



Bryssel 25.1.2017
COM(2017) 41 final

**KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, EUROOPPA-
NEUVOSTOLLE JA NEUVOSTOLLE**

Neljäs raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia

Neljäs raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia

I. JOHDANTO

Tämä on neljäs kuukausiraportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia. Se on tilannekatsaus, jossa käsitellään kahta pääpilaria: *terrorismin ja järjestäytyneen rikollisuuden ja niiden tukimekanismien torjuntaa* sekä *puolustusvalmiuden ja selviytymiskyvyn parantamista kyseisten uhkien varalta*. Tämän raportin neljä keskeistä aihetta ovat tietojärjestelmät ja niiden yhteentoimivuus, pehmeiden kohteiden suojeleminen, kyberuhkat ja tietosuojatutkimuksen yhteydessä.

Joulukuussa Berliinin joulumarkkinoilla tehty isku toi jälleen kerran esiin tietojärjestelmiemme vakavat heikkoudet. Niihin on puututtava kiireesti erityisesti EU:n tasolla, jotta voidaan auttaa jäsenvaltioiden raja- ja lainvalvontaviranomaisia hoitamaan vaativat tehtävänsä kentällä nykyistä tuloksellisemmin. Ongelmat liittyvät muun muassa siihen, että eri tietojärjestelmät eivät ole yhteydessä toisiinsa. Tämän ansiosta hyökkääjät voivat liikkua eri henkilöllisyyksiä käyttäen, myös yli rajojen, jäämättä kiinni. Toinen ongelma on se, että jäsenvaltiot eivät automaattisesti syötä kaikkia tarvittavia tietoja EU:n eri tietokantoihin. Nämä ovat käytännön täytäntöönpanoon liittyviä puutteita, jotka on korjattava välittömästi. Lisätoimia tarvitaan myös lainvalvontatoimien alalla rajoilla sekä sellaisten henkilöiden palauttamisessa, joiden turvapaikkahakemukset on hylätty.¹

Pehmeiden kohteiden suojelun osalta komissio nopeuttaa toimia, joiden tarkoituksena on koota jäsenvaltioiden asiantuntijat yhteen jakamaan parhaita käytäntöjä ja sopimaan vakio-ohjeista.

EU:hun kohdistuvaa kyberuhkaa käsitellään tiedotusvälineissä laajasti. Tässä raportissa tarkastellaan tällä alalla jo käynnistettyjä toimia. Niiden avulla pyritään sekä torjumaan uhkaa edistämällä sisäänrakennettua turvallisuutta alan teollisuuden kanssa ja verkko- ja tietoturvadirektiivin täytäntöönpanoa että tukemaan yhteistyötä jäsenvaltioiden välillä ja kansainvälisten organisaatioiden ja kumppanien kanssa, jotta kyberuhkiin voidaan puuttua heti kun niitä ilmenee. Komissio ja ulkoasioiden ja turvallisuuspolitiikan korkea edustaja määrittävät lähikuukausina toimet, joiden avulla näihin uhkiin voidaan vastata tehokkaasti kaikkialla EU:ssa vuonna 2013 hyväksytyn EU:n kyberturvallisuusstrategian pohjalta.

Yksityishenkilöiden yksityisyyden ja henkilötietojen suoja on keskeinen perusoikeus ja siksi kaikkien todelliseen turvallisuusunioniin tähtäävien toimien kulmakivi. Huhtikuussa 2016 hyväksytty direktiivi lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta takaa tietosuojan yhteisen korkean tason ja helpottaa siten asianomaisten tietojen vaihtoa jäsenvaltioiden lainvalvontaviranomaisten välillä. Komissio on myös käynnistänyt tietosuojapakettin yhteydessä sähköisen viestinnän tietosuojadirektiivin tarkistuksen, jonka tarkoituksena on sisällyttää direktiivin soveltamisalaan kaikki sähköisten viestintäpalvelujen tarjoajat ja yhdenmukaistaa sen säännökset yleisen tietosuojasetuksen kanssa. Ehdotuksella pyritään turvaamaan yksityisyydensuoja sähköisten viestintäpalvelujen yhteydessä ja luomaan samalla perusta sähköisen

¹ Komissio esittää lähiviikkoina tarkistetun palauttamista koskevan EU:n toimintaohjelman, ks. ”Komission kertomus Euroopan parlamentille, Eurooppa-neuvostolle ja neuvostolle eurooppalaisen raja- ja merivartioston toimintavalmiuteen saattamisesta”, COM(2017) 42.

viestinnän tietosuoja-asetuksen soveltamisalan rajoittamiselle esimerkiksi kansalliseen turvallisuuteen tai rikostutkintaan liittyvien syiden nojalla.

