EUROOPAN KOMISSIO

Bryssel 30.9.2010
KOM(2010) 517 lopullinen

2010/0273 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI

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

{SEC(2010) 1122} final
{SEC(2010) 1123}final

PERUSTELUT

1. EHDOTUKSEN PERUSTELUT JA TAVOITTEET

Ehdotuksen tarkoituksena on korvata tietojärjestelmiin kohdistuvista hyökkäyksistä 24 päivänä helmikuuta 2005 tehty neuvoston puitepäätös 2005/222/YOS[1]. Kuten puitepäätöksen johdanto-osan kappaleissa todettiin, sen tavoitteena oli parantaa jäsenvaltioiden oikeus- ja muiden toimivaltaisten viranomaisten, kuten poliisin ja muiden erikoistuneiden lainvalvontaviranomaisten, välistä yhteistyötä lähentämällä tietojärjestelmiin kohdistuvia hyökkäyksiä koskevia jäsenvaltioiden rikosoikeudellisia säännöksiä. Sillä otettiin käyttöön EU:n lainsäädäntöä, jolla voitiin puuttua sellaisiin rikoksiin kuin laiton tunkeutuminen tietojärjestelmään, laiton järjestelmän häirintä ja laiton datan vahingoittaminen ja johon sisältyivät säännöt oikeushenkilöiden vastuusta, lainkäyttövallasta ja tietojenvaihdosta. Jäsenvaltioiden oli toteutettava puitepäätöksen säännösten noudattamisen edellyttämät toimenpiteet viimeistään 16. maaliskuuta 2007.

Komissio julkaisi 14. heinäkuuta 2008 kertomuksen[2] puitepäätöksen täytäntöönpanosta. Kertomuksen päätelmissä todettiin, että merkittävää edistymistä oli tapahtunut useimmissa jäsenvaltioissa ja että täytäntöönpanon tasoa voitiin pitää suhteellisen hyvänä. Täytäntöönpano oli kuitenkin vielä kesken eräissä jäsenvaltioissa. Lisäksi kertomuksessa todettiin, että ”puitepäätöksen tekemisen jälkeen on noussut esiin uusia uhkakuvia eri puolilla Eurooppaa tehtyjen hyökkäysten myötä. Näitä uusia uhkia ovat erityisesti tietojärjestelmiin kohdistuvat yhtäaikaiset, laajamittaiset hyökkäykset ja niin kutsuttujen bottiverkkojen rikollisen käytön lisääntyminen.” Puitepäätöstä tehtäessä ei vielä osattu varautua tällaisiin hyökkäyksiin. Tämän kehityksen vuoksi komissio harkitsee sellaisten toimenpiteiden toteuttamista, joiden avulla uhka voitaisiin torjua tehokkaammin (ks. bottiverkon selitys seuraavassa jaksossa).

Tietoverkkorikollisuuden torjunnan parantamiseksi toteutettavien lisätoimien merkitystä korostettiin vuonna 2004 hyväksytyssä Haagin ohjelmassa vapauden, turvallisuuden ja oikeuden lujittamiseksi Euroopan unionissa sekä vuonna 2009 hyväksytyssä Tukholman ohjelmassa ja siihen liittyvässä toimintasuunnitelmassa[3]. Lisäksi jokin aika sitten esitetyssä Euroopan digitaalistrategiassa[4], joka on Eurooppa 2020 -strategian ensimmäinen lippulaivahanke, todettiin tarve puuttua uudenlaisiin rikoksen muotoihin, erityisesti tietoverkkorikoksiin Euroopan tasolla. Komissio on luotettavuuteen ja turvallisuuteen keskittyvällä toiminta-alalla sitoutunut toimenpiteisiin, joiden tarkoituksena on torjua tietojärjestelmiin kohdistuvat verkkohyökkäykset.

Tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen, joka allekirjoitettiin 23. marraskuuta 2001, katsotaan olevan tähän mennessä täydellisin kansainvälinen standardi, sillä se tarjoaa kattavan ja johdonmukaisen kehyksen tietoverkkorikollisuuden eri muotoihin puuttumista varten.[5] Tähän mennessä yleissopimuksen ovat allekirjoittaneet kaikki

---

1 EUVL L 69, 16.3.2005, s. 68.

2 Komission kertomus neuvostolle tietojärjestelmiin kohdistuvista hyökkäyksistä 24 päivänä helmikuuta 2005 tehdyn neuvoston puitepäätöksen 12 artiklan perusteella, KOM(2008) 448.

