huolehtia tietoturvasta. Viestintävirasto on lain mukaan fi-aluetunnusrekisteriä ylläpitävä viranomainen. Ahvenanmaanmaakuntahallinto ylläpitää ax-aluetunnusrekisteriä. Tietoyhteiskuntakaaren velvoitteet täyttävät sellaisenaan verkko- ja tietoturvadirektiivin 14 artiklassa asetetut 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 tietoturvallisuudesta huolehtimisesta sekä merkittävistä järjestelmien tietoturvallisuuteen liittyvistä häiriöistä ilmoittamisesta Viestintävirastolle ottaa tietoyhteiskuntakaareen.

###### Riskienhallinta- ja raportointivelvoitteiden valvonta

Voimassa olevaan lainsäädäntöön sisältyy edellä kuvatulla tavalla turvallisuusriskienhallintaan sekä poikkeamien 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 verkko- ja tietojärjestelmien turvallisuutta valvoisi sama viranomainen kuin muitakin 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 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. Luotto- ja maksulaitosten 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 tietoturvallisuuteen liittyvistä häiriöistä virastolle.

Juomaveden toimittamista ja jakeluun liittyvät vesihuoltolaitoksia koskevat turvallisuusriskienhallintavelvoitteet sisältyvät vesihuoltolakiin. Vesihuoltolain mukainen valvovia viranomaisia ovat toimialoillaan elinkeino-, liikenne- ja ympäristökeskus sekä kunnan terveydensuojeluviranomainen ja kunnan ympäristönsuojeluviranomainen. Juomaveden toimittamisen ja jakelun toimialalla ei ole vastaavaa keskitettyä sektorikohtaista valvontaviranomaista kuin muilla direktiivin täytäntöönpanoon kuuluvilla toimialoilla. 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. Sosiaali- ja terveysalan lupa- ja valvontaviranomainen ohjaa kuntien terveydensuojeluviranomaisia talousveden laatua ja valvontaa koskevissa asioissa. Juomaveden laadun varmistamiseksi sekä viranomaisten valvontatehtävien tehokkaaksi suorittamiseksi olisi säädettävä tietoturvaan liittyvien häiriöiden ilmoittamisesta Sosiaali- ja terveysalan lupa- ja valvontaviranomaiselle.

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 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). Riittävän toimivallan varmistamiseksi valvontaviranomaisten lakisääteiset tehtävät sekä lisäksi voimassa olevan lain viranomaisten tiedonsaantioikeuksia ja tietojen käsittelyn edellytyksiä koskeva sääntely kaipaavat tiettyjä tarkennuksia.

## Esityksen tavoitteet ja keskeiset ehdotukset

### 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, jollei 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 verkko- ja tietojärjestelmien käytöstä.

Esityksessä ehdotettaisiin tietyille yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjoajille velvollisuutta huolehtia verkko- ja tietojärjestelmiinsä liittyvästä riskienhallinnasta. Tavoitteena olisi varmistua, että yritykset 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 poikkeamien merkitystä, jotta tarvittaviin korjaaviin toimenpiteisiin voitaisiin ryhtyä.

### 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 tietoturva- tai muita riskienhallintaan sekä turvallisuuteen liittyviä velvoitteita verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvilla toimialoilla on tällä hetkellä voimassaolevan kansallisen lainsäädännön, EU-lainsäädännön sekä kansainvalist4n 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 fragmentoitunutta. Suurimmalla osalla soveltamisalaan kuuluvista toimialoista on säädetty riskienhallintaa ja 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 sanamuodosta voida tulkita, voidaanko tietyn velvoitteen katsoa kattavan myös tietojärjestelmien turvaamisen. Ilmoitusvelvollisuuksia on asetettu lähes kaikilla toimialoilla, mutta tietoturvahäiriöistä 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.

Lisäksi tietoturvallisuutta koskeva riskienhallinnan ei voida katsoa sillä tavoin eroavan muusta toimijan riskienhallinnasta, että niistä olisi ollut aiheellista säätää eri laeissa. 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 koskevat 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.

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 onkin 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 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 tietoturvaan liittyvät poikkeamailmoitukset 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 itseisarvon eikä palveluiden turvallisuuden ja jatkuvuuden kannalta mitoitettu osa paleluiden tarjontaa ja valvontaa. Ongelmallisena voidaan myös pitää sitä, ettei aina ole selvää johtuuko poikkeama esimerkiksi tietojärjestelmien turvallisuuteen vai onko kyseessä muuhun turvallisuuteen liittyvä poikkeama. Poikkeamilla saattaa todennäköisesti olla myös läheisiä liittymiä verkko- ja tietojärjestelmien turvallisuuden 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 sillä tavoin operatiivinen operatiivinen ja sen toiminnalla on niin läheinen yhteys direktiivin mukaisen CSIRT-toimijan tehtäviin, että olisi luontevampaa, että Viestintävirasto toimisi direktiivin mukaisena keskitettynä yhteyspisteenä.

