EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI 2013/40/EU,

annettu 12 päivänä elokuuta 2013,

tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta

EUROOPAN PARLAMENTTI JA EUROOPAN UNIONIN NEUVOSTO, jotka

ottavat huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 83 artiklan 1 kohdan,

ottavat huomioon Euroopan komission ehdotuksen,

sen jälkeen kun esitys lainsäätämisjärjestyksessä hyväksyttäväksi säädökseksi on toimitettu kansallisille parlamenteille,

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon ([1]),

noudattavat tavallista lainsäätämisjärjestystä ([2]),

sekä katsovat seuraavaa:

(1) Tämän direktiivin tavoitteina on lähentää tietojärjestelmiin kohdistuvia hyökkäyksiä koskevaa jäsenvaltioiden rikosoikeutta vahvistamalla vähimmäissäännöt rikosten määrittelylle ja sovellettaville seuraamuksille sekä parantaa yhteistyötä toimivaltaisten viranomaisten välillä, jäsenvaltioiden poliisi- ja muut erikoistuneet lainvalvontaviranomaiset mukaan luettuina, ja unionin toimivaltaisten erityisvirastojen ja -elinten, kuten Eurojust, Europol ja sen Euroopan verkkorikostorjuntakeskus, sekä Euroopan verkko- ja tietoturvaviraston (ENISA) välillä.

(2) Tietojärjestelmät ovat tärkeä osa poliittista, sosiaalista ja taloudellista vuorovaikutusta unionissa. Yhteiskunta on yhä enemmän riippuvainen tällaisista järjestelmistä. Sisämarkkinoiden sekä kilpailukykyisen ja innovoivan talouden kehittämisen kannalta on erittäin tärkeää, että nämä järjestelmät toimivat sujuvasti ja turvallisesti unionissa. Tietojärjestelmien asianmukaisen suojelun tason varmistamisen olisi oltava osa tehokkaita ja kattavia puitteita ehkäisytoimille, jotka liittyvät tietoverkkorikollisuuden vastaisiin rikosoikeudellisiin toimiin.

(3) Tietojärjestelmiä vastaan tehdyt hyökkäykset ja erityisesti järjestäytyneeseen rikollisuuteen liittyvät hyökkäykset ovat kasvava uhka unionissa ja maailmanlaajuisesti, ja samalla tietojärjestelmiin kohdistuvien terrorihyökkäysten tai poliittisista syistä tapahtuvien hyökkäysten mahdollisuus herättää lisääntyvää huolta, sillä tietojärjestelmät ovat osa jäsenvaltioiden ja unionin elintärkeää infrastruktuuria. Koska hyökkäykset uhkaavat turvallisemman tietoyhteiskunnan sekä vapauteen, turvallisuuteen ja oikeuteen perustuvan alueen toteuttamista, niihin on varauduttava unionin tasolla ja ne edellyttävät tehokkaampaa kansainvälistä yhteistyötä ja yhteensovittamista.

(4) Unionissa on useita elintärkeitä infrastruktuureja, joiden vahingoittumisella tai tuhoutumisella olisi huomattava rajatylittävä vaikutus. Elintärkeiden infrastruktuurien suojaamisvalmiuksia on lisättävä unionissa, joten toimenpiteitä verkkohyökkäysten torjumiseksi olisi tästä syystä täydennettävä ankarilla rikosoikeudellisilla seuraamuksilla, jotka kuvastavat tällaisten hyökkäysten vakavuutta. Elintärkeänä infrastruktuurina voidaan pitää sellaisia jäsenvaltioissa sijaitsevia hyödykkeitä ja järjestelmiä tai niiden osia, jotka ovat keskeisiä yhteiskunnan välttämättömien toimintojen, terveydenhuollon, turvallisuuden, turvatoimien sekä väestön taloudellisen tai sosiaalisen hyvinvoinnin ylläpitämiseksi, kuten voimalat, liikenneverkot tai julkiset verkot, ja joiden vahingoittumisella tai tuhoutumisella olisi merkittävä vaikutus jäsenvaltioon sen vuoksi, että näitä toimintoja ei kyetä ylläpitämään.

(5) On todisteita siitä, että jäsenvaltioiden tai julkisen tai yksityisen sektorin tiettyjen toimintojen kannalta elintärkeitä tietojärjestelmiä vastaan pyritään tekemään entistä vaarallisempia ja toistuvia laajamittaisia hyökkäyksiä. Tähän suuntaukseen liittyvät entistä pidemmälle kehitetyt menetelmät, kuten niin kutsuttujen bottiverkkojen luominen ja käyttö, mihin liittyy rikoksen useita eri vaiheita, joista jokainen yksin voi olla vakava riski yleiselle edulle. Tällä direktiivillä pyritään muun muassa ottamaan käyttöön rikosoikeudellisia seuraamuksia, jotka koskevat bottiverkkojen luomista eli sitä, että perustetaan etähallinta merkittävälle määrälle tietokoneita tartuttamalla ne haittaohjelmilla kohdennettujen verkkohyökkäysten kautta. Kun bottiverkko on luotu, bottiverkon muodostavat tartunnan saaneet tietokoneet on mahdollista aktivoida tietokoneiden käyttäjien tietämättä sellaisen tässä direktiivissä tarkoitetun laajamittaisen verkkohyökkäyksen käynnistämiseksi, joka yleensä kykenee aiheuttamaan vakavaa vahinkoa. Jäsenvaltiot voivat määritellä vakavan vahingon kansallisen lakinsa ja käytäntönsä mukaisesti, ja siihen voi kuulua yleiseltä merkitykseltään huomattavien järjestelmäpalvelujen vahingoittaminen tai huomattavien taloudellisten menetysten taikka henkilötietojen tai arkaluonteisten tietojen häviämisen aiheuttaminen.