3 EUVL C 198, 12.8.2005, EUVL C 115, 4.5.2010, KOM(2010) 171, 20.4.2010.

4 Komission tiedonanto KOM(2010) 245, 19.5.2010.

5 Tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus, Budapest 23.11.2001, CETS nro 185.

27 jäsenvaltiota, mutta vain 15 jäsenvaltiota on ratifioinut sen.[6] Yleissopimus tuli voimaan 1. heinäkuuta 2004. EU ei ole yleissopimuksen allekirjoittaja. Koska kyseessä on erittäin tärkeä yleissopimus, komissio kehottaa kaikkia niitä EU:n jäsenvaltioita, jotka eivät vielä ole ratifioineet yleissopimusta, tekemään sen mahdollisimman pian.

- **Yleinen tausta**

Tietoverkkorikollisuuden suurin syy on eri tekijöistä johtuva haavoittuvuus. Lainvalvontamekanismien riittämättömät toimet helpottavat näiden ilmiöiden esiintymistä ja pahentavat niistä aiheutuvia vaikeuksia, sillä tietyntyyppiset rikokset ovat kansainvälisiä. Raportointi tämän tyyppisestä rikollisuudesta on usein riittämätöntä osaksi siksi, että eräitä rikoksia ei havaita, ja osaksi siksi, että uhrit (toiminnanharjoittajat ja yritykset) eivät ilmoita rikoksista pelätessään saavansa huonon maineen ja haavoittuvuutensa julkitulon vaikuttavan tuleviin liiketoimintamahdollisuuksiin.

Lisäksi kansallisten rikoslainsäädäntöjen ja menettelyjen eroavaisuudet voivat johtaa eroihin tutkinnassa ja syytetoimissa, minkä johdosta eroavaisuuksia on myös tavassa, jolla näihin rikoksiin puututaan. Tietotekniikan kehitys on pahentanut näitä ongelmia, sillä kehityksen myötä on helpompi tuottaa ja levittää välineitä (haittaohjelmia ja bottiverkkoja), rikoksentekijät voivat toimia anonyymisti ja vastuu teoista jakautuu eri lainkäyttöalueille. Syytteen nostamiseen liittyvien vaikeuksien vuoksi järjestäytynyt rikollisuus voi saada huomattavia voittoja riskin ollessa vähäinen.

Tässä ehdotuksessa otetaan huomioon uudet tietoverkkorikollisuuden menetelmät, erityisesti bottiverkkojen käyttö. ’Bottiverkolla’ tarkoitetaan haittaohjelmien (tietokonevirusten) saastuttamien tietokoneiden muodostamaa verkkoa. Tällainen kaapattujen tietokoneiden (zombie-koneiden) muodostama verkko voidaan saada toimimaan halutulla tavalla, esimerkiksi hyökkäämään tietojärjestelmiä vastaan (tietoverkkohyökkäykset). Näitä zombie-koneita voi hallita toinen tietokone usein käyttäjien sitä tietämättä. Tätä isäntäkonetta kutsutaan myös komentopalvelimeksi. Komentopalvelinta hallinnoivat henkilöt ovat myös rikoksentekijöitä, sillä he käyttävät kaapattuja tietokoneita käynnistääkseen hyökkäyksiä tietojärjestelmiä vastaan. Näitä henkilöitä on erittäin vaikea jäljittää, sillä bottiverkon muodostavat ja hyökkäyksen tekevät tietokoneet voivat olla eri paikassa kuin rikoksentekijä itse.

Bottiverkon tekemät hyökkäykset ovat usein laajamittaisia. Laajamittaisia hyökkäyksiä ovat hyökkäykset, jotka voidaan toteuttaa sellaisten välineiden avulla, jotka vaikuttavat merkittävään määrään tietojärjestelmiä (tietokoneita), tai hyökkäykset, jotka aiheuttavat huomattavaa vahinkoa esimerkiksi järjestelmäpalvelujen keskeytyksinä, taloudellisina kustannuksina ja henkilötietojen menetyksinä. Laajamittaisten hyökkäysten aiheuttamilla vahingoilla on merkittävä vaikutus itse kohteen toimintaan ja/tai kohteen toimintaympäristöön. Tässä yhteydessä ’suurella bottiverkolla’ tarkoitetaan verkkoa, joka kapasiteettinsa ansiosta pystyy aiheuttamaan vakavaa vahinkoa. On vaikea määritellä bottiverkkoja koon mukaan, mutta suurimmissa bottiverkoissa on arvioitu olleen 40 000–100 000 liittymää (ts. tietokonetta) 24 tunnin ajanjaksolla[7].

