EUROOPAN
KOMISSIO

Bryssel 13.9.2017
COM(2017) 474 final

KOMISSION KERTOMUS EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE

tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta annetun direktiivin 2013/40/EU noudattamiseksi tarvittavien jäsenvaltioiden toimenpiteiden laajuuden arvioinnista

Sisällysluettelo

Sisällysluettelo 2
1. Johdanto 3
1.1 Direktiivin tavoitteet ja soveltamisala 3
1.2 Kertomuksen tarkoitus ja menetelmät 5
2. Toimenpiteet direktiivin saattamiseksi osaksi kansallista lainsäädäntöä 6
2.1 Oikeudelliset määritelmät (direktiivin 2 artikla) 6
a) Tietojärjestelmä 6
b) Data 6
c) Oikeushenkilö 6
d) Oikeudettomasti 7
2.2 Määritellyt rikokset (direktiivin 3–7 artikla) 7
a) Laiton tunkeutuminen tietojärjestelmään 7
b) Laiton järjestelmän häirintä 7
c) Laiton datan vahingoittaminen 7
d) Viestintäsalaisuuden loukkaus (tietojen laiton hankkiminen) 8
e) Rikosten tekemiseen käytettävät välineet 8
2.3 Mainittuja rikoksia koskevat yleiset säännöt (direktiivin 8–12 artikla) 8
a) Yllytys ja avunanto 8
b) Yritys 8
c) Seuraamukset 8
d) Oikeushenkilöiden vastuu 10
e) Oikeushenkilöille määrättävät seuraamukset 11
f) Lainkäyttövalta 11
2.4 Käytännön kysymykset (direktiivin 13–14 artikla) 12
a) Kansallisten yhteyspisteiden järjestäminen 12
b) Tietoa vakiintuneista kansallisista yhteyspisteistä 12
c) Ilmoituskanavat 12
d) Tilastotietojen kerääminen 12
e) Tilastotietojen siirtäminen komissiolle 13
3. Päätelmät ja jatkotoimet 13

1. Johdanto

Europolin vuonna 2016 laatiman internetiä hyödyntävää järjestäytynyttä rikollisuutta koskevan uhkakuva-arvion (IOCTA) mukaan kyberrikollisuus on muuttumassa yhä aggressiivisempaan ja hyökkäävämpään suuntaan. Kehitys on nähtävissä monissa kyberrikollisuuden muodoissa, kuten tietojärjestelmiin kohdistuvissa hyökkäyksissä.[1] Europolin mainitsemia vakavia hyökkäysmuotoja ovat muun muassa haittaohjelmien käyttö ja käyttäjän manipulointi tietojärjestelmään soluttautumiseksi ja sen kaappaamiseksi tai viestinnän salakuuntelemiseksi sekä laaja-alaiset verkkohyökkäykset esimerkiksi elintärkeään infrastruktuuriin. Hyökkäyksiä pidetään merkittävinä uhkina yhteiskuntaamme kohtaan.

Kun tiedosta yhä suurempi osa tallennetaan pilveen ja tieto ja rikolliset liikkuvat erittäin nopeasti, lainvalvontaviranomaisten välisestä rajat ylittävästä yhteistyöstä on tullut kyberrikollisuuden tutkinnassa ratkaisevan tärkeää.

Jotta tämänkaltaisen rikollisuuden torjunta olisi tehokasta, jäsenvaltioiden on päätettävä yhteisesti, millaista toimintaa pidetään tietojärjestelmähyökkäyksenä. Niiden on myös lähennettävä seuraamusten suuruusluokkia ja käytännön keinoja rikosten ilmoittamiseksi ja tietojen vaihtamiseksi viranomaisten välillä. Tätä varten Euroopan parlamentti ja neuvosto antoivat 12. elokuuta 2013 tietojärjestelmiin kohdistuvista hyökkäyksistä direktiivin 2013/40/EU[2] (”direktiivi”), joka korvasi neuvoston puitepäätöksen 2005/222/YOS.

1.1 Direktiivin tavoitteet ja soveltamisala

Direktiivin tavoitteina on lähentää jäsenvaltioiden[3] rikosoikeutta tietojärjestelmiin kohdistuvien hyökkäysten alalla sekä parantaa toimivaltaisten viranomaisten välistä yhteistyötä. Tämä tapahtuu vahvistamalla vähimmäissäännöt tietojärjestelmiin kohdistuvia hyökkäyksiä koskevien rikosten ja niiden seuraamusten määrittelylle ja vaatimalla viikon jokaisena päivänä ympärivuorokautisesti toimivia yhteysviranomaisia.

Direktiivissä **määritellään** seuraavat termit:

- ’Tietojärjestelmä’ 2 artiklan[4] a alakohdassa. Määritelmä on lähellä tietoverkkorikollisuutta koskevan 23. marraskuuta 2001 tehdyn Euroopan neuvoston yleissopimuksen (”Budapestin yleissopimus”) 1 artiklan a alakohdassa tarkoitettua tietojärjestelmän määritelmää sillä poikkeuksella, että direktiivin määritelmä kattaa yksitulkintaisesti myös itse datan.
- ’Data’ 2 artiklan b alakohdassa. Määritelmä vastaa Budapestin yleissopimuksen 1 artiklan b alakohdan määritelmää eli siinä viitataan tietokonejärjestelmän sijasta tietojärjestelmään.

[1] Europol, vuoden 2016 Internet Organised Crime Threat Assessment -raportti (IOCTA), saatavilla osoitteessa https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:fi:pdf

[3] Jäljempänä, ellei selkeästi tarkoiteta muuta, ’jäsenvaltioilla’ tai ’kaikilla jäsenvaltioilla’ tarkoitetaan niitä jäsenvaltioita, joita direktiivi sitoo, eli kaikkia EU-jäsenvaltioita lukuun ottamatta Tanskaa, joka ei osallistunut direktiivin hyväksymiseen Euroopan unionista tehtyyn sopimukseen ja Euroopan unionin toiminnasta tehtyyn sopimukseen (SEUT) liitetyn Tanskan asemaa koskevan pöytäkirjan 1 ja 2 artiklan mukaisesti. Yhdistyneen kuningaskunnan ja Irlannin asemaa koskevan pöytäkirjan N:o 21 3 artiklan mukaisesti molemmat valtiot osallistuivat direktiivin hyväksymiseen ja se sitoo niitä.

[4] Kaikki mainitut artiklat viittaavat direktiiviin, ellei toisin ilmoiteta.