(6) Laajamittaiset verkkohyökkäykset voivat aiheuttaa merkittäviä taloudellisia vahinkoja keskeyttämällä tietojärjestelmät ja viestinnän sekä aiheuttamalla kaupallisesti tärkeiden luottamuksellisten tietojen tai muun datan menetyksen tai muuttumisen. Erityisesti olisi kiinnitettävä huomiota innovatiivisten pienten ja keskisuurten yritysten tietoisuuden lisäämiseen tällaisista uhkista ja niiden haavoittuvaisuudesta tällaisten hyökkäysten osalta, koska ne ovat entistä riippuvaisempia tietojärjestelmien moitteettomasta toiminnasta ja saatavuudesta ja niillä on usein rajoitetut voimavarat tietoturvallisuutta varten.

([1]) EUVL C 218, 23.7.2011, s. 130.

([2]) Euroopan parlamentin kanta, vahvistettu 4. heinäkuuta 2013 (ei vielä julkaistu virallisessa lehdessä), ja neuvoston päätös, tehty 22. heinäkuuta 2013.

(7) Alan yhteiset määritelmät ovat tärkeitä sen varmistamiseksi, että jäsenvaltioilla on yhdenmukainen linja tämän direktiivin soveltamisessa.

(8) Rikostunnusmerkistöjen osalta on tarpeen omaksua yhteinen linja ottamalla käyttöön yhteinen rikosmääritelmä laittomista tunkeutumisista tietojärjestelmään, laittomasta järjestelmän häirinnästä, laittomasta datan vahingoittamisesta ja viestintäsalaisuuden loukkaamisesta (tietojen laiton hankkiminen).

(9) Viestintäsalaisuuden loukkaamiseen (tietojen laiton hankkiminen) kuuluvat viestin sisällön kuunteleminen, seuranta tai valvonta ja tietosisällön hankkiminen joko suoraan tunkeutumalla tietojärjestelmään ja käyttämällä sitä tai epäsuorasti teknisin keinoin käyttämällä elektronista salakuuntelua tai salakuuntelulaitteita, mutta se ei välttämättä rajoitu näihin.

(10) Jäsenvaltioiden olisi säädettävä tietojärjestelmiin kohdistuvista hyökkäyksistä määrättävistä seuraamuksista. Näiden seuraamusten olisi oltava tehokkaita, oikeasuhteisia ja varoittavia, ja niihin olisi kuuluttava vankeusrangaistus ja/tai sakko.

(11) Tässä direktiivissä säädetään rikosoikeudellisista seuraamuksista ainakin niiden tapausten osalta, jotka eivät ole vähäisiä. Jäsenvaltiot voivat kansallisen lakinsa ja käytäntönsä mukaisesti määritellä, mikä on vähäinen tapaus. Tapausta voidaan pitää vähäisenä esimerkiksi silloin, kun rikoksen aiheuttama yleiseen tai yksityiseen etuun, esimerkiksi tietokonejärjestelmän tai datan eheyteen taikka henkilön koskemattomuuteen, oikeuksiin tai muihin etuihin, kohdistuva vahinko ja/tai riski on merkityksetön tai luonteeltaan sellainen, että rikosoikeudellisen seuraamuksen määrääminen lakisääteisissä rajoissa tai rikosoikeudelliseen vastuuseen asettaminen ei ole tarpeen.

(12) Verkkohyökkäysten aiheuttamien uhkien ja riskien tunnistamisella ja niistä raportoimisella sekä tähän liittyvällä tietojärjestelmien haavoittuvuudella on merkitystä verkkohyökkäysten tehokkaan estämisen ja niihin puuttumisen sekä tietojärjestelmien turvallisuuden parantamisen kannalta. Kannustimien tarjoaminen voisi lisätä turvallisuuspuutteista raportoimista. Jäsenvaltioiden olisi pyrittävä tarjoamaan mahdollisuuksia turvallisuuspuutteiden oikeudelliselle toteamiselle ja niistä raportoimiselle.

(13) On tarkoituksenmukaista säätää ankarammista seuraamuksista silloin, kun tietojärjestelmään kohdistuvan hyökkäyksen toteuttaa rikollisjärjestö, sellaisena kuin se on määritelty järjestäytyneen rikollisuuden torjunnasta 24 päivänä lokakuuta 2008 tehdyssä neuvoston puitepäätöksessä 2008/841/YOS ([1]), kun verkkohyökkäys on laajamittainen ja vaikuttaa merkittävään määrään tietojärjestelmiä, mukaan lukien silloin, kun hyökkäyksen tarkoituksena on luoda bottiverkko, tai kun verkkohyökkäys aiheuttaa vakavaa vahinkoa, mukaan lukien silloin, kun hyökkäys toteutetaan bottiverkon kautta. On myös tarkoituksenmukaista säätää ankarammista seuraamuksista silloin, kun hyökkäys kohdistuu jäsenvaltioiden tai unionin elintärkeään infrastruktuuriin.