### 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 velvollisuudesta 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 keskeisen 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 keskeisen sataman pitäjää. Sähkömarkkinalain velvoitteet koskisivat verkonhaltijaa. Maakaasumarkkinalain velvoitteet koskisivat siirtoverkonhaltijaa ja vesihuoltolain velvoitteet vesihuoltolaitosta, joka toimittaa vettä vähintään 5000 kuutiometriä vuorokaudessa.

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.

## Esityksen vaikutukset

[Täydennetään lausuntokierroksen perusteella]

### Taloudelliset vaikutukset

### Vaikutukset viranomaisen toimintaan

### Yhteiskunnalliset vaikutukset

Esityksellä parannettaisiin yhteiskunnan toiminnan kannalta keskeisten 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, tietojenkalastelu ja muut tietoturvaloukkaukset, kuten laajamittaiset palvelunestohyökkäykset tai laaja-alaisesti levitettävät kiristyshaittaohjelmat, jotka ovat vuosien 2016 ja 2017 aikana aiheuttaneet merkittäviä häiriöitä myös yhteiskunnan toiminnan kannalta keskeisten palveluiden tarjontaan.

Esitetty ilmoitusvelvollisuus valvoville viranomaisille tietoturvallisuuteen liittyvistä häiriöistä parantaisi valvovien viranomaisten tietoturvallisuuden tilannekuvaa ja kasvattaisi tietoturvallisuuteen liittyvää osaamista eri toimialoilla.

## Asian valmistelu

### Valmisteluvaiheet ja -aineisto

Liikenne- ja viestintäministeriö asetti verkko- ja tietoturvadirektiivin täytäntöönpanoa tukevan työryhmän 4 päivänä lokakuuta 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 Trafi, 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, mutta erityisasiantuntija Riitta Autere toimi ministeriön yhdyshenkilönä. 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 joulukuussa 2016. Direktiivin valmistelua ja täytäntöönpanoa on myös käyty esittelemässä useissa sektorikohtaisissa tilaisuuksissa, valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmässä (VAHTI) sekä digitaalisen liiketoiminnan kasvuympäristön

rakentamiseen tähtäävän kärkihankkeen toimeenpanoa koordinoimaan 15 päivänä elokuuta 2015 asetetussa työryhmässä.

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

### Lausunnot ja niiden huomioon ottaminen

Ehdotus hallituksen esitykseksi on valmisteltu liikenne- ja viestintäministeriössä. Liikenne- ja viestintäministeriö on lähettänyt ehdotuksen lausunnoille […]

## Riippuvuus muista esityksistä

*Liikenne- ja viestintäministeriön hallinnonalan virastouudistus (LIIVI) ja Liikenneviraston liiken-teenohjaustehtävien yhtiöittäminen*

Liikenne- ja viestintäministeriö on 25 päivänä huhtikuuta 2017 asettanut hankkeen, jossa valmistellaan hallituksen esitys eduskunnalle laeiksi Liikenne- ja X-virastoista ja niihin liittyväksi lainsäädännöksi sekä asetuksiksi (LIIVI-hanke) ja hallituksen esitys eduskunnalle laiksi Liikenneviraston liikenteenohjaustoiminnon yhtiöittämisestä. Tavoittena 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 liiken-teeseen liittyvän tiedon hyödyntämistä yksityisellä sektorilla ja uuden liiketoiminnan syntymistä. Tavoitteena on, että liikenteen ohjauksella kerättävä tieto hyödyntää aiempaa tehokkaammin koko yhteiskuntaa.

Liikenne- ja viestintäministeriö on hankkeen toteuttamiseksi asettanut ohjausryhmän sekä neljä työryhmää. Liikenteen turvallisuusviraston ja Viestintäviraston yhdistämisestä vastaava työryhmän tehtävänä on myös selvittää Viestintäviraston kyberturvallisuusasioiden yhtiöittämistä tai siirtämistä Huoltovarmuuskeskukselle.

*Tiedonhallintalaki*

TÄYDENNÄ

### Esityksen suhde Ahvenanmaan itsehallintoon

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

## Lakiehdotusten perustelut

### Laki tietoyhteiskuntakaaren muuttamisesta

**3 §.** *Määritelmät.* Pykälään ehdotettaisiin lisättävän uudet määritelmät verkossa toimivaksi markkinapaikaksi, hakukonepalveluksi sekä pilvipalveluksi.

*Verkossa toimivalla markkinapaikalla* tarkoitettaisiin 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.

*Hakukonepalvelu* 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.