- ’Oikeushenkilö’ 2 artiklan c alakohdassa. Määritelmän tarkoituksena on varmistaa luonnollisten ja oikeushenkilöiden vastuu ja rajata sen ulkopuolelle valtiot, julkiset elimet ja julkisoikeudelliset kansainväliset järjestöt.
- Ilmaisu ’oikeudettomasti’ 2 artiklan d alakohdassa. Määritelmä koskee rikosoikeuden yleisperiaatetta, ja sen tarkoituksena on välttää sellaisen henkilön rikosoikeudellinen vastuu, joka toimii joko kansallisen lainsäädännön sallimissa puitteissa tai tietojärjestelmän tai sen osan omistajan tai muun oikeudenhaltijan luvalla.

Direktiivissä määritellään seuraavat **tietojärjestelmiin kohdistuvat rikokset:**

- laiton tunkeutuminen tietojärjestelmään sellaisenaan (3 artikla);
- laiton järjestelmän häirintä (4 artikla), joka kattaa sellaisen laittoman tunkeutumisen tietojärjestelmään, joka keskeyttää sen toiminnan tai estää sitä vakavasti;
- laiton datan vahingoittaminen (5 artikla), joka viittaa laittomaan dataan puuttumiseen, joka heikentää sen eheyttä tai saatavuutta;
- viestintäsalaisuuden loukkaus (6 artikla) eli tietojen hankkiminen oikeudettomasti luottamuksellisesta datan siirrosta, mukaan lukien tällaista dataa sisältävästä tietojärjestelmästä lähtevä sähkömagneettinen säteily;
- mainittujen rikosten tekemiseen käytettävien välineiden laiton toimittaminen (7 artikla). Tässä yhteydessä tällaisia välineitä voivat olla tietokoneohjelma sekä tietokoneen salasana tai muu data, joka mahdollistaa pääsyn tietojärjestelmään.

Lisäksi direktiivissä **laajennetaan rikosoikeudellinen vastuu** koskemaan myös luonnollisten ja oikeushenkilöiden toteuttamaa yllytystä ja avunantoa edellä mainittuihin rikoksiin sekä niiden yritystä (8 artikla). Yllytys ja avunanto kattaa kaikki 3–7 artiklassa tarkoitetut rikokset, kun taas yritys kattaa vain 4 ja 5 artiklan rikokset.

Direktiivissä tarkoitettujen rikosten **enimmäisrangaistusten** vähimmäistasot vahvistetaan 9 artiklassa:

- Lähtökohtaisesti kaikista paitsi 8 artiklassa mainituista rikoksista asetetaan vähintään kahden vuoden enimmäisvankeusrangaistus (9 artiklan 2 kohta).
- Vähintään kolmen vuoden enimmäisvankeusrangaistusta sovelletaan 4 ja 5 artiklassa tarkoitettuihin rikoksiin, kun rikos on vaikuttanut merkittävään määrään tietojärjestelmiä (ns. bottiverkkorikokset; 9 artiklan 3 kohta).
- Vähintään viiden vuoden enimmäisvankeusrangaistusta edellytetään 4 ja 5 artiklassa mainituista rikoksista, joiden tekijänä on rikollisjärjestö (9 artiklan 4 kohdan a alakohta), jotka aiheuttavat vakavaa vahinkoa (9 artiklan 4 kohdan b alakohta) tai jotka kohdistuvat elintärkeään infrastruktuuriin kuuluvaan tietojärjestelmään (9 artiklan 4 kohdan c alakohta).
- Kun 4 ja 5 artiklassa mainittu rikos tehdään toisen henkilön henkilötietojen väärinkäytön yhteydessä, jäsenvaltioiden olisi varmistettava, että sitä voidaan pitää raskauttavana asianhaarana, elleivät kyseiset asianhaarat jo kuulu jonkin muun rikoksen tunnusmerkistöön (9 artiklan 5 kohta).

Seuraavissa artikloissa määritetään **oikeushenkilöiden vastuun** vähimmäisvaatimukset (10 artikla) ja annetaan esimerkkiluettelo niille määrättävistä mahdollisista seuraamuksista (11 artikla).

Ottaen huomioon, että edellä mainitut rikokset voidaan tehdä (merkityksessä ’suorittaa’) paikassa, jossa rikoksentekijä todella toimii, kun taas niiden vaikutukset

kohdetietojärjestelmiin voivat tapahtua jossain muualla, 12 artiklassa säädetään velvollisuuksista ulottaa **lainkäyttövaltaa** seuraavien asioiden perusteella:

- alue, jossa rikoksentekijä on fyysisesti läsnä rikoksen tehdessään,
- kohdetietojärjestelmän sijainti,
- rikoksentekijän kansalaisuus,
- hänen asuinpaikkansa ja
- sen oikeushenkilön sijoittautumispaikka, jonka hyväksi rikos on tehty.

Mitä tulee tietojenvaihtoon, 13 artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että niillä on toimiva kansallinen **yhteyspiste** käytettävissä ympärivuorokautisesti ja kaikkina viikonpäivinä, jotta ne voivat vastata kiireellisiin ulkomailta tuleviin avunpyyntöihin 8 tunnin kuluessa.

Lisäksi jäsenvaltioiden on toteutettava tarvittavat toimenpiteet, joilla **helpotetaan** edellä mainituista rikoksista **ilmoittamista** kansallisille toimivaltaisille viranomaisille (13 artiklan 3 kohta) ja kerätään ja jaetaan vähimmäismäärä **tilastotietoa** näistä rikoksista (14 artikla).

1.2 Kertomuksen tarkoitus ja menetelmät

Direktiivin 16 artiklassa edellytetään, että jäsenvaltiot saattavat voimaan direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset 4. syyskuuta 2015 mennessä ja toimittavat ne komissiolle.

Tällä kertomuksella vastataan direktiivin 17 artiklan vaatimukseen, jonka mukaan komission on annettava Euroopan parlamentille ja neuvostolle kertomus, jossa arvioidaan, missä määrin jäsenvaltiot ovat toteuttaneet direktiivin noudattamiseksi tarvittavat toimenpiteet. Kertomuksessa on siis tarkoitus antaa tiivis mutta informatiivinen katsaus tärkeimmistä toimenpiteistä, joilla jäsenvaltiot ovat saattaneet direktiivin osaksi kansallista lainsäädäntöään.

Kansallisen lainsäädännön osaksi saattamiseen kuului tietojen kerääminen asiaan kuuluvista säädöksistä ja hallinnollisista toimenpiteistä, tietojen analysointi sekä uuden lainsäädännön laatiminen tai – useimmissa tapauksissa – olemassa olevien säädösten muuttaminen, prosessin läpivienti lainsäädännön hyväksymiseen saakka ja lopulta raportointi komissiolle.