(14) Toinen tärkeä seikka pyrittäessä yhdennettyyn lähestymistapaan tietoverkkorikollisuuden torjunnassa on tehokkaiden toimenpiteiden ottaminen käyttöön henkilöllisyysvarkauden ja muiden henkilöllisyyteen liittyvien rikosten estämiseksi. Mahdollista tarvetta unionin toimiin tällaisen rikollisen käyttäytymisen torjumiseksi voitaisiin myös harkita arvioitaessa kattavan horisontaalisen unionin välineen tarvetta.

(15) Neuvoston 27 ja 28 päivänä marraskuuta 2008 antamien päätelmien mukaan jäsenvaltioiden ja komission kanssa olisi luotava uusi strategia ottaen huomioon Euroopan neuvoston vuonna 2001 tekemän tietoverkkorikollisuutta koskevan yleissopimuksen sisältö. Kyseinen yleissopimus on oikeudellinen viitekehys torjuttaessa tietoverkkorikollisuutta, tietojärjestelmiin kohdistuvat hyökkäykset mukaan luettuina. Tämä direktiivi pohjautuu mainittuun yleissopimukseen. Olisi pidettävä ensisijaisena sitä, että kaikki jäsenvaltiot saattavat yleissopimuksen ratifiointimenettelyt päätökseen mahdollisimman pian.

(16) Koska hyökkäyksiä voidaan toteuttaa erilaisin tavoin ja koska laitteistot ja ohjelmistot kehittyvät nopeasti, tässä direktiivissä viitataan välineisiin, joita voidaan käyttää tässä direktiivissä säädettyjen rikosten tekemiseen. Tällaisia välineitä voivat olla haittaohjelmat, mukaan lukien haittaohjelmat, joilla voidaan luoda bottiverkkoja, joita käytetään verkkohyökkäysten tekemiseen. Vaikka tällainen väline olisi sopiva tai erityisen sopiva jonkin tässä direktiivissä säädetyn rikoksen tekemiseen, on mahdollista, että se on valmistettu laillisia tarkoituksia varten. Koska kriminalisointia on vältettävä siltä osin kuin tällaiset välineet on valmistettu ja saatettu markkinoille laillisia tarkoituksia varten, kuten tietotekniikkatuotteiden luotettavuuden tai tietojärjestelmien turvallisuuden testaamiseksi, yleisen tahallisuusedellytyksen lisäksi on edellytettävä myös välitöntä tahallisuutta käyttää näitä välineitä yhden tai useamman tässä direktiivissä säädetyn rikoksen tekemiseen.

(17) Tässä direktiivissä ei määrätä rikosoikeudellista vastuuta silloin, kun tässä direktiivissä säädettyjä rikoksia koskevat objektiiviset kriteerit täyttyvät mutta teot on tehty ilman tahallisuutta, esimerkiksi kun henkilö ei tiedä, että järjestelmään pääsyyn ei ollut lupaa, tai kun on kyse tietojärjestelmien luvallisesta testauksesta tai suojauksesta, kuten silloin, kun yritys tai myyjä antaa henkilölle tehtäväksi testata turvallisuusjärjestelmänsä vahvuutta. Sopimusvelvoitteet tai sopimukset tietojärjestelmiin pääsyn rajoittamiseksi käyttäjäpolitiikalla tai palveluehdoilla sekä työnantajan tietojärjestelmiin pääsyä ja niiden käyttöä henkilökohtaisiin tarkoituksiin koskevat työriidat eivät saisi aiheuttaa rikosoikeudellista vastuuta tämän direktiivin puitteissa, jos järjestelmiin pääsyä pidettäisiin näissä olosuhteissa luvattomana ja se muodostaisi ainoan perusteen rikosoikeudelliselle menettelylle. Tämä direktiivi ei rajoita kansallisessa ja unionin oikeudessa säädettyä tietojensaantioikeutta, mutta se ei myöskään saa olla laittoman tai mielivaltaisen tietojensaannin peruste.

([1]) EUVL L 300, 11.11.2008, s. 42.

(18) Eri olosuhteet voivat helpottaa verkkohyökkäysten tekemistä; tekijällä voi esimerkiksi työnsä puolesta olla käyttöoikeus verkkohyökkäyksen kohteeksi joutuneiden tietojärjestelmien turvajärjestelmiin. Tällaiset olosuhteet olisi kansallisen lain puitteissa otettava asianmukaisesti huomioon rikosoikeudellisten menettelyjen aikana.

(19) Jäsenvaltioiden olisi kansallisessa laissaan säädettävä raskauttavista asianhaaroista oikeusjärjestelmänsä raskauttavia asianhaaroja koskevien sovellettavien sääntöjen mukaisesti. Niiden olisi varmistettava, että tuomarit voivat harkita näitä raskauttavia asianhaaroja tuomitessaan rikoksentekijöitä. Tuomari voi harkita näitä asianhaaroja yhdessä tietyn tapauksen muiden tosiseikkojen kanssa.

(20) Tässä direktiivissä ei säädetä edellytyksistä, joiden olisi täytyttävä lainkäyttövallan käyttämiseksi jonkin tässä direktiivissä tarkoitetun rikoksen osalta, kuten että uhri on tehnyt ilmoituksen rikoksen tekopaikassa tai että se valtio, jossa rikos tehtiin, on tehnyt ilmiannon tai että tekijään ei ole kohdistettu syytetoimia rikoksen tekopaikassa.

(21) Valtioiden ja julkisten elinten on tämän direktiivin yhteydessä täysimääräisesti taattava ihmisoikeuksien ja perusvapauksien kunnioittaminen voimassa olevien kansainvälisten velvoitteiden mukaisesti.