*Pilvipalvelun* määritelmä kattaisi palvelut, jotka mahdollistavat 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 tarjotaan 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 jossa 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).

**247 a §.** *Verkossa toimivan markkinapaikan, hakukonepalvelun sekä pilvipalvelun tarjoajan velvollisuus huolehtia tietoturvasta.* 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 mukaiset tietojärjestelmät voivat koostua esimerkiksi tämän lain 3 §:n 25 kohdassa tarkoitetuista telepäätelaitteista taikka tiedoista, joita näissä järjestelmissä säilytetään, käsitellään, haetaan tai siirretään. 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. 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.

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 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun direktiivin (EU) 2016/1148 nojalla annetussa komission täytäntöönpanoasetuksessa [täydennä yksilöintitiedot].

Pykälän 3 momentin mukaan 1 momentissa tarkoitettua riskienhallintavelvoite ei koske toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun direktiivin (EU) 2016/1148 16 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.

Säännöksillä pannaan täytäntöön toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun direktiivin (EU) 2016/1148 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, poikkeaman kesto sekä maantieteellinen levinneisyys alueella, johon poikkeama vaikuttaa. verkko- ja tietoturvadirektiivin nojalla annetussa Euroopan komission täytäntöönpanosäädöksessä [täydennä yksilöintitiedot].

Pykälän uudessa 3 momentissa säädettäisiin Viestintäviraston oikeudesta velvoittaa palvelun tarjoaja tiedottamaan tapahtumasta 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 asiasta.

Ehdotettu uusi 4 momentti vastaisi muutoin voimassa olevan lain 2 momenttia, mutta lisäksi siinä annettaisiin Viestintävirastolle annettaisiin toimivalta antaa määräyksiä myös uudessa 2 momentissa tarkoitettujen ilmoituksien 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.

**313 §.** *Valvonta-asioiden käsittely Viestintävirastossa.* Pykälän 2 momentin 2 kohtaa ehdotettaisiin muutettavan 2 kohtaan lisättäisiin Viestintävirastolle oikeus jättää asia tutkimatta, jos asialla on 247 a §:ssä tarkoitettujen palveluiden riskinhallinnan kannalta vain vähäinen merkitys. Tarkoituksena olisi antaa Viestintävirastolle oikeus käsitellä tämän lain 275 §:n 2 momentissa tarkoitettu 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.

**308 §.** *Yhteistyö eri viranomaisten kanssa.* Pykälään ehdotettaisiin lisättävän uusi 3 momentti, jossa säädettäisiin Viestintäviraston velvoitteesta 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 direktiivin mukaisista häiriöilmoituksista.

**318 §.** *Tietojen luovuttaminen viranomaisesta.* Pykälään ehdotettaisiin lisättävän uusi 2 momentti, jossa säädettäisiin Viestintäviraston oikeudesta luovuttaa tietoja verkko- ja tietoturvadirektiivin kannalta keskeisten valvontaviranomaisten kanssa. Tarkoituksena olisi varmistaa, että verkko- ja tietoturvadirektiivin mukaisia velvoitteita valvovat eri viranomaiset pystyisivät vaihtamaan valvontatehtäviensä kannalta merkityksellistä tietoa.

### Laki ilmailulain muuttamisesta

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

Pykälän 1 momentissa säädetty riskienhallintavelvoite säädettäisiin ehdotetun tietoyhteiskuntakaaren 247 a §:än 1 momenttia vastaavilla perusteilla. 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.

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. Merkittävällä riskillä tarkoitettaisiin poikkeama-asetuksen 4 artiklassa tarkoitettua riskiä vastaavaa riskiä.

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 mukaisin keskeisten palveluiden tarjoajina. Arvioidessa sitä, onko toimija yhteiskunnan toiminnan kannalta merkittävä, olisi huomioitava verkko- ja tietoturvadirektiivin 5 artiklan 2 kohdan mukaiset kriteerit.

**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 momentissasäädettäisiin velvoitteesta ilmoittaaLiikenteen turvallisuusvirastolle merkittävästä poikkeamasta, joka voi muodostaa merkittävän riskin ilmailun turvallisuudelle. Poikkeamalla tarkoitettaisiin vastaavaa tietoturvallisuuteen liittyvää häiriötä kuin ehdotetussa tietoyhteiskuntakaaren 275 §:ssä. Poikkeaman merkittävyyden määrittämiseksi olisi otettava huomioon erityisesti niiden käyttäjien lukumäärä, joihin häiriö vaikuttaa, poikkeaman kesto sekä maantieteellinen levinnäisyys. Merkittävällä riskillä ilmailun turvallisuudelle tarkoitettaisiin poikkeama-asetuksen 4 artiklassa tarkoitettua merkittävää vaikutusta.

Pykälän 2 ja 3 momentit säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 ja 4 momentit.