---

6 Yleissopimuksen ratifiointia koskeva yleiskatsaus (CETS nro 185) on internet-osoitteessa http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

7 Liittymien määrä 24 tunnin ajalta on yleisesti käytetty mittayksikkö, kun arvioidaan bottiverkkojen kokoa.

- **Voimassa olevat aiemmat säännökset**

EU:n tasolla puitepäätöksellä lähennettiin vähimmäistason verran jäsenvaltioiden lainsäädäntöä monien tietoverkkorikosten säätämiseksi rangaistaviksi, mukaan lukien laiton tunkeutuminen tietojärjestelmään, laiton järjestelmän häirintä, laiton datan vahingoittaminen sekä rikokseen yllyttäminen ja avunanto tai rikoksen yritys.

Vaikka jäsenvaltiot ovat yleensä panneet puitepäätöksen säännökset täytäntöön, päätöksessä on monia puutteita, kun otetaan huomioon rikosten (tietoverkkohyökkäykset) kokoon ja lukumäärään liittyvät suuntaukset. Puitepäätöksellä lähennetään lainsäädäntöä vain muutamien rikosten osalta, eikä siinä käsitellä täysimääräisesti laajamittaisista hyökkäyksistä yhteiskuntaan kohdistuvaa mahdollista uhkaa. Siinä ei myöskään oteta riittävästi huomioon rikosten vakavuutta ja niistä langetettavia seuraamuksia.

Myös muiden voimassa olevien tai suunniteltujen EU:n hankkeiden ja ohjelmien puitteissa puututaan tietoverkkohyökkäyksiin liittyviin ongelmiin tai käsitellään sellaisia seikkoja kuin verkkoturvallisuus ja internetin käyttäjien turvallisuus. Näitä ovat toimet, joita tuetaan rikosten ehkäisemistä ja torjuntaa koskevan ohjelman[8], rikosoikeuden ohjelman[9], internetin käyttöturvallisuutta koskevan ohjelman[10] ja elintärkeää tietoinfrastruktuuria koskevan aloitteen[11] puitteissa. Puitepäätöksen lisäksi toinen tärkeä voimassa oleva oikeudellinen väline on lasten seksuaalisen hyväksikäytön ja lapsipornografian torjumisesta tehty puitepäätös 2004/68/YOS.

Hallinnollisella tasolla tietokoneiden saastuttaminen niin, että niistä tulee bottiverkkoja, on jo kielletty EU:n yksityisyyden suojaa ja tietosuojaa koskevien sääntöjen[12] perusteella. Erityisesti kansalliset hallintoelimet toimivat jo yhteistyössä roskapostikysymystä käsittelevien viranomaisten yhteysverkoston kanssa. Kyseisten sääntöjen perusteella jäsenvaltioiden on kiellettävä viestien sieppaaminen julkisissa viestintäverkoissa ja julkisesti saatavilla olevissa sähköisissä viestintäpalveluissa ilman asianomaisten käyttäjien lupaa tai laillista valtuutusta.

Ehdotus noudattaa näitä sääntöjä. Jäsenvaltioiden olisi kiinnitettävä huomiota hallinto- ja lainvalvontaviranomaisten välisen yhteistyön parantamiseen asioissa, joihin liittyy sekä hallinnollisia että rikosoikeudellisia seuraamuksia.

- **Johdonmukaisuus suhteessa unionin muuhun politiikkaan ja muihin tavoitteisiin**

Tavoitteet ovat johdonmukaisia järjestäytyneen rikollisuuden torjuntaa, tietokoneverkkojen vahvistamista, elintärkeiden tietoinfrastruktuurien suojelua ja tietosuojaa koskevien EU:n politiikkojen kanssa. Tavoitteet ovat myös internetin käyttöturvallisuutta koskevan ohjelman mukaisia. Kyseinen ohjelma perustettiin edistämään internetin ja uusien online-teknologioiden turvallisempaa käyttöä ja torjumaan laitonta sisältöä.

---

8 Ks. http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 Ks. http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm

10 Ks. http://ec.europa.eu/information_society/activities/sip/index_en.htm

11 Ks. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12 Direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (EYVL L 201, 31.7.2002), sellaisena kuin se on muutettuna direktiivillä 2009/136/EY (EUVL L 337, 18.12.2009).