(22) Tällä direktiivillä vahvistetaan G8:n tai Euroopan neuvoston ympärivuorokautisen ja kaikkina viikonpäivinä toimivan yhteyspisteverkoston kaltaisten verkkojen merkitystä. Näiden yhteyspisteiden olisi voitava antaa tehokasta apua ja siten esimerkiksi helpottaa saatavilla olevien tietojen vaihtoa sekä teknisten neuvojen tai oikeudellisten tietojen antamista tutkimuksissa tai menettelyissä, jotka koskevat tietojärjestelmiin ja dataan liittyviä rikoksia ja joissa pyynnön esittänyt jäsenvaltio on osallisena. Verkkojen sujuvan toimimisen varmistamiseksi kullakin yhteyspisteellä olisi oltava valmiudet viestiä nopeasti toisen jäsenvaltion yhteyspisteen kanssa, ja niiden olisi saatava tukea muun muassa koulutetulta ja valmiudet omaavalta henkilöstöltä. Kun otetaan huomioon, miten nopeasti laajamittaisia verkkohyökkäyksiä voidaan toteuttaa, jäsenvaltioiden olisi voitava vastata ripeästi yhteyspisteverkoston esittämiin kiireellisiin pyyntöihin. Tällaisissa tapauksissa voi olla asianmukaista, että tietopyyntöön liittyy yhteydenotto puhelimitse sen varmistamiseksi, että pyynnön vastaanottanut jäsenvaltio käsittelee pyynnön nopeasti ja antaa palautetta kahdeksan tunnin kuluessa.

(23) Yhtäältä viranomaisten ja toisaalta yksityissektorin ja kansalaisyhteiskunnan välinen yhteistyö on hyvin tärkeää ehkäistäessä ja torjuttaessa tietojärjestelmiin kohdistuvia hyökkäyksiä. Palveluntarjoajien, tuottajien, lainvalvontaelinten ja oikeusviranomaisten välistä yhteistyötä on edistettävä ja parannettava kunnioittaen samalla täysimääräisesti oikeusvaltioperiaatetta. Tällaiseen yhteistyöhön voi sisältyä palveluntarjoajien antama tuki mahdollisten todisteiden säilyttämisessä ja rikoksentekijöiden tunnistamista auttavien tietojen tarjoamisessa sekä viimeisenä keinona sellaisten tietojärjestelmien tai toimintojen, jotka on kaapattu tai joita on käytetty laittomiin tarkoituksiin, sulkeminen kansallisen lain ja käytännön mukaisesti osittain tai kokonaan. Jäsenvaltioiden olisi myös harkittava yhteistyö- ja kumppanuusverkostojen perustamista palveluntarjoajien ja tuottajien kanssa tietojen vaihtamiseksi tämän direktiivin soveltamisalaan kuuluvien rikosten osalta.

(24) Tässä direktiivissä säädetyistä rikoksista on tarpeen kerätä vertailukelpoista tietoa. Merkitykselliset tiedot olisi saatettava unionin toimivaltaisten erityisvirastojen ja -elinten kuten Europolin ja ENISAn saataville niiden tehtävien ja tiedonsaantitarpeiden mukaisesti, jotta tietoverkkorikollisuutta sekä verkko- ja tietoturvallisuutta koskevasta ongelmasta saataisiin parempi käsitys unionin tasolla, millä edistettäisiin tehokkaampien vastatoimenpiteiden laatimista. Jäsenvaltioiden olisi toimitettava tietoja rikoksentekijöiden toimintatavasta Europolille ja sen Euroopan verkkorikostorjuntakeskukselle tietoverkkorikollisuutta koskevan uhka-arvioinnin ja sitä koskevien strategisten analyysien tekemiseksi Euroopan poliisiviraston (Europol) perustamisesta 6 päivänä huhtikuuta 2009 tehdyn neuvoston päätöksen 2009/371/YOS [1] mukaisesti. Tietojen toimittamisella voidaan helpottaa nykyisten ja tulevien uhkien parempaa ymmärtämistä ja edistää näin asianmukaisempaa ja kohdistetumpaa päätöksentekoa tietojärjestelmiin kohdistuvien hyökkäysten torjumiseksi ja ehkäisemiseksi.

(25) Komission olisi annettava kertomus tämän direktiivin soveltamisesta ja tehtävä tarpeelliset lainsäädäntöehdotukset, joilla mahdollisesti laajennettaisiin sen soveltamisalaa ottaen huomioon tietoverkkorikollisuuden alalla tapahtuva kehitys. Tällainen kehitys voisi sisältää teknologisen kehityksen, esimerkiksi sellaisen teknologisen kehityksen, jonka ansiosta voidaan tehokkaammin valvoa tietojärjestelmiin kohdistuvia hyökkäyksiä tai jolla helpotetaan tällaisten hyökkäysten ehkäisemistä tai niiden vaikutusten minimoimista. Komission olisi tätä tarkoitusta varten otettava huomioon saatavilla olevat asiaan kuuluvien toimijoiden ja erityisesti Europolin ja ENISAn laatimat analyysit ja raportit.