Pykälän 4 momentissa säädettäisiin Liikenteen turvallisuusviraston oikeudesta antaa tarkempia määräyksiä pykälässä tarkoitettujen ilmoituksen sisällöstä, muodosta ja toimittamisesta.

### Laki rautatielain muuttamisesta

 **41 a §.** *Velvollisuus huolehtia tietoturvasta.* Ehdotettu pykälä on uusi. Pykälässä säädettäisiin valtion rataverkon haltijan ja liikenteenohjauspalveluja tarjoavan yrityksen velvollisuudesta huolehtia käyttämiinsä rautatieliikenteen turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä velvollisuudesta ilmoittaa Liikenteen turvallisuusvirastolle merkittävästä järjestelmiensä tietoturvallisuuteen liittyvästä häiriöstä, joka voi muodostaa rautatiejärjestelmälle merkittävän turvallisuusriskin.

Pykälän 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite säädettäisiin samoin perustein kuin tietoyhteiskuntakaaren 247 a § 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite. 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.

Pykälän 2 momentissa säädettäisiin velvoitteesta ilmoittaatietoturvallisuuteen liittyvästä häiriöstä, joka voi aiheuttaa rautatiejärjestelmälle merkittävän turvallisuusriskin, Liikenteen turvallisuusvirastolle. Tietoturvallisuuteen liittyvällä merkittävällä häiriöllä tarkoitettaisiin vastaavaa häiriötä kuin ehdotetussa tietoyhteiskuntakaaren 275 §:ssä. Häiriön merkittävyyttä tulisi arvioida ilmailulakiin ehdotettua128 b §:n 1 momenttia vastaavilla kriteereillä. Merkittävällä turvallisuusriskillä tarkoitettaisiin rautatielain 39 §:n 2 momentissa tarkoitettua riskiä. Järjestelmillä tarkoitettaisiin 1 momentissa tarkoitettuja viestintäverkkoja ja tietojärjestelmiä.

Pykälän 2 ja 3 momentit säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 ja 4 momentit.

Pykälän 4 momentti säädettäisiin vastaavin perustein kuin ehdotetun ilmailulain 128 b §:n 4 momentti.

### Laki alusliikennepalvelulain muuttamisesta

**16 §.** *Alusliikennepalvelun ylläpito.* Pykälään ehdotettaisiin lisättävän uusi 5 momentti, jossa säädettäisiin alusliikennepalvelun tarjoajan velvollisuudesta huolehtia käyttämiinsä merenkulun turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Riskienhallintavelvoite säädettäisiin samoin perustein kuin tietoyhteiskuntakaaren 247 a § 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite. 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.

 **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 Liikenteen turvallisuusvirastollemerkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi merkittävästi vaikuttaa merenkulun turvallisuuteen. Tietoturvallisuuteen liittyvällä merkittävällä häiriöllä tarkoitettaisiin vastaavaa häiriötä kuin ehdotetussa tietoyhteiskuntakaaren 275 §:ssä. Häiriön merkittävyyttä tulisi arvioida ilmailulakiin ehdotettua128 b §:n 1 momenttia vastaavilla kriteereillä. Järjestelmillä tarkoitettaisiin ehdotetun 16 §:n 5 momentissa tarkoitettuja viestintäverkkoja ja tietojärjestelmiä.

Pykälän 2 ja 3 momentit säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 ja 4 momentit.

Pykälän 4 momentti säädettäisiin vastaavin perustein kuin ehdotetun ilmailulain 128 b §:n 4 momentti.

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

 **7 e §.** *Satamanpitäjän velvollisuus huolehtia tietoturvasta.* Ehdotettu pykälä on uusi. Pykälässä säädettäisiin yhteiskunnan toiminnan kannalta keskeisen sataman pitäjän velvollisuudesta huolehtia käyttämiinsä merenkulun turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta sekä velvollisuudesta ilmoittaa järjestelmiensä tietoturvallisuuteen liittyvästä merkittävästä häiriöstä Liikenteen turvallisuusvirastolle.

Pykälän 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite säädettäisiin samoin perustein kuin tietoyhteiskuntakaaren 247 a § 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite. 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.

Pykälän 2 momentissa säädettäisiin velvoitteesta ilmoittaa Liikenteen turvallisuusvirastolle merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi merkittävästi vaikuttaa merenkulun turvallisuuteen. Tietoturvallisuuteen liittyvällä merkittävällä häiriöllä tarkoitettaisiin vastaavaa häiriötä kuin ehdotetussa tietoyhteiskuntakaaren 275 §:ssä. Häiriön merkittävyyttä tulisi arvioida ilmailulakiin ehdotettua128 b §:n 1 momenttia vastaavilla kriteereillä.