II. TIETOJÄRJESTELMIEN JA NIIDEN YHTEENTOIMIVUUDEN LUJITTAMINEN

Puheenjohtaja Juncker korosti syyskuussa 2016 pitämässään puheessa unionin tilasta, että on tärkeää korjata tiedonhallinnan puutteet ja parantaa **tietojärjestelmien yhteentoimivuutta ja -kytkentää**. Tähän viitataan myös Eurooppa-neuvoston joulukuussa 2016 antamissa päätelmissä. Viimeaikaiset tapahtumat ovat jälleen osoittaneet, että EU:n nykyiset tietokannat on kiireellisesti liitettävä yhteen muun muassa siksi, että raja- ja lainvalvontaviranomaiset tarvitsevat käytännön työhön välineitä henkilöllisyyspetosten paljastamiseen. Esimerkiksi Berliinissä joulukuussa 2016 tehdyn terrori-iskun tekijä onnistui liikkumaan jäsenvaltiosta toiseen paljastumatta, koska käytti ainakin 14:ää eri henkilöllisyyttä. On olemassa selkeä tarve evätä terroristeilta ja rikollisilta tällainen mahdollisuus luomalla edellytykset sille, että nykyisissä ja tulevaisuudessa EU:n tietojärjestelmissä voidaan tehdä samanaikaisia hakuja biometristen tunnistusten perusteella.

Komissio käynnisti tähän liittyvän työn huhtikuussa 2016 antamassaan tiedonannossa ”Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi”². Tiedonannossa tarkastellaan nykyisten järjestelmien toimintapuutteita, EU:n tietoarkkitehtuurin aukkoja, eri tavoin hallintoitavista tietojärjestelmistä muodostuvan kokonaisuuden monimutkaisuudesta johtuvia ongelmia ja yleistä hajanaisuutta, joka on seurausta siitä, että nykyiset järjestelmät on suunniteltu yksilöllisesti eikä osana yhteentoimivaa kokonaisuutta. Osana tätä prosessia komissio on perustanut **tietojärjestelmiä ja niiden yhteentoimivuutta käsittelevän korkean tason asiantuntijaryhmän**, jossa ovat edustettuina EU:n virastot, jäsenvaltiot ja asianomaiset sidosryhmät. Asiantuntijaryhmä esitti 21. joulukuuta 2016 puheenjohtajansa **väliraportin**³, jossa ehdotetaan ensisijaisena toimenpiteenä keskitetyn hakuportaalin luomista. Portaalin avulla lainvalvonnasta ja rajaturvallisuudesta vastaavat viranomaiset voisivat tehdä EU:n tietokannoissa ja -järjestelmissä hakuja samanaikaisesti. Väliraportissa korostetaan myös tietojen laadun tärkeyttä, sillä tietojärjestelmien avulla saatavat tulokset perustuvat niihin syötettyjen tietojen laatuun ja muotoon. Siksi raportissa esitetään suosituksia EU:n tietojärjestelmiin syötettävien tietojen laadun parantamiseksi automaattisen laadunvalvonnan avulla.

Komissio toteuttaa pian jatkotoimia keskitetyn hakuportaalin luomiseksi. Tätä varten ryhdytään yhdessä tietotekniikkavirasto eu-LISAn kanssa kehittämään portaalia, jonka avulla on mahdollista tehdä samanaikaisesti hakuja kaikissa tarvittavissa EU:n järjestelmissä. Asiaa koskevan selvityksen pitäisi valmistua kesäkuuhun mennessä, ja sen pohjalta portaalin prototyyppiä voitaisiin päästä suunnittelemaan ja testaamaan vielä ennen vuoden loppua. Komissio katsoo, että Europolin olisi kuitenkin samalla jatkettava työtään sellaisen rajapintajärjestelmän kehittämiseksi, jonka avulla jäsenvaltioiden

² Tiedonanto ”Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi”, COM(2016) 205 final.

³ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1>

etulinjan virkailijat voivat tehdä automaattisesti hakuja Europolin tietokantoihin samalla kun he tekevät hakuja omiin kansallisiin järjestelmiinsä.

Kehittämällä tietojärjestelmien yhteentoimivuutta pyritään pääsemään eroon rajaturvallisuutta ja sisäistä turvallisuutta koskevan EU:n tietoarkkitehtuurin hajanaisuudesta ja siitä johtuvista katvealueista. Kun tietokannoissa käytetään yhteistä henkilötietorekisteriä, kuten EU:n rajanylitystietojärjestelmää ja EU:n matkustustieto- ja lupajärjestelmää (ETIAS) koskevissa ehdotuksissa esitetään, yhdellä henkilöllä voi olla eri tietokannoissa vain yksi henkilöllisyys. Näin estetään väärin henkilöllisyyksien käyttö. Korkean tason asiantuntijaryhmän väliraportissa esitetyn ehdotuksen mukaisesti komissio on aluksi pyytänyt eu-LISAA analysoimaan yhteiseen biometriseen tunnistuspalveluun liittyviä teknisiä ja operatiivisia näkökohtia. Tällaisen palvelun avulla olisi mahdollista tehdä biometrinen tunnistaminen perusteella hakuja eri tietokannoissa ja paljastaa näin tietyn henkilön jossakin toisessa järjestelmässä käyttämä väärä henkilöllisyys. Lisäksi korkean tason asiantuntijaryhmän olisi nyt arvioitava, olisiko rajatietojärjestelmää ja matkustustieto- ja lupajärjestelmää varten suunniteltua **yhteistä henkilötietorekisteriä** tarpeen laajentaa muihin järjestelmiin ja olisiko se teknisesti mahdollista ja oikeasuhteista. Biometriseen tunnistuspalveluun tallennettavien biometrinen tietojen lisäksi tällaisessa yhteisessä henkilötietorekisterissä olisi myös alfanumeerisia henkilötietoja. Asiantuntijaryhmän on määrä esittää tätä koskevat havaintonsa loppuraportissaan huhtikuun 2017 loppuun mennessä.

Viimeaikaisten turvallisuuteen vaikuttavien tapahtumien vuoksi on syytä tarkastella uudelleen **tietojen pakollista yhteiskäyttöä** jäsenvaltioiden välillä. Komission joulukuussa 2016 hyväksymässä ehdotuksessa **Schengenin tietojärjestelmän** lujittamisesta esitetään – ensi kertaa – jäsenvaltioille velvollisuutta tehdä järjestelmässä kuulutuksia terrorismirikosten yhteydessä etsittävistä henkilöistä. Lainsäädäntövallan käyttäjien on nyt tärkeää hyväksyä ehdotetut toimenpiteet ripeästi. Komissio on valmis selvittämään, olisiko tiedonvaihtoa koskeva velvoite otettava käyttöön myös muiden EU:n tietokantojen yhteydessä.

III. EU:N PEHMEIDEN KOHTEIDEN SUOJELU TERRORI-ISKUILTA

Berliinissä tehty isku oli uusi ns. pehmeisiin kohteisiin kohdistettu isku EU:n alueella. Pehmeät kohteet ovat tyypillisesti siviilikohteita, joihin kerääntyy paljon ihmisiä (esimerkiksi julkiset tilat, sairaalat, koulut, urheiluareenat, kulttuurikeskukset, kahvilat ja ravintolat, ostoskeskukset ja liikenteen solmukohdat). Tällaiset paikat ovat luonnostaan haavoittuvia ja vaikeita suojella, minkä lisäksi niille on ominaista se, että iskun potentiaalisten uhrien määrä on erittäin todennäköisesti suuri. Juuri näistä syistä tällaiset paikat ovat terroristien suosiossa. Pehmeisiin kohteisiin, kuten liikennevälineisiin, kohdistettujen uusien iskujen uhka on edelleen suuri. Näin todetaan saatavilla olevissa arvioinneissa, muun muassa Daeshin toimintatapojen muutoksia koskevassa Europolin raportissa⁴.