Ehdotusta on tarkasteltu perusteellisesti sen varmistamiseksi, että säännökset ovat täysin perusoikeuksien ja erityisesti henkilötietojen suojan, sananvapauden ja tiedonvälityksen vapauden, oikeudenmukaista oikeudenkäyntiä koskevan oikeuden, syyttömyysolettaman ja puolustautumisoikeuden sekä laillisuusperiaatteen ja rikoksista määrättävien rangaistusten oikeasuhteisuuden periaatteen mukaiset.

2. KUULEMISET JA VAIKUTUSTEN ARVIOINTI

- **Intressitahojen kuuleminen**

Alan asiantuntijoita kuultiin laajalti useissa kokouksissa, joissa käsiteltiin tietoverkkorikollisuuden torjuntaan liittyviä seikkoja, mukaan lukien rikoksista johtuvat oikeudelliset jatkotoimet (syytetoimet). Erityisesti kuultiin jäsenvaltioiden hallitusten ja yksityissektorin, näihin kysymyksiin erikoistuneiden tuomarien ja syyttäjien, kansainvälisten järjestöjen, EU:n virastojen ja asiantuntijaelimien edustajia. Useat asiantuntijat ja organisaatiot ovat myöhemmin toimittaneet komissiolle lausuntoja ja antaneet tietoja.

Kuulemisen yhteydessä nousivat esille seuraavat keskeiset seikat:

– EU:n toimien tarve tällä alalla,

– tarve kriminalisoida nykyisen puitepäätöksen ulkopuolelle jäävät rikosmuodot, erityisesti uudenlaiset tietoverkkohyökkäykset (bottiverkot),

– tarve poistaa kansainvälisissä tapauksissa tutkinnan ja syytetoimien tiellä olevat esteet.

Kuulemisen aikana saatu palaute on otettu huomioon vaikutusten arvioinnissa.

Asiantuntijatiedon käyttö

Ulkopuolisia asiantuntijoita on kuultu sidosryhmien kanssa käydyissä kokouksissa.

Vaikutusten arviointi

Asetettujen tavoitteiden saavuttamiseksi on selvitetty eri toimintavaihtoehtoja.

- Toimintavaihtoehto 1: nykytilanteen säilyttäminen / ei uusia EU:n toimia

Tämä vaihtoehto tarkoittaa sitä, että EU ei toteuta uusia toimia tämäntyyppisen tietoverkkorikollisuuden eli tietojärjestelmiin kohdistuvien hyökkäysten torjumiseksi. Käynnissä olevia toimia jatketaan, erityisesti ohjelmia, joiden tavoitteena on lujittaa elintärkeän tietoinfrastruktuurin suojaamista ja parantaa julkisen ja yksityisen sektorin yhteistyötä tietoverkkorikollisuuden torjumiseksi.

- Toimintavaihtoehto 2: ohjelman laatiminen tietojärjestelmiin kohdistuvien hyökkäysten torjunnan lujittamiseksi muilla kuin lainsäädännöllisillä toimenpiteillä

Elintärkeän tietoinfrastruktuurin suojaamiseen tähtäävän ohjelman lisäksi muissa kuin lainsäädännöllisissä toimenpiteissä keskityttäisiin rajatylittävään lainvalvontaan ja julkisen ja yksityisen sektorin yhteistyöhön. Näiden pehmeiden sääntelyvälineiden tavoitteena olisi oltava koordinoitujen toimien edistäminen EU:n tasolla, mukaan lukien lainvalvontaviranomaisten yhteyspisteistä koostuvan nykyisen ympärivuorokautisen

verkoston lujittaminen, tietoverkkorikollisuuden asiantuntijoista ja lainvalvontaviranomaisista koostuvan julkisen ja yksityisen sektorin yhteyspisteiden muodostaman EU:n verkoston perustaminen, vakiomuotoisen EU:n palvelusopimuksen laatiminen yksityisen sektorin toimijoiden kanssa tehtävää lainvalvontayhteistyötä varten ja lainvalvontaviranomaisille suunnattujen tietoverkkorikoksien tutkintaa koskevien koulutusohjelmien järjestämisen tukeminen.

- Toimintavaihtoehto 3: puitepäätöksen sääntöjen kohdennettu päivittäminen (nykyisen puitepäätöksen korvaaminen uudella direktiivillä), jotta voidaan puuttua tietojärjestelmiin kohdistuvien laajamittaisten hyökkäysten (bottiverkot) uhkaan, ja kun on kyse teoista, jotka on tehty salaamalla rikoksentekijän todellinen henkilöllisyys ja aiheuttamalla vahinkoa henkilöllisyyden oikealle omistajalle, parantaa jäsenvaltioiden lainvalvontaviranomaisten yhteyspisteiden tehokkuutta ja korjata tietoverkkohyökkäyksiä koskevien tilastotietojen puute.