(26) Jotta tietoverkkorikollisuutta voidaan torjua tehokkaasti, on tarpeen vahvistaa tietojärjestelmien kestävyyttä toteuttamalla asianmukaisia toimia niiden suojaamiseksi tehokkaammin verkkohyökkäyksiltä. Jäsenvaltioiden olisi toteutettava tarpeelliset toimenpiteet suojatakseen niiden elintärkeät infrastruktuurit verkkohyökkäyksiltä, ja osana tätä niiden olisi tarkasteltava tietojärjestelmiensä ja niihin liittyvien tietojen suojaamista. Yksi olennainen osa kattavaa lähestymistapaa tietoverkkorikollisuuden torjumiseksi tehokkaasti on se, että oikeushenkilöt varmistavat tietojärjestelmien suojaamisen ja turvallisuuden asianmukaisen

[1] EUVL L 121, 15.5.2009, s. 37.

tason esimerkiksi julkisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamisen yhteydessä yksityisyyttä, sähköistä viestintää ja tietosuojaa koskevan unionin voimassa olevan lainsäädännön mukaisesti. Sellaisia uhkia ja haavoittuvaisuuksia vastaan, joiden voidaan kohtuudella katsoa olevan tunnistettavissa, olisi tarjottava asianmukainen suojan taso erityisalojen uusimpien keinojen ja erityisten tietojenkäsittelytilanteiden mukaisesti. Tällaisesta suojasta aiheutuvien kustannusten ja rasitteen olisi oltava oikeassa suhteessa verkkohyökkäyksen kohteiksi joutuneille aiheutuvaan todennäköiseen vahinkoon nähden. Jäsenvaltioita kannustetaan asiaankuuluviin toimiin kansallisen lakinsa puitteissa vastuun toteuttamiseksi tapauksissa, joissa oikeushenkilö ei selvästi ole tarjonnut asianmukaista suojaa verkkohyökkäyksiä vastaan.

(27) Merkittävät puutteet ja eroavuudet jäsenvaltioiden lainsäädännöissä ja rikosoikeudellisissa menettelyissä tietojärjestelmiin kohdistuvien hyökkäysten osalta saattavat vaikeuttaa järjestäytyneen rikollisuuden ja terrorismin torjuntaa sekä hankaloittaa tehokasta poliisi- ja oikeudellista yhteistyötä tällä alalla. Koska nykyaikaiset tietojärjestelmät eivät tunne maantieteellisiä rajoja, niihin kohdistuvilla hyökkäyksillä on rajat ylittävä ulottuvuus, mikä korostaa pikaista tarvetta lähentää edelleen jäsenvaltioiden rikosoikeutta tällä alalla. Lisäksi rikosoikeudenkäyntejä koskevien toimivaltaristiriitojen ehkäisemisestä ja ratkaisemisesta 30 päivänä marraskuuta 2009 annetun neuvoston puitepäätöksen 2009/948/YOS ([1]) asianmukaisen täytäntöönpanon ja soveltamisen pitäisi helpottaa tietojärjestelmiin kohdistuvia hyökkäyksiä koskevien syytetoimien yhteensovittamista. Jäsenvaltioiden olisi yhteistyössä unionin kanssa myös pyrittävä parantamaan tietojärjestelmien, tietokoneverkkojen ja datan turvallisuuteen liittyvää kansainvälistä yhteistyötä. Kaikissa tietojenvaihtoa koskevissa kansainvälisissä sopimuksissa olisi otettava asianmukaisesti huomioon tietojen siirron ja varastoimisen turvallisuus.

(28) Toimivaltaisten lainvalvonta- ja oikeusviranomaisten parempi yhteistyö unionissa on olennaisen tärkeää tietoverkkorikollisuuden tehokkaassa torjunnassa. Tässä yhteydessä olisi kannustettava tehostamaan toimia asianmukaisen koulutuksen tarjoamiseksi viranomaisille, jotta lisättäisiin ymmärrystä tietoverkkorikollisuudesta ja sen vaikutuksista ja edistettäisiin yhteistyötä ja parhaiden käytäntöjen vaihtoa esimerkiksi unionin toimivaltaisten erityisvirastojen ja -elimien välityksellä. Tällaisella koulutuksella olisi pyrittävä muun muassa lisäämään tietoisuutta erilaisista kansallisista oikeusjärjestelmistä, rikostutkinnan mahdollisista oikeudellisista ja teknisistä haasteista sekä toimivallan jaosta kansallisten viranomaisten välillä.

(29) Tässä direktiivissä kunnioitetaan ihmisoikeuksia ja perusvapauksia sekä noudatetaan erityisesti Euroopan unionin perusoikeuskirjassa ja ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä yleissopimuksessa tunnustettuja periaatteita, mukaan lukien henkilötietojen suoja, oikeus yksityisyyteen, sananvapaus ja tiedonvälityksen vapaus, oikeus oikeudenmukaiseen oikeudenkäyntiin, syyttömyysolettama ja puolustautumisoikeus sekä laillisuusperiaate ja rikoksista määrättävien rangaistusten oikeasuhteisuuden periaate. Tässä direktiivissä pyritään erityisesti varmistamaan näiden oikeuksien ja periaatteiden noudattaminen täysimääräisesti, ja se on pantava täytäntöön tämän mukaisesti.

(30) Henkilötietojen suoja on Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklan 1 kohdan sekä Euroopan unionin perusoikeuskirjan 8 artiklan mukaisesti perusoikeus. Sen vuoksi henkilötietojen käsittelyssä tämän direktiivin täytäntöönpanon yhteydessä olisi täysimääräisesti noudatettava asiaan kuuluvaa unionin tietosuojalainsäädäntöä.

(31) Euroopan unionista tehtyyn sopimukseen ja Euroopan unionin toiminnasta tehtyyn sopimukseen liitetyn, Yhdistyneen kuningaskunnan ja Irlannin asemasta vapauden, turvallisuuden ja oikeuden alueen osalta tehdyn pöytäkirjan 3 artiklan mukaisesti nämä jäsenvaltiot ovat ilmoittaneet haluavansa osallistua tämän direktiivin hyväksymiseen ja soveltamiseen.