Määräaikaan mennessä 22 jäsenvaltiota oli ilmoittanut komissiolle saattaneensa direktiivin kokonaan osaksi lainsäädäntöään. Marraskuussa 2015 komissio aloitti rikkomusmenettelyt kansallisten täytäntöönpanotoimien ilmoittamatta jättämisestä viittä jäljellä olevaa jäsenvaltiota vastaan. Nämä maat olivat BE, BG, EL, IE ja SI.[5] Toukokuun 31. päivänä 2017 rikkomusmenettelyt kansallisten täytäntöönpanotoimien ilmoittamatta jättämisestä olivat vielä vireillä BE:n, BG:n ja IE:n kanssa.[6]

Tässä kertomuksessa esitetty kuvaus ja analyysi perustuvat jäsenvaltioiden 31. toukokuuta 2017 mennessä toimittamiin tietoihin.[7] Mainitun päivämäärän jälkeen vastaanotettuja

[5] Jäsenvaltioista käytetään tässä asiakirjassa lyhenteitä osoitteessa http://publications.europa.eu/code/fi/fi-5000600.htm esitetyn taulukon mukaisesti.

[6] Tietoa komission rikkomusmenettelyä koskevista päätöksistä on saatavilla osoitteessa http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=fi.

[7] IE ilmoitti 31. toukokuuta 2017, että direktiivi oli pantu täysimääräisesti täytäntöön.

ilmoituksia ei ole otettu huomioon. Huomioon on otettu kaikki ilmoitetut kansallista lainsäädäntöä koskevat toimenpiteet ja niiden lisäksi oikeuden päätökset sekä – soveltuvin osin – yleinen oikeusteoria. Lisäksi komissio otti analyysin aikana suoraan yhteyttä jäsenvaltioihin silloin, kun oli tarpeen ja asianmukaista saada lisätietoja tai selvennyksiä. Kaikki kerätyt tiedot otettiin analyysia varten huomioon.

Tässä kertomuksessa mainittujen asioiden lisäksi direktiiviin saattamiseen osaksi kansallista lainsäädäntöä voi liittyä muita haasteita tai muita säännöksiä, joista ei ole raportoitu komissiolle, tai tulevaisuuden lainsäädännön kehitystä tai muuhun kuin lainsäädäntöön liittyvää kehitystä. Siksi kertomus ei estä komissiota arvioimasta edelleen joitakin säännöksiä ja jatkamasta jäsenvaltioiden tukemista direktiivin saattamisessa osaksi kansallista lainsäädäntöä ja sen täytäntöönpanossa.

2. Toimenpiteet direktiivin saattamiseksi osaksi kansallista lainsäädäntöä

2.1 Oikeudelliset määritelmät (direktiivin 2 artikla)

Direktiivin 2 artiklassa annetaan oikeudelliset määritelmät termeille ’tietojärjestelmä’ (a alakohta), ’data’ (b), ’oikeushenkilö’ (c) ja ilmaisulle ’oikeudettomasti’ (d). Vain CY ja UK (Gibraltar) ovat antaneet lainsäädäntöä, joka kattaa edellä mainitut määritelmät kokonaisuudessaan. Yksityiskohtaisesti tämä tarkoittaa seuraavaa:

a) Tietojärjestelmä

Direktiivin määritelmä perustuu Budapestin yleissopimuksen 1 artiklan a alakohdassa annettuun määritelmään termille ’tietojärjestelmä’, ja siinä lisätään itse data tietojärjestelmän osaksi. CY, EL, IE, FI, HR, MT, PT ja UK (Gibraltar) ovat antaneet oikeudellisia säännöksiä, joihin sisältyy tietojärjestelmän määritelmä, kun taas jäsenvaltioiden DE, ES, F, LU, LV, PL, SE ja SK ilmoittamat tiedot eivät olleet tyhjentävät. Jäljellä olevien jäsenvaltioiden AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI ja UK (Gibraltaria lukuun ottamatta) vastaavissa oikeudellisissa määritelmissä ei erikseen mainita ’dataa’. Tämä merkitsee viittausta Budapestin yleissopimuksen 1 artiklan a alakohtaan, jonka määritelmä tietojärjestelmälle on yhtä kattava.

b) Data

Termi ’data’ määritellään jäsenvaltioiden AT, BG, CY, CZ, DE, EE, EL IE, FI, HR, LT, MT, NL, PT, RO ja UK (Gibraltar) lainsäädännössä, kun taas jäsenvaltioiden ES, FR, IT, LU, LV, PL, SE, SK ja UK (Gibraltaria lukuun ottamatta) ilmoittamat tiedot eivät olleet tyhjentävät. Kuitenkin SE:n tapauksessa erityisesti määritelmään viittaaviin artikloihin viittaaminen tekee määritelmästä tarpeettoman. Mitä tulee muihin jäsenvaltioihin, HU viittaa datan määritelmään vain direktiivin 4 ja 5 artiklassa mainittujen rikosten yhteydessä, kun taas sekä BE:ltä että SI:ltä puuttuu datan määritelmästä kokonaan maininta ”ohjelmasta, jonka avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon”.

c) Oikeushenkilö

Lukuun ottamatta LU:ta, joka ei ilmoittanut tyhjentävää tietoa 2 artiklan c alakohdan saattamisesta osaksi kansallista lainsäädäntöä, ’oikeushenkilön’ määritelmän saattaminen osaksi kansallista lainsäädäntöä ei aiheuttanut ongelmia. Tämä johtuu siitä, että se löytyy yleisesti jo jäsenvaltioiden siviili- ja kauppaoikeussäännöksistä. Vain CY:llä on direktiivin täytäntöönpanotoimissa sitä koskeva erityissäännös.

d) Oikeudettomasti
Mitä tulee 2 artiklan d alakohdan ilmaisun ’oikeudettomasti’ määritelmään, vain CY, IE, RO ja UK (Gibraltar) ilmoittivat sen saattamisesta osaksi kansallista lainsäädäntöä, kun taas 23 jäsenvaltiolta tätä määritelmää koskevat täytäntöönpanotoimet puuttuivat kokonaan. On kuitenkin todettava, että kaikissa jäsenvaltioissa on yleinen periaate, jonka mukaan rikosoikeudellista vastuuta ei synny toimista, joiden tekemiseen on ollut asianmukainen lupa.