⁴ Europol, *Changes in modus operandi of Islamic State (IS) revisited*, marraskuu 2016 – Europol Public Information, saatavilla osoitteessa <https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited>

Vuonna 2015 hyväksytyssä Euroopan turvallisuusagendassa ja vuonna 2016 hyväksytyssä turvallisuusunionia koskevassa tiedonannossa korostetaan, että on toteutettava lisätoimia turvallisuuden parantamiseksi ja kehitettävä innovatiivisia havaitsemisvälineitä ja teknologiaa pehmeiden kohteiden suojelemiseksi. Komissio on tukenut jäsenvaltioita ja kannustanut niitä jakamaan parhaita käytäntöjä parempien välineiden kehittämiseksi pehmeisiin kohteisiin kohdistettujen iskujen ehkäisemistä ja niihin reagoimista varten. Tämän työn pohjalta on laadittu operatiivisia käsikirjoja ja ohjeistusta. Komissio laatii parhaillaan tiiviissä yhteistyössä jäsenvaltioiden asiantuntijoiden kanssa kattavaa turvallisuusmenettelyjen käsikirjaa ja toimintamalleja, joita voidaan soveltaa erilaisissa pehmeissä kohteissa (esimerkiksi ostoskeskuksissa, sairaaloissa, urheilu- ja kulttuuritapahtumissa). Tavoitteena on antaa jäsenvaltioille vuoden 2017 alkupuolella ohjeita pehmeiden kohteiden suojelusta niiden omien parhaiden käytäntöjen pohjalta.

Lisäksi komissio kutsuu jäsenvaltioiden viranomaiset helmikuussa pidettävään ensimmäiseen pehmeiden kohteiden suojelua koskevaan työpajaan. Tarkoituksena on vaihtaa tietoja ja määrittää parhaita käytäntöjä pehmeiden kohteiden suojelua ja yleistä turvallisuutta koskevaa monitahoista ongelmakenttää varten. Komissio myös rahoittaa sisäisen turvallisuuden rahastosta Belgian, Alankomaiden ja Luxemburgin toteuttamaa pilottihanketta, jonka avulla on tarkoitus perustaa alueellinen osaamiskeskus lainvalvonta-alan erityistoimenpiteitä varten. Keskus tarjoaisi koulutusta poliiseille, jotka usein joutuvat reagoimaan iskuihin ensimmäisinä.

Vastaaminen pehmeisiin kohteisiin kohdistuviin iskuihin on keskeisellä sijalla myös pelastuspalveluun liittyvässä komission toiminnassa. Komissio ilmoitti joulukuussa toimista, joita se aikoo toteuttaa yhdessä jäsenvaltioiden kanssa EU:n kansalaisten suojelemiseksi ja haavoittuvuuden vähentämiseksi välittömästi terrori-iskujen jälkeen. Tarkoituksena on lujittaa iskujen jälkiseurausten hoitoon osallistuvien toimijoiden keskinäistä koordinointia. Komissio on myös luvannut tukea jäsenvaltioiden toimia helpottamalla yhteisten koulutustilaisuuksien ja harjoitusten järjestämistä ja varmistamalla jatkuvan vuoropuhelun olemassa olevien yhteyspisteiden ja asiantuntijaryhmien puitteissa. Komissio tukee myös erityisten toimintamallien kehittämistä terrori-iskuihin vastaamiseksi unionin pelastuspalvelumekanismien puitteissa sekä aloitteita, joiden yhteydessä voidaan jakaa kokemuksia ja antaa yleisölle tietoa tästä aiheesta.