(32) Euroopan unionista tehtyyn sopimukseen ja Euroopan unionin toiminnasta tehtyyn sopimukseen liitetyn, Tanskan asemasta tehdyn pöytäkirjan 1 ja 2 artiklan mukaisesti Tanska ei osallistu tämän direktiivin hyväksymiseen, direktiivi ei sido Tanskaa eikä sitä sovelleta Tanskaan.

(33) Jäsenvaltiot eivät voi riittävällä tavalla saavuttaa tämän direktiivin tavoitteita eli sitä, että tietojärjestelmiin kohdistuvista hyökkäyksistä määrätään kaikissa jäsenvaltioissa tehokkaat, oikeasuhteiset ja varoittavat rikosoikeudelliset seuraamukset ja että oikeusviranomaisten ja muiden toimivaltaisten viranomaisten välistä yhteistyötä tehostetaan ja siihen kannustetaan, vaan ne voidaan niiden laajuuden tai vaikutusten vuoksi saavuttaa paremmin unionin tasolla. Sen vuoksi unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Mainitussa artiklassa vahvistetun suhteellisuusperiaatteen mukaisesti tässä direktiivissä ei ylitetä sitä, mikä on näiden tavoitteiden saavuttamiseksi tarpeen.

(34) Tämän direktiivin tarkoituksena on muuttaa tietojärjestelmiin kohdistuvista hyökkäyksistä 24 päivänä helmikuuta 2005 tehdyn neuvoston puitepäätöksen 2005/222/YOS ([2]) säännöksiä ja laajentaa niiden soveltamisalaa. Koska muutokset ovat määrältään ja sisällöltään merkittäviä, puitepäätös 2005/222/YOS olisi selkeyden vuoksi korvattava kokonaisuudessaan tämän direktiivin hyväksymiseen osallistuvien jäsenvaltioiden osalta,

([1]) EUVL L 328, 15.12.2009, s. 42.

([2]) EUVL L 69, 16.3.2005, s. 67.

OVAT HYVÄKSYNEET TÄMÄN DIREKTIIVIN:

1 artikla

Kohde

Tässä direktiivissä vahvistetaan vähimmäissäännöt, jotka koskevat rikosten ja seuraamusten määrittelyä tietojärjestelmiin kohdistuvien hyökkäysten alalla. Sen tarkoituksena on myös helpottaa näiden rikosten estämistä ja parantaa oikeusviranomaisten ja muiden toimivaltaisten viranomaisten välistä yhteistyötä.

2 artikla

Määritelmät

Tässä direktiivissä tarkoitetaan:

a) 'tietojärjestelmällä' laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten, sekä dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään sen tai niiden toimintaa, käyttöä, suojausta tai huoltoa varten;

b) 'datalla' sellaisessa muodossa olevien tosiseikkojen, tietojen tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon;

c) 'oikeushenkilöllä' yksikköä, jolla on sovellettavan lain mukaan oikeushenkilön asema, lukuun ottamatta valtioita tai julkisia elimiä niiden käyttäessä julkista valtaa, tai julkisoikeudellisia kansainvälisiä järjestöjä;

d) ilmaisulla 'oikeudettomasti' tässä direktiivissä tarkoitettua toimintaa, mukaan lukien järjestelmään tunkeutuminen, sen häirintä tai tietojen hankkiminen, johon ei ole järjestelmän tai sen osan omistajan tai muun oikeudenhaltijan lupaa tai joka ei ole sallittua kansallisen lain nojalla.

3 artikla

Laiton tunkeutuminen tietojärjestelmään

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että tunkeutuminen tietojärjestelmään tai sen osaan tahallisesti ja oikeudettomasti on rikosoikeudellisesti rangaistava teko, kun tunkeutuminen on tehty murtamalla turvajärjestely, ainakin jos kyse ei ole vähäisestä tapauksesta.

4 artikla

Laiton järjestelmän häirintä

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että tietojärjestelmän toiminnan vakava estäminen tai keskeyttäminen tahallisesti ja oikeudettomasti dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla taikka saattamalla data käyttökelvottomaksi on rikosoikeudellisesti rangaistava teko, ainakin jos kyse ei ole vähäisestä tapauksesta.

5 artikla

Laiton datan vahingoittaminen

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että tietojärjestelmässä olevan datan tuhoaminen, vahingoittaminen, turmeleminen, muuttaminen, poistaminen tai saattaminen käyttökelvottomaksi tahallisesti ja oikeudettomasti on rikosoikeudellisesti rangaistava teko, ainakin jos kyse ei ole vähäisestä tapauksesta.

6 artikla

Viestintäsalaisuuden loukkaus (tietojen laiton hankkiminen)

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että teknisin keinoin tapahtuva tietojen hankkiminen tahallisesti ja oikeudettomasti tietojärjestelmän sisäisestä tai tietojärjestelmien välisestä luottamuksellisesta datan siirrosta, mukaan lukien tällaista dataa sisältävästä tietojärjestelmästä lähtevä sähkömagneettinen säteily, on rikosoikeudellisesti rangaistava teko, ainakin jos kyse ei ole vähäisestä tapauksesta.