2.2 Määritellyt rikokset (direktiivin 3–7 artikla)

a) Laiton tunkeutuminen tietojärjestelmään
Direktiivin 3 artikla, joka viittaa laittomaan tunkeutumiseen tietojärjestelmään, on katettu jäsenvaltioiden AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE ja SK lainsäädännössä.

Muiden jäsenvaltioiden (BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI ja UK) kohdalla vastaava kansallinen rikoskuvaus ei tee eroa sen välillä, onko kyse tunkeutumisesta koko tietojärjestelmään vai osaan siitä, vaikka tästä on nimenomaisesti direktiivissä säädetty. Lisäksi DE:n täytäntöönpano ei kata yksinkertaista tietokonelaitteistoihin tunkeutumista, ja AT ja LU mainitsevat erityistä tarkoitusperää (tarkoitus saada tietoa tai tehdä haittaa tai vilpillinen tarkoitusperä) koskevia lisävaatimuksia ja LV merkittävää haittaa koskevia lisävaatimuksia. Jäsenvaltioiden BE, BG, FR, HR, LU, MT, PT, RO, SI ja UK tapauksessa kansallisten säännösten soveltamisala on laajempi kuin direktiivin, sillä näissä säännöksissä rikosoikeudellinen vastuun syntyminen ei edellytä minkään turvatoimenpiteen kiertämistä. Muut jäsenvaltiot viittaavat joko kirjaimellisesti siihen, että turvatoimenpiteen kiertäminen kuuluu rikoksen tunnusmerkistöön (CY, EL ja SK) tai käyttävät samantyyppistä terminologiaa kuvaamaan tätä näkökohtaa (AT, CZ, DE, EE, ES, FI, HU, IT, LT, LV, NL, PL ja SE).

b) Laiton järjestelmän häirintä
Direktiivin 4 artiklassa viitataan laittomaan järjestelmän häirintään. Direktiivissä luetellaan kahdeksan mahdollista toimea (datan syöttö, siirtäminen, vahingoittaminen, tuhoaminen, turmeleminen, muuttaminen, poistaminen tai saattaminen käyttökelvottomaksi) ja kaksi mahdollista mainitun toimen seurausta (tietojärjestelmän toiminnan vakava estäminen tai keskeyttäminen). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE ja UK (Gibraltaria lukuun ottamatta) ovat antaneet direktiiviä vastaavat lainsäädäntötoimet. BG viittaa ainoastaan viruksen syöttämiseen, kun taas loput jäsenvaltiot (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK ja UK) jättävät erikseen mainitsematta 1–4 mahdollista toimea. Tässä yhteydessä voidaan havaita, että useimmat ongelmat koskivat termejä ’turmeleminen’ (puuttui 8 tapauksessa) ja ’saattaminen käyttökelvottomaksi’ (puuttui 9 tapauksessa).

c) Laiton datan vahingoittaminen
Direktiivin 5 artikla kattaa laittoman datan vahingoittamisen ja siinä luetellaan kuusi mahdollista toimea: datan tuhoaminen, vahingoittaminen, turmeleminen, muuttaminen, poistaminen tai saattaminen käyttökelvottomaksi. CY, EL, IE ja MT ovat saattaneet säännöksen kirjaimellisesti osaksi lainsäädäntöään; BE, CZ, LT, PT ja SE käyttivät yleisluontoisempia termejä kattamaan kaikki mahdolliset toimet. Muiden jäsenvaltioiden täytäntöönpanotoimet eivät kata jokaista mahdollisuutta, vaan viittaavat vain viiteen vaihtoehtoon (FI ja SK) tai vieläkin harvempiin (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL, RO, SI ja UK). Useimmat ongelmat koskivat termejä ’vahingoittaminen’ (puuttui 8 kertaa), ’turmeleminen’ (13 kertaa), ’poistaminen’ (11 kertaa) ja ’saattaminen käyttökelvottomaksi’ (13 kertaa). FI täydentää direktiivin sanamuotoa vaatimuksella, jonka

mukaan rikosoikeudellisen vastuun syntyminen edellyttää, että ”aikomuksena on tuottaa haittaa tai taloudellista vahinkoa”, kun taas LT ja LV edellyttävät, että ”toimesta aiheutuu suurta vahinkoa tai merkittävää haittaa”.

d) Viestintäsalaisuuden loukkaus (tietojen laiton hankkiminen)
Direktiivin 6 artiklassa viitataan tietojen laittomaan hankkimiseen, ja artikla keskittyy luottamukselliseen datan siirtämiseen ja dataa sisältävästä tietojärjestelmästä lähtevään sähkömagneettiseen säteilyyn. CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK ja UK (Gibraltar) ovat antaneet lainsäädäntöä, joka kattaa täysin 6 artiklan. Direktiivin yleinen datan hankkimiseen liittyvä soveltamisala rajoittuu viesteihin (AT ja BG), henkilön tarkkailuun (EE) tai tiedonvaihtoon (FR ja HU). Lisäksi seuraavien jäsenvaltioiden täytäntöönpanotoimet eivät kata sähkömagneettista säteilyä: BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI ja UK (Gibraltaria lukuun ottamatta). Eräät jäsenvaltiot myös edellyttävät erityistä tarkoitusperää (kuten tiedonsaantia, taloudellista hyötyä tai haitan aiheuttamista – ks. AT, EL, HU) tai erityisiä lisätoimia (esimerkiksi tallettaminen tai saadun tiedon salaisen luonteen tiedostaminen – ks. BG ja HU).

e) Rikosten tekemiseen käytettävät välineet
Direktiivin 7 artiklassa säädetään rangaistavaksi lukuisia toimia, joissa 3–6 artiklassa mainittujen rikosten tekemiseen käytetään jotakin välinettä, kuten tietokoneohjelmia tai tunnuslukuja. Rangaistavia toimia ovat tällaisten välineiden tuottaminen, myynti, käyttöön hankkiminen, tuonti, jakelu ja muu saataville asettaminen. AT BE, CY, DE, EL, IE ja SK ovat antaneet vastaavaa kansallista lainsäädäntöä. Jotkin jäsenvaltiot eivät kata kaikkia mainittuja rikoksia (EE, IT, MT, PL ja SI). Toiset taas eivät viittaa 7 artiklan tekijään 3–6 artiklassa mainittujen rikosten mukaisesta rikoksentekijästä poikkeavana henkilönä (CZ ja SI). Eräät edellyttävät erityistä tarkoitusperää (vahingon tuottaminen tai vilpillinen toiminta – ks. FI, IT ja LU), tiettyä seurausta, kuten salassapitovelvollisuuden loukkaamista (BG) tai ainakin mainittujen rikkomusten valmistelua (SE). Lopulta 7 artiklan täytäntöönpanossa löytyi puutteita kaikkien lueteltujen toimien osalta. Näin asia oli jäsenvaltioiden BG, CZ, EE, ES, FR, HR, HU, IT, LT, LU, LV, PL, PT, RO, SI ja UK kohdalla. Näistä LU:n lainsäädännössä mainitaan erikseen viisi kuudesta direktiivissä luetellusta mahdollisesta toimesta, kun taas muut jäsenvaltiot viittaavat selkeästi vain neljään tai harvempaan.