Komissio aikoo myös selvittää yhdessä jäsenvaltioiden kanssa, millaisen EU:n tuen avulla voitaisiin edistää selviytymiskyvyn vahvistamista ja parantaa turvallisuutta mahdollisten pehmeiden kohteiden ympäristössä. Jäsenvaltiot voisivat hakea rahoitusta myös Euroopan investointipankilta (EIP), muun muassa Euroopan strategisten investointien rahaston kautta, EU:n ja EIP-ryhmän linjausten mukaisesti. Hankkeisiin sovellettaisiin tavanomaisia lainsäädäntöön perustuvia päätöksentekomenettelyjä.

Komissio järjesti marraskuussa 2016 työpajan, jossa käsiteltiin monien eri sidosryhmien kanssa erityisesti julkisiin liikennevälineisiin liittyviä pehmeitä kohteita, kuten lento- tai rautatieasemien julkisia tiloja. Työpajassa korostettiin, että on otettava tasapuolisesti huomioon turvallisuustarpeet, matkustusmukavuus ja kuljetusten sujuvuus. Työpajan päätelmissä korostetaan, että on tärkeää luoda turvallisuuskulttuuri, jonka piiriin kuuluvat paitsi henkilöstö myös matkustajat. Tarvittavia vastatoimia voidaan suunnitella paikallisen riskienarvioinnin pohjalta, minkä lisäksi on tehostettava yhteydenpitoa kaikkien asianosaisten kesken.

IV. KYBERUHKIIN VASTAAMINEN

Kyberrikollisuus ja kyberhyökkäykset ovat unionissa keskeisiä haasteita. EU:n tasolla toteutettavilla toimilla voidaan edistää kollektiivisen häiriönsietokyvyn lujittamista. Kybertapahtumista aiheutuu päivittäin vakavaa haittaa kansalaisille ja suurta taloudellista vahinkoa eurooppalaisille yrityksille ja koko talouselämälle. Kyberhyökkäykset ovat hybridiuhkien keskeinen osatekijä, sillä kun ne ajoitetaan tapahtumaan samaan aikaan kuin fyysinen uhka, vaikkapa terrori-isku, niiden vaikutus voi olla tuhoisa. Niiden avulla voidaan myös horjuttaa valtion vakautta tai haastaa sen poliittiset instituutiot ja perustavanlaatuiset demokraattiset menettelyt. Kun verkkoteknologian käyttö jatkuvasti lisääntyy, myös yhteiskuntiemme kriittinen infrastruktuuri (sairaaloista ydinvoimaloihin) on yhä haavoittuvampi.

Vuonna 2013 hyväksytty EU:n kyberturvallisuusstrategia on osa niitä keskeisiä politiikkatoimia, joilla vastataan kyberturvallisuuden haasteisiin. Keskeinen toimenpide on heinäkuussa 2016 hyväksytty verkko- ja tietoturvadirektiivi⁵. Siinä luodaan edellytykset tehokkaammalle EU:n tason yhteistyölle ja verkkouhkien sietokyvyille tukemalla yhteistyötä ja tietojenvaihtoa jäsenvaltioiden kesken sekä edistämällä yksittäisiin kybertapahtumiin liittyvää operatiivista yhteistyötä ja riskejä koskevien tietojen jakamista. Jotta voitaisiin varmistaa direktiivin yhdenmukainen täytäntöönpano eri aloilla ja yli rajojen, komissio järjestää jäsenvaltioille direktiivin yhteistyöryhmän ensimmäisen kokouksen helmikuussa 2017.

Komissio ja korkea edustaja hyväksyivät huhtikuussa 2016 hybridiuhkien torjuntaa koskevan yhteisen kehityksen⁶. Siinä esitetään 22 operatiivista tointia, joiden avulla pyritään lisäämään tietoisuutta, parantamaan häiriönsietokykyä ja kriiseihin vastaamista sekä kehittämään yhteistyötä EU:n ja Naton välillä. Neuvoston kehotuksen mukaisesti komissio ja korkea edustaja arvioivat toimien edistymistä viimeistään heinäkuussa 2017 esitettävässä raportissa.