Pykälän 3 ja 4 momentit säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 ja 4 momentit.

Pykälän 5 momentti säädettäisiin vastaavin perustein kuin ehdotetun ilmailulain 128 b §:n 4 momentti.

Pykälän 6 momentin asetuksenantovaltuuden mukaan Valtioneuvoston asetuksella säädetään tarkemmin, milloin 1 momentissa tarkoitettua satamaa on pidettävä yhteiskunnan toiminnan kannalta merkittävänä. Tarkoituksena olisi, että asetuksella voitaisiin tarkoituksen mukaisin raja-arvoin määritellä ne satamat, joidenka pitäjiin riskienhallintavelvoitetta sovellettaisiin, sillä kaikkia satamanpitäjiä ei olisi tarkoituksen mukaista 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.

### Laki liikenteenpalveluista annetun lain muuttamisesta

**III OSA.** PALVELUT

**2 luku.** Tietojen ja tietojärjestelmien yhteentoimivuus

**7 §.** *Älykkään liikennejärjestelmän ylläpitäjän velvollisuus huolehtia tietoturvasta.* 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.

Pykälän 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite säädettäisiin samoin perustein kuin tietoyhteiskuntakaaren 247 a § 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite.

Pykälän 2 momentissa säädettäisiin velvoitteesta ilmoittaa Liikenteen turvallisuusvirastolle merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi muodostaa älykkään liikennejärjestelmän turvallisuudelle merkittävän riskin. Tietoturvallisuuteen liittyvällä merkittävällä häiriöllä tarkoitettaisiin vastaavaa häiriötä kuin ehdotetussa tietoyhteiskuntakaaren 275 §:ssä. Häiriön merkittävyyttä tulisi arvioida ilmailulakiin ehdotettua128 b §:n 1 momenttia vastaavilla kriteereillä.

Pykälän 3 ja 4 momentit säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 ja 4 momentit.

Pykälän 5 momentti säädettäisiin vastaavin perustein kuin ehdotetun ilmailulain 128 b §:n 4 momentti.

### Laki sähkömarkkinalain muuttamisesta

 **29 a §.** *Verkonhaltijan velvollisuus huolehtia tietoturvasta.* 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 sekä sellaisia suljetun jakeluverkon haltijoita, joiden sähköverkkoon ei ole liitetty jakeluverkkoa.

Pykälän 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite säädettäisiin samoin perustein kuin tietoyhteiskuntakaaren 247 a § 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite.

Pykälän 2 momentissa säädettäisiin velvoitteesta ilmoittaa Energiavirastolle merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena sähkönjakelu voi keskeytyä jakeluverkossa merkittävässä laajuudessa, Energiavirastolle. Tietoturvallisuuteen liittyvällä merkittävällä häiriöllä tarkoitettaisiin vastaavaa häiriötä kuin ehdotetussa tietoyhteiskuntakaaren 275 §:ssä. Häiriön merkittävyyttä tulisi arvioida ilmailulakiin ehdotettua128 b §:n 1 momenttia vastaavilla kriteereillä. Ilmoituskynnys, silloin kun häiriön seurauksena sähkönjakelu voi keskeytyä merkittävässä laajuudessa, vastaisi sähkömarkkinalain 59 §:n ilmoituskynnystä. Järjestelmillä tarkoitettaisiin 1 momentissa tarkoitettuja viestintäverkkoja ja tietojärjestelmiä.

Pykälän 2 ja 3 momentit säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 ja 4 momentit.

Pykälän 4 momentti säädettäisiin vastaavin perustein kuin ehdotetun ilmailulain 128 b §:n 4 momentti.

Pykälän 6 momentissa rajattaisiin pykälän 1 ja 2 momentin velvoitteiden ulkopuolelle sähkönjakelu suljetussa jakeluverkossa sekä sähkönjakelu suurjännitteisessä jakeluverkossa, johon ei ole liitetty jakeluverkkoa, koska näiden palveluiden ei voida katsoa olevan verkko- ja tietoturvadirektiivin tarkoittamalla tavalla keskeisiä yhteiskunnan toiminnan kannalta.

**62 §.** *Suljettua jakeluverkkoa koskevat erityissäännökset.* Pykälään ehdotettaisiin lisättävän, ettei suljettuun jakeluverkkoon ja suljetun jakeluverkonhaltijaan ei 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.

### Laki maakaasumarkkinalain muuttamisesta

**34 a §.** *Siirtoverkonhaltijan velvollisuus huolehtia tietoturvasta.* 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 momentissa säädettäväksi ehdotettu riskienhallintavelvoite säädettäisiin samoin perustein kuin tietoyhteiskuntakaaren 247 a § 1 momentissa säädettäväksi ehdotettu riskienhallintavelvoite.