Käyttöön hankkiminen on saatettu osaksi vain ES:n kansallista lainsäädäntöä.

2.3 Mainittuja rikoksia koskevat yleiset säännöt (direktiivin 8–12 artikla)

a) Yllytys ja avunanto
Direktiivin 8 artiklan 1 kohdassa edellytetään jäsenvaltioiden varmistavan, että yllytys ja avunanto 3–7 artiklassa tarkoitettujen rikosten tekemiseen on rikosoikeudellisesti rangaistava teko. Kaikki jäsenvaltiot ovat saattaneet tämän säännöksen osaksi kansallista lainsäädäntöään.

b) Yritys
Direktiivin 8 artiklan 2 kohdan mukaan 4–5 artiklassa tarkoitettujen rikosten yrittäminen on rikosoikeudellisesti rangaistava teko. PT ei kata kaikenlaisia yrityksiä tehdä 4 artiklassa tarkoitettuja rikoksia ja SE:lta puuttuu rikosoikeudellinen vastuu ”viestintäsalaisuuden rikkomisen” yrittämisestä, mutta muilla jäsenvaltioilla on voimassa lainsäädäntöä, jolla tämä säännös on pantu täytäntöön.

c) Seuraamukset
aa) Yleinen säännös

Direktiivin 9 artiklan 1 kohta edellyttää, että jäsenvaltiot ottavat yleisesti käyttöön direktiivin kattamista rikoksista määrättävät tehokkaat, oikeasuhteiset ja varoittavat rikosoikeudelliset seuraamukset. Vaikka näin on tehty lähes kaikissa jäsenvaltioissa, AT, BE, BG, IT, PT, SE ja SI eivät täytä enimmäisrangaistusten vähimmäistasoja, joista säädetään kaikkien tapausten osalta 9 artiklan 2 kohdassa (ks. kohta 1.1 edellä). Tämä vaikuttaa 9 artiklan 1 kohdan saattamiseen osaksi kansallista lainsäädäntöä, sillä voidaan päätellä, että 9 artiklan 2 kohdan vähimmäisvaatimukset edustavat vähimmäistasoa sille, että rikosoikeudelliset seuraamukset ovat tehokkaita, oikeasuhteisia ja varoittavia.

bb) Enimmäisrangaistuksen yleinen vähimmäistaso

Direktiivin 9 artiklan 2 kohdan mukaisesti enimmäisrangaistuksen vähimmäistaso on 3–7 artiklassa tarkoitetuissa tavanomaisissa rikoksissa kahden vuoden pituinen vankeusrangaistus. Useimmat jäsenvaltiot ovat panneet tämän säännöksen täytäntöön. Vain kuuden jäsenvaltion kohdalla on joitakin eroavaisuuksia: AT (kuuden kuukauden pituinen enimmäisvankeusrangaistus), BG (yhden vuoden pituinen enimmäisvankeusrangaistus kaikista rikoksista paitsi viestintäsalaisuuden loukkaamisesta), IT (yhden vuoden pituinen enimmäisvankeusrangaistus 7 artiklan b alakohdan rikoksesta), PT (yhden vuoden pituinen enimmäisvankeusrangaistus 3 artiklan rikoksesta), SE (yhden vuoden pituinen enimmäisvankeusrangaistus rikoksesta ”vahingon tuottaminen”) ja SI (yhden vuoden pituinen enimmäisvankeusrangaistus 3, 6 ja 7 artiklan rikoksista). BE:n tapauksessa 3, 6 ja 7 artiklan enimmäisrangaistuksen vähimmäistaso saavutetaan vain, kun rikokset tehdään petollisin tarkoitusperin.

cc) Rikos vaikuttanut merkittävään määrään tietojärjestelmiä

Direktiivin 9 artiklan 3 kohdassa nostetaan enimmäisrangaistuksen vähimmäistaso kolmeen vuoteen vankeutta, kun 4 ja 5 artiklassa tarkoitettu rikos on vaikuttanut merkittävään määrään tietojärjestelmiä. Yleisesti ottaen jäsenvaltiot ovat antaneet vastaavaa lainsäädäntöä, joskin DE viittaa vain tietojärjestelmiin, ”joilla on huomattavaa merkitystä toisilleen”, FI edellyttää, että rikosta arvioidaan ”kokonaisuutena” korkeamman rangaistuksen soveltamiseksi, ja LV ei viittaa huomattavaan määrään tietojärjestelmiä (tai vastaavaan sanamuotoon), vaan ainoastaan ”huomattavan haitan” aiheuttamiseen. BG ja SI eivät ilmoittaneet tyhjentäviä tietoja.

dd) Rikollisjärjestöt

Direktiivin 9 artiklan 4 kohdan a alakohdan mukaan vähintään viiden vuoden pituista enimmäisvankeusrangaistusta tulisi soveltaa 4 ja 5 artiklassa tarkoitettuihin rikoksiin, kun tekijänä on puitepäätöksessä 2008/841/YOS määritelty rikollisjärjestö.