Komissio edistää myös teknologista innovointia muun muassa ohjaamalla EU:n tutkimusvaroja sellaisten uusien ratkaisujen ja teknologioiden kehittämiseen, joiden avulla voidaan lujittaa kyberhyökkäysten sietokykyä (mm. sisäänrakennettua turvallisuutta koskevat hankkeet). Kesällä 2016 komissio käynnisti yhdessä alan toimijoiden kanssa 1,8 miljardin euron arvoisen julkisen ja yksityisen sektorin kyberturvallisuuskumppanuuden.⁷

Digitalisoinnista on tulossa liikenteen alalla merkittävä tekijä, jonka avulla voidaan toteuttaa nykyisten liikennejärjestelmien kipeästi kaivattu uudistus. Nopeasti etenevä digitalisointi tuo muassaan monia etuja, mutta toisaalta se lisää liikenteen haavoittuvuutta kyberturvallisuusriskien kannalta. Tätä uhkaa pyritään lieventämään toteuttamalla monenlaisia toimia eri tasoilla, erityisesti lentoliikenteessä mutta myös meri-, joki-

⁵ Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

⁶ JOIN (2016)18.

⁷ Hankkeesta ilmoitettiin vuonna 2016 Euroopan kyberresilienssijärjestelmää koskevassa tiedonannossa, COM(2016) 410 final.

rautatie- ja tieliikenteessä.⁸ Lisäksi olisi edelleen selkeytettävä, yhdenmukaistettava ja täydennettävä niiden eri sidosryhmien toimia, jotka eri tavoin pyrkivät parantamaan kyberuhkien sietokykyä.

Koska kyberuhkat ovat nopeasti kehittyviä, komissio ja korkea edustaja määrittävät lähikuukausina toimia, joiden avulla niihin voidaan vastata tehokkaasti EU:n tasolla vuonna 2013 hyväksytyn EU:n kyberturvallisuusstrategian pohjalta.

V. HENKILÖTIETOJEN SUOJAAMINEN RIKOSTUTKINNAN TEHOKKUUDESTA TINKIMÄTTÄ

Direktiivi lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta⁹ on merkittävä osa terrorismin ja vakavan rikollisuuden torjuntaa. Siinä vahvistetaan yhteiset tietosuojanormit, joiden puitteissa jäsenvaltioiden lainvalvontaviranomaiset voivat vaihtaa tarvittavia tietoja sujuvasti samalla kun uhrien, todistajien ja rikoksesta epäiltyjen tiedot on asianmukaisesti suojattu.

Jotta lisäksi voitaisiin turvata sekä yksilöiden että yritysten viestinnän luottamuksellisuus ja kaikkien markkinatoimijoiden tasavertaiset toimintaedellytykset huhtikuussa 2015 hyväksytyn digitaalisten sisämarkkinoiden strategian tavoitteiden mukaisesti, komissio hyväksyi 11. tammikuuta 2017 ehdotuksen **sähköisen viestinnän tietosuojasetukseksi**¹⁰ (jolla korvataan direktiivi 2002/58/EY). Samoin kuin voimassa olevalla direktiivillä, tarkistetulla sähköisen viestinnän tietosuojasetuksella täsmennetään yleistä tietosuojasetusta¹¹ ja vahvistetaan kehys, joka sääntelee yksityisyyden ja henkilötietojen suojaa sähköisen viestinnän alalla.

Tarkistuksen seurauksena kaikki sähköinen viestintä, myös silloin kun viestintä on vain jonkin muun palvelun liitännäistoiminto, katsotaan luottamukselliseksi tai rajoitetun jakelun piiriin kuuluvaksi, riippumatta siitä, käytetäänkö siinä perinteisiä vai internetin kautta välitettäviä (Over-the-Top) viestintäpalveluja (esim. Skype, WhatsApp), jotka ovat

⁸ Esimerkkejä tästä ovat erilaiset kansainväliset ohjeet, joita on laatinut mm. Kansainvälinen merenkulkujärjestö (IMO), ja kansainvälisen siviili-ilmailujärjestön (ICAO) äskettäin hyväksymä päätöslauselma, joka perustuu EU:n ja Yhdysvaltojen aloitteeseen. Lisäksi Euroopan lentoturvallisuusvirasto kehittää parhaillaan reaktiivisempaa toimintatapaa poikkeuksellisista tapahtumista raportointiin. Sisäänrakennettua turvallisuutta sovelletaan kehitteillä oleviin uusiin järjestelmiin, kuten SESAR-yhteisyrityksen työstämään eurooppalaiseen ilmaliikenteen hallinnan yleissuunnitelmaan.