Pykälän 2 momentissa säädettäisiin velvoitteesta ilmoittaa Energiavirastolle merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena maakaasun siirto voi keskeytyä merkittävässä laajuudessa. Tietoturvallisuuteen liittyvällä merkittävällä häiriöllä tarkoitettaisiin vastaavaa häiriötä kuin ehdotetussa tietoyhteiskuntakaaren 275 §:ssä. Häiriön merkittävyyttä tulisi arvioida ilmailulakiin ehdotettua128 b §:n 1 momenttia vastaavilla kriteereillä. Järjestelmillä tarkoitettaisiin 1 momentissa tarkoitettuja viestintäverkkoja ja tietojärjestelmiä.

Pykälän 2 ja 3 momentit säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 ja 4 momentit.

Pykälän 4 momentti säädettäisiin vastaavin perustein kuin ehdotetun ilmailulain 128 b §:n 4 momentti.

### Laki sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 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.

**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.

### Laki vesihuoltolain muuttamisesta

**15 b §.** *Tietoturvaan liittyvien häiriöiden ilmoittaminen.* Pykälässä säädettäisiin tietoturvallisuuteen liittyvien häiriöiden ilmoittamisesta Sosiaali- ja terveysalan lupa- ja valvontavirastolle sekä Sosiaali- ja terveysalan lupa- ja valvontaviraston oikeudesta antaa ilmoituksia koskevia määräyksiä.

Pykälän 1 momentissa säädettäisiin velvoitteesta ilmoittaatietoturvallisuuteen merkittävästä liittyvästä häiriöstä, joiden seurauksena talousveden jakelu voi keskeytyä merkittävässä laajuudessa tai talousveden laatuvaatimusten täyttäminen voi merkittävästi vaarantua, Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Tietoturvallisuuteen liittyvällä merkittävällä häiriöllä tarkoitettaisiin vastaavaa häiriötä kuin ehdotetussa tietoyhteiskuntakaaren 275 §:ssä. Häiriön merkittävyyttä tulisi arvioida ilmailulakiin ehdotettua128 b §:n 1 momenttia vastaavilla kriteereillä. Talousveden laatuvaatimuksilla tarkoitettaisiin terveydensuojelulain (763/1994) 17 §:ssä tarkoitettuja vaatimuksia. Pykälän velvoite koskisi vesihuoltolaitosta, joka toimittaa vettä vähintään 5 000 kuutiometriä vuorokaudessa. Tarkoituksena on rajata velvoite verkko- ja tietoturvadirektiivin kannalta keskeisiin palveluntarjoajiin.

Pykälän 2 ja 3 momentit säädettäisiin vastaavin perustein kuin ehdotetun tietoyhteiskuntakaaren 275 §:n 3 ja 4 momentit.

Pykälän 4 momentti säädettäisiin vastaavin perustein kuin ehdotetun ilmailulain 128 b §:n 4 momentti.

## Voimaantulo

Lait ehdotetaan tulemaan voimaan 1 päivänä toukokuuta 2018.

## 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. Kuitenkin on huomioitava. että yksityiselämän ja henkilötietojen suojan kannalta lähtökohtana on, että oikeushenkilöt eivät kuulu säännöksen 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).

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 (PeVL 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.

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 5 momentissa, alusliikennepalvelulain muuttamisesta annetun lain 18 a §:n4 momentissa, eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta annetun lain muuttamisesta annetun lain 7 e §:n 5 momentissa, liikenteen palveluista annetun lain muuttamisesta annetun lain 7 §:n 5 momentissa, Energiavirastolle sähkömarkkinalain muuttamisesta annetun lain 29 a §:n 5 momentissa ja maakaasumarkkinalain 34 a §:n 5 momentissa sekä Sosiaali- ja terveysalan lupa- ja valvontavirastolle vesihuoltolain muuttamisesta annetun lain 15 b §:n 5 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

**LAKI**

**tietoyhteiskuntakaaren muuttamisesta**

Eduskunnan päätöksen mukaisesti

*muutetaan* tietoyhteiskuntakaaren (917/2014) 275 §, 313 §:n 2 momentin 2 kohta sekä

*lisätään* 3 §:n 1 momenttiin, sellaisena kuin se on laissa (456/2016), uusi 2 b, 12 a ja 35 a kohta, lakiin uusi 247 a §, 308 §:ään uusi 3 momentti, 318 §:ään uusi 2 momentti, jolloin nykyinen 2, 3 ja 4 momentti siirtyvät 3, 4 ja 5 momentiksi seuraavasti:

3 §

*Määritelmät*

Tässä laissa tarkoitetaan:

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

2 b) *Hakukonepalvelulla* palvelua, joka etsii käyttäjän hakuun perustuen osumia määrittelemättömästä joukosta verkkosivustoja ja antaa käyttäjälle hakutuloksena linkkejä verkkosivustoille;

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

12 a) *Pilvipalvelulla* palvelua, joka mahdollistaa verkon välityksellä pääsyn hajautettuihin tietoteknisiin resursseihin;

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

35 a) *Verkossa toimivalla markkinapaikalla* palvelua, jonka välityksellä käyttäjät voivat tehdä verkossa kauppa- tai palvelusopimuksia elinkeinonharjoittajien kanssa.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

247 a §

*Verkossa toimivan markkinapaikan, hakukonepalvelun ja pilvipalvelun tarjoajan velvollisuus huolehtia tietoturvasta*

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 häiriöidenkäsittely;
3. liiketoiminnan jatkuvuuden hallinta;
4. seuranta, tarkastukset ja testaukset;
5. kansainvälisten standardien noudattaminen.

Edellä 1 momentissa tarkoitettua riskienhallintavelvoite ei koske toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun direktiivin (eu) 2016/1148 (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 verkko- ja tietoturvavirastolle vuosittain tiivistelmäraportin ilmoituksista.

Tämän lain 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 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 ilmoituksien sisällöstä, muodosta ja toimittamisesta.

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

308 §

*Yhteistyö eri viranomaisten kanssa*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

Viestintäviraston on toimittava yhteistyössä muiden jäsenvaltioiden verkko- ja tietoturvallisuutta valvovien viranomaisten, tietoturvaloukkauksiin reagoivien yksiköiden sekä EU:n verkko- ja tietoturvadirektiivin 10 artiklan mukaisen yhteistyöryhmän kanssa. Viestintävirasto toimittaa yhteistyöryhmälle vuosittain direktiivin 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 tai muiden tietojenluovuttamista koskevien rajoitusten estämättä oikeus luovuttaa laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto Energiavirastolle, Liikenteen turvallisuusvirastolle, Sosiaali- ja terveysalan lupa- ja valvontaviranomaiselle sekä Finanssivalvonnalle, jos se on näille säädettyjen tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämätöntä.

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

**LAKI**

**Ilmailulain muuttamisesta**

Eduskunnan päätöksen mukaisesti

*lisätään* ilmailulakiin (864/2014) uusi 128 a ja b §, seuraavasti

128 a §

*Velvollisuus huolehtia tietoturvasta*

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

Edellä 1 momentissa tarkoitetun toimijan on Liikenteen turvallisuusviraston pyynnöstä annettava sellaiset tiedot, jotka ovat tarpeen arvioitaessa 1 momentissa säädettyjen velvoitteiden noudattamista.

Liikenteen turvallisuusviraston on arvioitava 1 momentissa tarkoitetun riskienhallinnan vaikutuksia ilmailun turvallisuuteen. Virasto voi velvoittaa 1 momentissa tarkoitetun toimijan ryhtymään korjaaviin toimenpiteisiin ilmailun turvallisuuteen kohdistuvan merkittävän riskin poistamiseksi.

Liikenteen turvallisuusvirastolla on oikeus salassapitosäännösten tai 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 välttämätöntä tietoturvallisuuteen liittyvien tehtävien hoitamiseksi.

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

128 b §

*Tietoturvapoikkeamien ilmoittaminen*

Tämän lain 128 a §:ssä tarkoitetun toimijan on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sellaisesta sen 128 a §:ssä tarkoitettuihin järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä poikkeamasta, joka voi muodostaa merkittävän riskin ilmailun turvallisuudelle.

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 jäsenvaltiota ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteenturvallisuusvirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

**LAKI**

**Rautatielain muuttamisesta**

Eduskunnan päätöksen mukaisesti

*lisätään* rautatielakiin (304/2011) uusi 41 a §, seuraavasti:

41 a §

*Velvollisuus huolehtia tietoturvasta*

Valtion rataverkon haltijan sekä liikenteenohjauspalveluja tarjoavan yhtiön on huolehdittava käyttämiinsä rautatiejärjestelmän turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Valtion rataverkon haltijan sekä liikenteenohjauspalveluja tarjoavan yhtiön on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sellaisista sen järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi muodostaa rautatiejärjestelmälle merkittävän turvallisuusriskin.

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 jäsenvaltiota ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteenturvallisuusvirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

**LAKI**

**Alusliikennepalvelulain muuttamisesta**

Eduskunnan päätöksen mukaisesti

*lisätään* alusliikennepalvelulain (623/2005) 16 §:n uusi 5 momentti sekä lakiin uusi 18 a §, seuraavasti:

16 §

*Alusliikennepalvelun ylläpito*

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

VTS-viranomaisen on huolehdittava käyttämiinsä merenkulun turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta

18 a §

*Tietoturvaan liittyvistä häiriöistä ilmoittaminen*

VTS-viranomaisen on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sellaisista sen järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi aiheuttaa merkittävän vaaran merenkulun turvallisuudelle.