Tässäkin tapauksessa suurin osa jäsenvaltioista on saattanut 9 artiklan 4 kohdan a alakohdan osaksi kansallista lainsäädäntöään. LU:n ja SI:n rikoslainsäädännössä rikollisjärjestöjen tekemiä rikoksia koskevat säännökset eivät kata kyberrikoksia. BE:n lainsäädännössä säädetään vain kolmen vuoden enimmäisvankeusrangaistuksesta 5 artiklassa tarkoitetuista rikoksista, DE:n lainsäädäntö ei kata luonnollisia henkilöitä näiden rikosten uhreina, FI:n lainsäädäntö edellyttää rikoksen lisäarviointia ”kokonaisuutena” ja SE:n lainsäädännössä säädetään neljän vuoden enimmäisvankeusrangaistuksesta, joka määrätään ”suuren vahingon aiheuttamisesta”.

ee) Vakavan vahingon aiheuttaminen

Direktiivin 9 artiklan 4 kohdan b alakohdassa enimmäisvankeusrangaistuksen vähimmäispituudeksi määritetään viisi vuotta mistä tahansa 4 ja 5 artiklassa tarkoitetuista rikoksista, jos siitä on aiheutunut vakavaa vahinkoa. Vaikka vakavaa vahinkoa ei olekaan määritelty, kaikki jäsenvaltiot paitsi BG, DE, FI, HU, LU ja SE ovat antaneet direktiiviä

vastaavaa lainsäädäntöä. HU ei ilmoittanut tyhjentäviä tietoja. BG ei saavuta viiden vuoden enimmäisrangaistuksen vähimmäisvaatimusta, kun taas LU viittaa yleiseen vakavan vahingon aiheuttamista koskevaan rangaistuslausekkeeseen, joka ei kata mitään kyberrikoksia. Lainsäädännössä on pieniä eroavaisuuksia jäsenvaltioissa DE (lainsäädäntö ei kata luonnollisia henkilöitä rikosten uhreina), FI (korkeampiin rangaistuksiin edellytetään rikoksen lisäarviointia ”kokonaisuutena”) ja SE (neljän vuoden enimmäisvankeusrangaistus ”suuren vahingon aiheuttamisesta”).

ff) Elintärkeän infrastruktuurin tietojärjestelmät

Viiden vuoden enimmäisvankeusrangaistuksen vähimmäisvaatimusta sovelletaan myös, jos 4 ja 5 artiklassa mainittu rikos koskettaa elintärkeiden infrastruktuurien tietojärjestelmiä, kuten 9 artiklan 4 kohdan c alakohdassa ilmaistaan.

Suurin osa jäsenvaltioista on antanut tätä säännöstä vastaavaa lainsäädäntöä, mutta BG ei ilmoittanut erityisesti täytäntöönpanoa koskevaa tietoa. BE on asettanut kolmen vuoden pituisen enimmäisrangaistuksen 5 artiklan rikoksille. DE ei ota uhreina huomioon luonnollisia henkilöitä. FI edellyttää rikoksen lisäarviointia ”kokonaisuutena”, IT edellyttää rikoksen aiheuttavan ”tuhoa”, PT edellyttää, että hyökkäys tapahtuu ”vakavalla ja pitkäaikaisella tavalla” eikä viittaa 5 artiklaan, ja SE täyttää direktiivin vaatimuksen vain ”suurta tuhoa” aiheuttavien rikosten osalta.

gg) Henkilöllisyysvarkaus ja muut henkilöllisyyteen liittyvät rikokset

Direktiivin 9 artiklan 5 kohdassa edellytetään jäsenvaltioiden varmistavan, että jos 4 ja 5 artiklassa tarkoitetut rikokset on tehty käyttämällä väärin toisen henkilön henkilötietoja tarkoituksena voittaa kolmannen osapuolen luottamus ja aiheuttaen näin vahinkoa henkilöllisyyden oikealle omistajalle, tätä voidaan kansallisen lain mukaisesti pitää raskauttavana asianhaarana, jolleivät nämä asianhaarat jo kuulu jonkin muun rikoksen tunnusmerkistöön. Laaja harkintavalta on johtanut laajaan täytäntöönpanotoimien skaalaan jäsenvaltioiden välillä. BE ja EL eivät ole ilmoittaneet täytäntöönpanosta, eikä CZ:n rikoslainsäädännössä ole tätä koskevia erillissäännöksiä. Raskauttamisnäkökulman ovat valinneet AT, CY, ES, IE, MT, PT ja SE (viimeksi mainittu viittaa ”erityisen suunnittelun” asianhaaraan), kun taas kaikki muut jäsenvaltiot viittaavat tätä erityistä rikosta koskeviin lisäsäännöksiin. Erityissäännöksiin viittaavien jäsenvaltioiden täytäntöönpano-ongelmissa on havaittavissa seuraavaa: BG ja NL edellyttävät erityistä tarkoitusperää (”hyödyn hankkiminen” ja ”tarkoitus tekeytyä toiseksi tai väärinkäyttää henkilöllisyyttä”), DE viittaa vain ”henkilökohtaisiin tietoihin, jotka eivät ole yleisesti saatavilla”, FR viittaa ainoastaan henkilön nimeen eikä muihin henkilötietoihin, LV edellyttää, että rikos aiheuttaa ”huomattavaa haittaa”, RO kattaa vain ”asiakirjan” käytön ja edellyttää petoksen tapahtumista.

d) Oikeushenkilöiden vastuu

aa) Yleisesti

Direktiivin 10 artiklan 1 kohdassa edellytetään, että oikeushenkilö voidaan saattaa vastuuseen 3–8 artiklassa tarkoitetuista rikoksista, jos rikoksentekijällä on oikeus edustaa oikeushenkilöä (a alakohta), valtuus tehdä päätöksiä oikeushenkilön puolesta (b) tai valtuus harjoittaa valvontaa oikeushenkilössä (c). Kaikki jäsenvaltiot ovat antaneet artiklaa vastaava lainsäädäntöä, ja täytäntöönpanossa on vain pieniä puutteita: BG ei kata 6 artiklan rikosta ja HR ei viittaa siihen, että rikoksentekijällä olisi valtuus harjoittaa valvontaa oikeushenkilössä (10 artiklan 1 kohdan c alakohta).

bb) Ohjauksen tai valvonnan puutteellisuuden vuoksi

Direktiivin 10 artiklan 2 kohdassa edellytetään, että jäsenvaltiot voivat saattaa oikeushenkilön vastuuseen, kun mikä tahansa 3–8 artiklassa tarkoitettu rikos on johtunut 10 artiklan 1 kohdassa tarkoitetun henkilön harjoittaman ohjauksen tai valvonnan puutteesta. Lähes kaikki jäsenvaltiot noudattavat tätä säännöstä, mutta LU ei ilmoittanut tyhjentäviä tietoja ja BG ei viittaa 6 artiklan mukaisen rikoksen tekemiseen.

e) Oikeushenkilöille määrättävät seuraamukset

aa) Pakolliset seuraamukset

Direktiivin 11 artiklan 1 kohdassa edellytetään, että jäsenvaltiot säätävät rikosoikeudellisista ja muista sakoista tehokkaina, oikeasuhteisina ja varoittavina seuraamuksina oikeushenkilöille. Kaikki jäsenvaltiot paitsi IE ja UK ovat ilmoittaneet kansallisista täytäntöönpanotoimistaan. Näissä kahdessa maassa mahdollisten sakkojen enimmäismäärää ei ole määritelty, sillä konkreettisia säännöksiä puuttuu. Siksi sakkojen tehokkuutta, oikeasuhteisuutta tai varoittavuutta ei voida arvioida.