⁹ Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta. Direktiivi tuli voimaan 5. toukokuuta 2016, ja jäsenvaltioiden on määrä saattaa se osaksi kansallista lainsäädäntöään viimeistään 6. toukokuuta 2018. Komissio on perustanut jäsenvaltioiden kanssa asiantuntijaryhmän, jossa vaihdetaan näkemyksiä tämän ns. poliisidirektiivin täytäntöönpanosta.

¹⁰ Sähköisen viestinnän tietosuojasetus, COM(2017) 10.

¹¹ Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus). Asetusta aletaan soveltaa 25. toukokuuta 2018.

toiminnallisesti vastaavia ja joista on tullut monille käyttäjille tavallisten teleoperaattoreiden vaihtoehtoja.¹² Sen lisäksi, että palveluntarjoajien on ehdotuksen mukaan kunnioitettava asiakkaidensa tekemiä yksityisyysasetuksia koskevia valintoja heidän tietojensa käytön, tallentamisen ja käsittelyn yhteydessä, EU:n ulkopuolelle sijoittautuneiden palveluntarjoajien on nimettävä itselleen jäsenvaltioon sijoittautunut edustaja. Tämän ansiosta jäsenvaltiot voivat myös helpottaa lainvalvonta- ja oikeusviranomaisten yhteistyötä palveluntarjoajien kanssa sähköiseen todistusaineistoon pääsyn yhteydessä (ks. jäljempänä).

Samoin kuin nykyisissä sähköisen viestinnän tietosuojasäännöissä, lainvalvonta- ja oikeusviranomaisten pääsy rikostutkinnassa tarvittaviin sähköisiin tietoihin säännellään ehdotetun sähköisen viestinnän tietosuoja-asetuksen 11 artiklaan perustuvalla poikkeuksella¹³. Kyseisen säännöksen nojalla viestinnän luottamuksellisuutta voidaan rajoittaa unionin tai jäsenvaltion lainsäädäntötoimenpiteellä, jos tällainen rajoitus on välttämätön ja oikeasuhteinen toimenpide, jonka tavoitteena on kansallisen turvallisuuden, puolustuksen ja yleisen turvallisuuden ja rikosten torjunnan, tutkinnan, selvittämisen ja syyteharkinnan tai rikosoikeudellisten seuraamusten täytäntöönpanon varmistaminen. Tällä säännöksellä on erityistä merkitystä niiden kansallisten sääntöjen kannalta, jotka koskevat **tietojen säilyttämistä** ja joilla muun muassa veloitetaan televiestintäpalvelujen tarjoajat säilyttämään viestintätiedot tietyn ajan mahdollista lainvalvontatarkoituksessa tapahtuvaa pääsyä varten. Merkitys perustuu siihen, että sen jälkeen kun Euroopan yhteisöjen tuomioistuin vuonna 2014 kumosi tietojen säilyttämistä koskevan direktiivin¹⁴, EU:ssa ei ole ollut tietojen säilyttämistä koskevaa säädöstä, ja eräät jäsenvaltiot ovat hyväksyneet tietojen säilyttämistä koskevia kansallisia lakeja. Ruotsin ja Yhdistyneen kuningaskunnan antamat tietojen säilyttämistä koskevat lait johtivat kanteen nostamiseen unionin tuomioistuimessa, joka antoi päätöksensä asiassa *Tele2* 21. joulukuuta 2016¹⁵. Tuomioistuin katsoi, että kansallinen säännöstö, jossa rikollisuuden torjumiseksi säädetään tilaajien ja käyttäjien liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä kaikkien sähköisten viestintävälineiden osalta, on ristiriidassa unionin oikeuden kanssa. Tuomion vaikutuksia analysoidaan parhaillaan, ja komissio antaa ohjeita siitä, miten tietojen säilyttämistä koskeva kansallinen lainsäädäntö olisi tuomion perusteella laadittava.