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 häiriö muita Euroopan unionin jäsenvaltiota ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

 Liikenteenturvallisuusvirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

**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 §, seuraavasti:

7 e §

*Satamanpitäjän velvollisuus huolehtia tietoturvasta*

Yhteiskunnan toiminnan kannalta keskeisen satamanpitäjän on huolehdittava käyttämiinsä merenkulun turvallisuuden kannalta merkittäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Satamanpitäjän on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sen järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi merkittävästi vaikuttaa merenkulun turvallisuuteen.

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 jäsenvaltiota ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteenturvallisuusvirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

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

**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 tietoturvasta

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

Älykkään liikennejärjestelmän ylläpitäjän on ilmoitettava viipymättä Liikenteen turvallisuusvirastolle sen järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joka voi muodostaa älykkään liikennejärjestelmän merkittävän turvallisuusriskin.

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 jäsenvaltiota ja ilmoitettava tarvittaessa muille asiaan liittyville jäsenvaltioille.

Liikenteenturvallisuusvirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

**LAKI**

**Sähkömarkkinalain muuttamisesta**

Eduskunnan päätöksen mukaisesti

*muutetaan* sähkömarkkinalain (588/2013) 62 §, sellaisena kun se on laissa (lisää numero), sekä, *lisätään* lakiin uusi 29 a §, seuraavasti:

29 a §

*Verkonhaltijan velvollisuus huolehtia tietoturvasta*

Verkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Verkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen järjestelmiin 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 jäsenvaltiota ja ilmoitettava tarvittaessa muille jäsenvaltioille.

Energiavirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

Edellä 1 ja 2 momentissa säädettyä ei sovelleta suurjännitteisen jakeluverkon haltijaan, jonka sähköverkkoon ei ole liitetty jakeluverkkoa.

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.

**LAKI**

**Maakaasumarkkinalain muuttamisesta**

Eduskunnan päätöksen mukaisesti

*lisätään* maakaasumarkkinalakiin (lisää numero) uusi 34 a §, seuraavasti:

34 a §

*Siirtoverkonhaltijan velvollisuus huolehtia tietoturvasta*

Siirtoverkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Siirtoverkonhaltijan on ilmoitettava viipymättä Energiavirastolle sellaisesta sen järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, joiden seurauksena maakaasun siirto voi keskeytyä siirtoverkossa merkittävässä laajuudessa. Jos häiriöstä ilmoittaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse.

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

Energiavirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

**LAKI**

**Sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain muuttamisesta**

Eduskunnan päätöksen mukaisesti

*muutetaan* sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 27 §, 28 §:n otsikko, 1 momentin johtolause 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, Viestintävirastolle ja kuluttaja-asiamiehelle niiden tehtävien hoitamista varten;

— — — — — — — — — — — — — — — — — — — — — — — — — — — — — — — —

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.

**LAKI**

**Vesihuoltolain muuttamisesta**

Eduskunnan päätöksen mukaisesti

*lisätään* vesihuoltolakiin (119/2001) uusi 15 b §, seuraavasti:

15 b §

*Tietoturvapoikkeamien ilmoittaminen*

Vesihuoltolaitoksen, joka toimittaa vettä vähintään 5 000 kuutiometriä vuorokaudessa, on ilmoitettava viipymättä Sosiaali- ja terveysalan lupa- ja valvontavirastolle sellaisesta sen järjestelmiin kohdistuvasta merkittävästä tietoturvallisuuteen liittyvästä häiriöstä, jonka seurauksena talousveden jakelu voi keskeytyä merkittävässä laajuudessa tai talousveden laatuvaatimusten täyttäminen voi merkittävästi vaarantua.

Jos häiriöstä ilmoittaminen yleisen edun mukaista, Sosiaali- ja terveysalan lupa- ja valvontavirasto voi velvoittaa palvelun tarjoajan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. Sosiaali- ja terveysalan lupa- ja valvontaviraston on arvioitava koskeeko 2 momentissa tarkoitettu häiriö muita Euroopan unionin jäsenvaltiota ja ilmoitettava tarvittaessa muille jäsenvaltioille.

Mitä 1 ja 2 momentissa säädetään vesihuoltolaitoksesta, koskee myös laitosta, joka toimittaa vettä vesihuoltolaitokselle

Sosiaali- ja terveysalan lupa- ja valvontavirasto voi antaa tarkempia määräyksiä ilmoituksen sisällöstä, muodosta ja toimittamisesta.

1. (EU)2016/1148 johdanto-osa kohta 28 [↑](#footnote-ref-1)