bb) Valinnaiset seuraamukset

Direktiivin 11 artiklan 1 kohdassa luetellaan lisäksi mahdollisia vaihtoehtoja oikeushenkilöihin kohdistuville lisärangaistuksille. Näitä ovat: oikeuden menettäminen julkisista varoista myönnettäviin etuuksiin tai tukiin (tämän valitsivat CY, CZ, EL, ES, HR, HU, LU, MT, PL, PT ja SK), väliaikainen tai pysyvä kielto harjoittaa liiketoimintaa (AT, BE, CY, CZ, EL, ES FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI ja SK), tuomioistuimen valvontaan asettaminen (CY, ES, FR, MT, PT ja RO), tuomioistuimen määräys purkaa oikeushenkilö (CY, CZ, EL, ES, FR, HR, HU, LT, LU, LV, MT, PT, RO, SI ja SK) ja rikoksen tekemiseen käytettyjen tilojen sulkeminen väliaikaisesti tai pysyvästi (BE, CY, WS, FR, LT, MT, PT ja RO). BG, DE, EE, IE, FI, NL ja UK eivät siis valinneet vaihtoehdoista yhtäkään.

cc) Seuraamukset laiminlyönneistä

Direktiivin 11 artiklan 2 kohdan mukaan jäsenvaltioiden on varmistettava, että 10 artiklan 2 kohdassa tarkoitettuihin laiminlyöntirikoksiin syyllistyneisiin oikeushenkilöihin sovelletaan tehokkaita, oikeasuhteisia ja varoittavia seuraamuksia. LU ei ilmoittanut tyhjentäviä tietoja. Kaikki muut jäsenvaltiot paitsi IE ja UK toimittivat vastaavat oikeudelliset säännöksensä. IE:n ja UK:n tapauksessa puutteet olivat samat kuin 11 artiklan 1 kohdan tapauksessa: (ks. kohta aa) edellä).

f) Lainkäyttövalta

aa) Vaaditut lainkäyttövallan perusteet

Direktiivin 12 artiklan 2 ja 3 kohdassa jäsenvaltioita edellytetään ulottamaan oma lainkäyttövaltansa 3–8 artiklassa tarkoitettuihin rikoksiin, kun rikos tehdään kokonaan tai osittain jäsenvaltion alueella – joko niin, että rikoksentekijä on siellä fyysisesti rikoksen tekoaikaan, tai niin, että rikos kohdistuu jäsenvaltion alueella sijaitsevaan tietojärjestelmään – tai jos rikos on tapahtunut ulkomailla, mutta tekijä on ollut jäsenvaltion kansalainen. Useimmat jäsenvaltiot ovat antaneet vastaavaa kansallista lainsäädäntöä; IT:n lainsäädännössä ei määritetä lainkäyttövaltaa, kun kansalainen on ulkomailla tavallisten rikosten tapauksessa, LV:n ja SI:n lainsäädäntö viittaa epäselviin alueellisiin näkökohtiin liittyviin säännöksiin, MT:n lainsäädäntö, joka koskee rikoksen osittaista tapahtumista omalla alueella, on epäselvä, ja UK viittaa tietokoneeseen tietojärjestelmän sijasta.

bb) Muut lainkäyttövallan perusteet

Direktiivin 12 artiklan 3 kohdassa määrätään, että jos jäsenvaltiot ulottavat lainkäyttövaltansa tapauksiin, joissa rikoksentekijän vakinainen asuinpaikka on sen alueella (tämän valitsivat

AT, CY, CZ, IE, FI, HR, LT, LV, NL, SE ja SK) tai jos rikos on tehty sen alueelle sijoittautuneen oikeushenkilön hyväksi (CY, CZ, LV, PT, RO ja SK), tästä tulisi ilmoittaa komissiolle.

2.4 Käytännön kysymykset (direktiivin 13–14 artikla)

a) Kansallisten yhteyspisteiden järjestäminen
Direktiivin 13 artiklan 1 kohdassa kehotetaan jäsenvaltioita luomaan toimiva kansallinen yhteyspiste 3–8 artiklassa tarkoitettuja rikoksia koskevaa tietojenvaihtoa varten. Säännöksen nojalla jäsenvaltioiden on varmistettava, että käyttöön otetaan sellaiset menettelyt, joiden avulla toimivaltainen viranomainen voi vastata kiireellisiin avunpyyntöihin kahdeksan tunnin kuluessa pyynnön saamisesta. Ilmoitettujen tietojen mukaan useimmat jäsenvaltiot ovat perustaneet tarvittavat rakenteet. IE ja RO mainitsivat, että niiden yhteyspisteet ovat käytettävissä vain rajoitettuina aikoina joka päivä, mikä ei mahdollistaisi viranomaisen reagointia kahdeksan tunnin kuluessa pyynnöstä jokaisessa tapauksessa. Useat jäsenvaltiot ilmoittivat, että ne ottavat käyttöön olemassa olevia yhteyspisteiden välisiä verkostoja, jotka on perustettu G7-verkoston kautta tai Euroopan neuvoston kyberrikollisuutta koskevan Budapestin yleissopimuksen puitteissa.

b) Tietoa vakiintuneista kansallisista yhteyspisteistä
Direktiivin 13 artiklan 2 kohdan mukaisesti jäsenvaltioiden on toimitettava yhteyspisteidensä yhteystiedot komissiolle, joka toimittaa tiedot edelleen muille jäsenvaltioille. Kaikki jäsenvaltiot ovat toimittaneet tarvittavat tiedot.

c) Ilmoituskanavat
Direktiivin 13 artiklan 3 kohdan mukaan jäsenvaltioiden on varmistettava, että käyttöön otetaan asianmukaiset ilmoituskanavat, joilla helpotetaan 3–6 artiklassa tarkoitetuista rikoksista ilmoittamista toimivaltaisille kansallisille viranomaisille. HR, IT, IE ja PT eivät ilmoittaneet tyhjentäviä tietoja. Mitä tulee muihin jäsenvaltioihin, ilmoituskanavien toteuttamiseen näyttää olevan erilaisia lähestymistapoja. Useimmat jäsenvaltiot (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK ja UK) ovat ilmoittaneet sellaisia kanavia koskevista toimenpiteistä, jotka tekevät ilmoittamisesta helpompaa asiasta alun perin raportoivalle henkilölle tai organisaatioille, esimerkiksi kyberhyökkäyksen uhrille (LV:n ilmoittamat tiedot itse ilmoituskanavasta olivat epäselvät). Muut jäsenvaltiot (AT, ES ja LU) kuitenkin ilmoittivat täsmälleen samat tiedot kuin 13 artiklan 1 ja 2 kohdan täytäntöönpanon osalta, mikä antaa sen vaikutelman, että toimenpiteet helpottavat lähinnä viranomaisten välistä viestintää.