7 artikla

Rikosten tekemiseen käytettävät välineet

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että seuraavien välineiden tuottaminen, myynti, käyttöön hankkiminen, tuonti, levittäminen tai muu saataville asettaminen tahallisesti ja oikeudettomasti ja tarkoituksin, että niitä käytetään 3–6 artiklassa tarkoitettujen rikosten tekemiseen, on rikosoikeudellisesti rangaistava teko, ainakin jos kyse ei ole vähäisestä tapauksesta:

a) tietokoneohjelma, joka on suunniteltu tai muutettu ensisijaisesti 3–6 artiklassa tarkoitettujen rikosten tekemistä varten;

b) tietojärjestelmän salasana, pääsykoodi tai muu vastaava tieto, joka mahdollistaa pääsyn tietojärjestelmään tai sen osaan.

8 artikla

Yllytys, avunanto ja yritys

1. Jäsenvaltioiden on varmistettava, että yllytys tai avunanto 3–7 artiklassa tarkoitettuihin rikoksiin on rikosoikeudellisesti rangaistava teko.

2. Jäsenvaltioiden on varmistettava, että 4 ja 5 artiklassa tarkoitettujen rikosten yritys on rikosoikeudellisesti rangaistava teko.

9 artikla

Seuraamukset

1. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 3–8 artiklassa tarkoitetuista rikoksista voidaan määrätä tehokkaat, oikeasuhteiset ja varoittavat rikosoikeudelliset seuraamukset.

2. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 3–7 artiklassa tarkoitetuista rikoksista säädetään vankeusrangaistus, jonka enimmäiskesto on vähintään kaksi vuotta, ainakin jos kyse ei ole vähäisestä tapauksesta.

3. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 4 ja 5 artiklassa tarkoitetuista rikoksista säädetään vankeusrangaistus, jonka enimmäiskesto on vähintään kolme vuotta, kun ne on tehty tahallisesti ja kun on vaikutettu

merkittävään määrään tietojärjestelmiä käyttämällä 7 artiklassa tarkoitettua välinettä, joka on suunniteltu tai muutettu ensisijaisesti tätä tarkoitusta varten.

4. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 4 ja 5 artiklassa tarkoitetuista rikoksista säädetään vankeusrangaistus, jonka enimmäiskesto on vähintään viisi vuotta, kun

a) ne on tehty rikollisjärjestön puitteissa, sellaisena kuin se on määritelty puitepäätöksessä 2008/841/YOS, riippumatta siitä, mikä on siinä säädetty seuraamus;

b) ne aiheuttavat vakavaa vahinkoa; tai

c) ne kohdistuvat elintärkeään infrastruktuuriin kuuluvaan tietojärjestelmään.

5. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, 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 kansallisen lain mukaisesti rangaistavan rikoksen tunnusmerkistöön.

10 artikla

Oikeushenkilöiden vastuu

1. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että oikeushenkilöt voidaan saattaa vastuuseen 3–8 artiklassa tarkoitetuista rikoksista, jotka on oikeushenkilön hyväksi tehnyt joko yksin tai oikeushenkilön elimen jäsenenä toimiva henkilö, jonka johtava asema oikeushenkilössä perustuu johonkin seuraavista:

a) oikeus edustaa oikeushenkilöä;

b) valtuus tehdä päätöksiä oikeushenkilön puolesta;

c) valtuus harjoittaa valvontaa oikeushenkilössä.

2. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että oikeushenkilöt voidaan saattaa vastuuseen, jos 1 kohdassa tarkoitetun henkilön harjoittaman ohjauksen tai valvonnan puutteellisuus on mahdollistanut sen, että oikeushenkilön alaisuudessa toimiva henkilö on tehnyt 3–8 artiklassa tarkoitettuja rikoksia kyseisen oikeushenkilön hyväksi.

3. Edellä 1 ja 2 kohdassa tarkoitettu oikeushenkilöiden vastuu ei estä rikosoikeudellista menettelyä sellaisia luonnollisia henkilöitä vastaan, jotka ovat tekijöinä, yllyttäjinä tai avunantajina 3–8 artiklassa tarkoitetuissa rikoksissa.

11 artikla

Oikeushenkilöille määrättävät seuraamukset

1. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 10 artiklan 1 kohdan mukaisesti vastuulliseksi todettua oikeushenkilöä voidaan rangaista tehokkain, oikeasuhteisin ja varoittavin seuraamuksin, joihin kuuluvat rikosoikeudelliset tai muut sakot ja joihin voi kuulua muita seuraamuksia, kuten:

a) oikeuden menettäminen julkisista varoista myönnettäviin etuuksiin tai tukiin;

b) väliaikainen tai pysyvä kielto harjoittaa liiketoimintaa;

c) tuomioistuimen valvontaan asettaminen;

d) tuomioistuimen määräys purkaa oikeushenkilö;

e) rikoksen tekemiseen käytettyjen tilojen sulkeminen väliaikaisesti tai pysyvästi.

2. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 10 artiklan 2 kohdan mukaisesti vastuulliseksi todettua oikeushenkilöä voidaan rangaista seuraamuksilla tai muilla toimenpiteillä, jotka ovat tehokkaita, oikeasuhteisia ja varoittavia.

12 artikla

Lainkäyttövalta

1. Jäsenvaltioiden on ulotettava lainkäyttövaltansa 3–8 artiklassa tarkoitettuihin rikoksiin, jos

a) rikos on tehty kokonaan tai osittain niiden alueella; tai

b) rikoksen on tehnyt niiden kansalainen, ainakin jos teko katsotaan rikokseksi siellä, missä se tehtiin.