Rikoksista jää digitaalisia jälkiä, joita voidaan käyttää todisteena oikeudenkäynnissä. Epäiltyjen välinen sähköinen viestintä on usein lainvalvontaviranomaisten ja syyttäjien ainoa johtolanka. Pääsy **sähköiseen todistusaineistoon** saattaa kuitenkin edellyttää sekä teknisesti että oikeudellisesti monimutkaisia ja raskaita menettelyjä, jotka hidastavat tutkinnan nopeaa etenemistä, varsinkin jos aineisto on tallennettu ulkomaille tai pilvipalveluun. Näiden ongelmien poistamiseksi komissio arvioi parhaillaan ratkaisuja, joiden avulla tutkijat voisivat saada pääsyn rajat ylittävään sähköiseen todistusaineistoon.

¹² Tämä perustuu toimintatapaan, joka omaksuttiin komission 14. syyskuuta 2016 esittämässä eurooppalaista sähköisen viestinnän säännöstöä koskevassa direktiiviehdotuksessa (televiestintäpaketti), COM(2016) 590 final.

¹³ Ks. ehdotuksen 11 artiklan 1 kohta. Tämä tietojen säilyttämistä koskeva lauseke perustuu suoraan sähköisen viestinnän tietosuoja-direktiivin 15 artiklaan, ja se on myös yleisen tietosuoja-asetuksen vaatimusten mukainen. Tällaisessa rajoituksessa on noudatettava keskeisiltä osin perusoikeuksia, ja sen on oltava välttämätön, asianmukainen ja oikeasuhteinen toimenpide.

¹⁴ Unionin tuomioistuimen tuomio 8.4.2014, *Digital Rights Ireland*, yhdistetyt asiat C-293/12 ja C-594/12.

¹⁵ Unionin tuomioistuimen tuomio 21.12.2016, *Tele2*, yhdistetyt asiat C-203/15 ja C-698/15.

Vaihtoehtoja ovat esimerkiksi keskinäisen oikeusavun tehostaminen, yhteistyön tekeminen suoraan internetpalvelujen tarjoajien kanssa ja sellaisten kriteerien laatiminen, joiden perusteella määriteltäisiin lainvalvonnallinen toimivalta kybertoimintaympäristössä, sovellettavia tietosuojasääntöjä täysimääräisesti noudattaen.¹⁶ Komissio raportoi etenemisestä oikeus- ja sisäasiain neuvostolle 9. joulukuuta 2016.¹⁷

Komissio on selvittänyt kattavan (ja edelleen käynnissä olevan) asiantuntijakuulemisen avulla sähköisen todistusaineiston hankintaan liittyviä lukuisia ja usein monimutkaisia ongelmia. Näin on saatu parempi kuva nykyisistä säännöistä ja käytännöistä jäsenvaltioissa ja voitu määrittää mahdollisia toimintavaihtoehtoja. Edistymisraportissa esitetään yhteenveto ideoista, joita tähän mennessä on tullut esiin tiedonkeruun ja asiantuntijoiden kuulemisen yhteydessä. Komissio tarkastelee niitä lähemmin tulevana kuukausina sidosryhmiä kuullen. Komissio esittää asiaa koskevan aloitteen vuoden 2017 aikana, kuten komission työohjelmassa todetaan.

VI. PÄÄTELMÄT

Seuraava raportti julkaistaan 1. maaliskuuta. Siinä tarkastellaan näiden ja muiden keskeisten toimien täytäntöönpanon edistymistä.

¹⁶ Ks. Euroopan turvallisuusagenda (COM(2015) 185 final) ja komission tiedonanto ”Euroopan turvallisuusagendan valjastaminen terrorismin torjuntaan ja toimivan ja todellisen turvallisuusunionin perustamisen valmisteluun” (COM(2016) 230 final).

¹⁷ Neuvosto antoi 9. kesäkuuta 2016 päätelmät rikosoikeudellisten toimien tehostamisesta kybertoimintaympäristössä ja kehotti niissä komissiota toteuttamaan konkreettisia toimia, kehittämään EU:n yhteisen toimintamallin ja esittämään toimia kesäkuuhun 2017 mennessä.