d) Tilastotietojen kerääminen
Direktiivin 14 artiklan 1 ja 2 kohdan mukaan jäsenvaltioiden on varmistettava, että niillä on järjestelmä, jonka avulla voidaan kirjata, tuottaa ja antaa tilastotietoja vähintään 3–7 artiklassa tarkoitettujen, jäsenvaltioiden rekisteröimien rikosten lukumäärästä ja näistä rikoksista syytteeseen asetettujen ja tuomittujen henkilöiden lukumäärästä. Saatujen ilmoitusten perusteella useimmat jäsenvaltiot näyttävät ottaneen käyttöön sekä lainsäädännöllisiä että hallinnollisia toimia varmistaakseen tiedon keräämisen, yleensä yleisen, kansallisen sähköisen järjestelmän keinoin. Monet jäsenvaltiot eivät ilmoittaneet tyhjentäviä tietoja (EL, IE, UK (Gibraltar, Pohjois-Irlanti ja Skotlanti)). Yksi syy tähän oli, että direktiivin tarkoittamia yksittäisiä rikoksia koskevia tietoja ei voida kerätä erikseen (BE, DE, ja SE) tai kerätty tieto ei kata kaikkia direktiivin tarkoittamia rikoksia (RO).

e) Tilastotietojen siirtäminen komissiolle
Direktiivin 14 artiklan 3 kohdassa kehotetaan jäsenvaltioita ilmoittamaan mainitut tilastotiedot komissiolle. Kaikki jäsenvaltiot, jotka ilmoittivat toimenpiteistä, paitsi UK (Gibraltar, Pohjois-Irlanti ja Skotlanti) ja HU, ovat vahvistaneet ottaneensa velvoitteen täytäntöönpanemiseksi käyttöön joko oikeudellisia tai hallinnollisia toimenpiteitä tai molempia. EL, ES, LU ja SI eivät ilmoittaneet tyhjentäviä tietoja.

3. Päätelmät ja jatkotoimet

Direktiivi on johtanut huomattavaan edistykseen siinä, että kyberhyökkäysten kriminalisointi on kaikissa jäsenvaltioissa vertailukelpoisella tasolla, mikä helpottaa tämäntyyppisiä rikoksia tutkivien lainvalvontaviranomaisten rajatylittävää yhteistyötä. Jäsenvaltiot ovat tarkistaneet rikoslakejaan ja muuta asiaan kuuluvaa lainsäädäntöä, virtaviivaistaneet menettelyjä ja perustaneet tai parantaneet yhteistyöhankkeita. Komissio tunnustaa jäsenvaltioiden suuret pyrkimykset saattaa tämä direktiivi osaksi kansallista lainsäädäntöään.

Direktiivin koko potentiaali voitaisiin kuitenkin saada paljon paremmin käyttöön, jos kaikki jäsenvaltiot toteuttaisivat kaikki sen säännökset kokonaisuudessaan. Tähänastisen analyysin perusteella tärkeimpiä parannuksia, jotka jäsenvaltioiden on saatava aikaan, on määritelmien käyttö (2 artikla), jolla on vaikutusta siihen, miten laajasti rikokset direktiivin perusteella kansallisessa lainsäädännössä määritellään. Lisäksi vaikuttaa siltä, että jäsenvaltioille on ollut haastavaa sisällyttää lainsäädäntöönsä kaikki rikoksiin liittyviä toimia määrittelevät mahdollisuudet (3–7 artikla) ja kyberhyökkäyksistä määrättäviä rangaistuksia (9 artikla) koskevat yhteiset normit. Muut ongelmat vaikuttavat liittyvän asianmukaisia ilmoituskanavia koskevien hallinnollisten säännösten täytäntöönpanoon (13 artikla 3 kohta) sekä direktiivissä mainittujen rikosten seurantaan ja tilastointiin (14 artikla).

Komissio jatkaa jäsenvaltioiden tukemista direktiivin täytäntöönpanossa. Mahdollisen rajatylittävää yhteistyötä koskevan panoksen näkökulmasta tällä tarkoitetaan erityisesti direktiivin toiminnallisia säännöksiä, jotka koskevat tietojenvaihtoa (13 artiklan 1 ja 2 kohta), ilmoituskanavia (13 artiklan 3 kohta) ja seurantaa ja tilastointia (14 artikla). Tähän liittyen komissio antaa jäsenvaltioille uusia mahdollisuuksia tunnistaa ja vaihtaa parhaita käytäntöjä vuoden 2017 loppupuolella.

Komissio ei pidä tällä hetkellä tarpeellisena ehdottaa direktiiviin muutoksia. Yhtenä tavoitteenaan tukea rikostutkintaa, joka koskee tietojärjestelmiin kohdistuvia hyökkäyksiä, kyberrikoksia ja muuntyyppisiä rikoksia, komissio harkitsee tässä yhteydessä toimenpiteitä, joilla parannetaan sähköisen todistusaineiston rajatylittävää saatavuutta rikostutkinnan yhteydessä, ja ehdottaa lainsäädäntötoimia vuoden 2018 alkuun mennessä.[8] Komissio harkitsee myös salauksen roolia rikostutkinnassa ja raportoi havainnoistaan viimeistään lokakuussa 2017.[9]

Komissio on sitoutunut varmistamaan, että direktiivi saatetaan kokonaisuudessaan osaksi kansallista lainsäädäntöä kaikkialla EU:ssa ja että säännökset pannaan asianmukaisesti

[8] Alustava vaikutustenarviointi sähköisen todistusaineiston rajatylittävän saatavuuden parantamisesta, 4. elokuuta 2017, on luettavissa englanniksi osoitteessa ec.europa.eu

[9] Tiedonanto – kahdeksas raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia, COM(2017) 354 final.

täytäntöön. Tähän kuuluu sen valvonta, ovatko kansalliset toimenpiteet direktiivin säännösten mukaisia. Tarvittaessa komissio käyttää perussopimuksiin perustuvia täytäntöönpanovaltuuksiaan rikkomusmenettelyjen keinoin.