2. Ulottaessaan lainkäyttövaltansa 1 kohdan a alakohdan mukaisesti jäsenvaltion on varmistettava, että sillä on lainkäyttövalta, kun

a) rikoksentekijä tekee rikoksen ollessaan fyysisesti sen alueella, riippumatta siitä, kohdistuuko rikos sen alueella sijaitsevaan tietojärjestelmään; tai

b) rikos kohdistuu sen alueella sijaitsevaan tietojärjestelmään, riippumatta siitä, tekeekö rikoksentekijä rikoksen ollessaan fyysisesti sen alueella.

3. Jäsenvaltion on ilmoitettava komissiolle, jos se päättää ulottaa lainkäyttövaltansa alueensa ulkopuolella tehtyyn 3–8 artiklassa tarkoitettuun rikokseen, mukaan lukien silloin, kun

a) rikoksentekijän vakinainen asuinpaikka on sen alueella; tai

b) rikos on tehty sen alueelle sijoittautuneen oikeushenkilön hyväksi.

13 artikla

Tietojenvaihto

1. Jäsenvaltioiden on varmistettava, että niillä on toimiva kansallinen yhteyspiste ja että ne hyödyntävät nykyistä ympärivuorokautisesti ja kaikkina viikonpäivinä toimivien yhteyspisteiden verkostoa 3–8 artiklassa tarkoitettuja rikoksia koskevaa tietojenvaihtoa varten. Jäsenvaltioiden on myös huolehdittava siitä, että niillä on käytettävissä menettelyt, jotta toimivaltainen viranomainen voi kiireellisten avunpyyntöjen osalta ilmoittaa 8 tunnin kuluessa pyynnön vastaanottamisesta ainakin sen, vastataanko pyyntöön sekä missä muodossa ja arviolta milloin tällainen vastaus toimitetaan.

2. Jäsenvaltioiden on ilmoitettava komissiolle 1 kohdassa tarkoitettu nimetty yhteyspiste. Komissio toimittaa tämän tiedon muille jäsenvaltioille sekä unionin toimivaltaisille erityisvirastoille ja -elimille.

3. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että käytettävissä on asianmukaiset ilmoituskanavat, jotta helpotetaan sitä, että 3–6 artiklassa tarkoitetuista rikoksista voidaan ilmoittaa toimivaltaisille kansallisille viranomaisille ilman aiheetonta viivytystä.

14 artikla

Seuranta ja tilastot

1. Jäsenvaltioiden on varmistettava, että niillä on järjestelmä, jonka avulla voidaan kirjata, tuottaa ja antaa tilastotietoja 3–7 artiklassa tarkoitetuista rikoksista.

2. Edellä 1 kohdassa tarkoitettujen tilastotietojen on katettava vähintään olemassa olevat tiedot 3–7 artiklassa tarkoitettujen, jäsenvaltioiden rekisteröimien rikosten lukumäärästä sekä 3–7 artiklassa tarkoitetuista rikoksista syytteeseen asetettujen ja tuomittujen henkilöiden lukumäärästä.

3. Jäsenvaltioiden on toimitettava tämän artiklan nojalla kerätyt tiedot komissiolle. Komission on varmistettava, että tilastollisista kertomuksista julkaistaan konsolidoitu selvitys, joka toimitetaan unionin toimivaltaisille erityisvirastoille ja -elimille.

15 artikla

Puitepäätöksen 2005/222/YOS korvaaminen

Korvataan puitepäätös 2005/222/YOS tämän direktiivin hyväksymiseen osallistuvien jäsenvaltioiden osalta rajoittamatta kuitenkaan näiden jäsenvaltioiden velvollisuutta noudattaa määräaikaa, johon mennessä puitepäätös on saatettava osaksi kansallista lainsäädäntöä.

Tämän direktiivin hyväksymiseen osallistuvien jäsenvaltioiden osalta viittauksia puitepäätökseen 2005/222/YOS pidetään viittauksina tähän direktiiviin.

16 artikla

Saattaminen osaksi kansallista lainsäädäntöä

1. Jäsenvaltioiden on saatettava tämän direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset voimaan viimeistään 4 päivänä syyskuuta 2015.

2. Jäsenvaltioiden on toimitettava komissiolle kirjallisina ne säännökset, joilla jäsenvaltioiden tästä direktiivistä aiheutuvat velvoitteet saatetaan osaksi kansallista lainsäädäntöä.

3. Näissä jäsenvaltioiden antamissa säädöksissä on viitattava tähän direktiiviin tai niihin on liitettävä tällainen viittaus, kun ne virallisesti julkaistaan. Jäsenvaltioiden on säädettävä siitä, miten viittaukset tehdään.

17 artikla

Raportointi

Komissio toimittaa viimeistään 4 päivänä syyskuuta 2017 Euroopan parlamentille ja neuvostolle kertomuksen, jossa arvioidaan, missä määrin jäsenvaltiot ovat toteuttaneet tämän direktiivin noudattamisen edellyttämät toimenpiteet, ja johon liitetään tarvittaessa lainsäädäntöehdotuksia. Komissio ottaa huomioon myös tietoverkkorikollisuuden alalla tapahtuneen teknisen ja oikeudellisen kehityksen erityisesti tämän direktiivin soveltamisalalla.

18 artikla

Voimaantulo

Tämä direktiivi tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

19 artikla

Osoitus

Tämä direktiivi on osoitettu jäsenvaltioille perussopimusten mukaisesti.

Tehty Brysselissä 12 päivänä elokuuta 2013.

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*
M. SCHULZ	L. LINKEVIČIUS