Tässä vaihtoehdossa otetaan käyttöön kohdennettu (ts. rajoitettu) lainsäädäntö tarkoituksena torjua tietojärjestelmiin kohdistuvia laajamittaisia hyökkäyksiä. Näin vahvistettuun lainsäädäntöön liittyisi muita kuin lainsäädännöllisiä toimenpiteitä, joiden tarkoituksena olisi lujittaa rajatylittävää operatiivista yhteistyötä kyseisenlaisten hyökkäysten torjumiseksi. Tämä helpottaisi lainsäädäntötoimenpiteiden täytäntöönpanoa. Näiden toimenpiteiden tavoitteena olisi parantaa elintärkeän tietoinfrastruktuurin valmiuksia, turvallisuutta ja kestävyyttä sekä vaihtaa tietoja parhaista käytänteistä.

- Toimintavaihtoehto 4: tietoverkkorikollisuuden torjumiseen tähtäävän kattavan EU-lainsäädännön käyttöön ottaminen

Tähän vaihtoehtoon liittyisi uusi kattava EU:n lainsäädäntö. Toimintavaihtoehtoon 2 sisältyvien pehmeiden sääntelyvälineiden lisäksi ja toimintavaihtoehtoon 3 liittyvän päivittämisen lisäksi tässä toimintavaihtoehdossa puututtaisiin myös muihin internetin käyttöön liittyviin oikeudellisiin ongelmiin. Toimenpiteiden piiriin eivät kuuluisi pelkästään tietojärjestelmiin kohdistuvat hyökkäykset, vaan myös sellaiset seikat kuin talousalan tietoverkkorikollisuus, laiton internetsisältö, sähköisten todisteiden kerääminen/säilyttäminen/siirtäminen ja lainkäyttövaltaa koskevat yksityiskohtaisemmat säännöt. Lainsäädäntöä sovellettaisiin rinnakkain tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen kanssa, ja siihen sisältyisivät edellä mainitut muut kuin lainsäädännölliset toimenpiteet.

- Toimintavaihtoehto 5: tietoverkkorikollisuutta koskevan Euroopan neuvoston yleissopimuksen päivittäminen

Tämän vaihtoehdon toteutuminen edellyttäisi huomattavia uudelleenneuvotteluja nykyisestä yleissopimuksesta. Se olisi pitkällinen prosessi ja vastoin vaikutusten arvioinnissa ehdotettua toiminta-aikataulua. Kansainvälisesti ei myöskään näytä olevan halukkuutta neuvotella yleissopimus uudelleen. Yleissopimuksen päivittämistä ei sen vuoksi voida katsoa toteuttamiskelpoiseksi vaihtoehdoksi, koska se ei sovi vaaditun toiminta-aikataulun puitteisiin.

Parhaaksi arvioitu toimintavaihtoehto: muiden kuin lainsäädännöllisten toimenpiteiden (vaihtoehto 2) ja puitepäätöksen kohdennetun päivittämisen (vaihtoehto 3) yhdistelmä

Taloudellisten, sosiaalisten ja perusoikeuksiin kohdistuvien vaikutusten analyysin perusteella vaihtoehdot 2 ja 3 tarjoavat parhaan lähestymistavan ongelmaan ja niillä saavutetaan ehdotuksen tavoitteet.

Valmistellessaan tätä ehdotusta komissio teki vaikutusten arvioinnin.

3. EHDOTUKSEEN LIITTYVÄT OIKEUDELLISET NÄKÖKOHDAT

- **Ehdotetun toimen lyhyt kuvaus**

Vaikka direktiivillä kumotaan puitepäätös 2005/222/YOS, siinä säilytetään puitepäätöksen nykyiset säännökset ja siihen sisällytetään seuraavat uudet seikat:

– Aineellisen rikosoikeuden osalta yleensä

A. Direktiivissä säädetään rangaistavaksi rikoksen tekemisessä käytettyjen laitteiden tai välineiden tuotanto, myynti, hankkiminen, tuonti, levittäminen tai muu saataville asettaminen.

B. Direktiiviin sisältyvät seuraavat raskauttavat olosuhteet:

- hyökkäysten laajamittaisuus – bottiverkkoihin tai vastaaviin välineisiin puututtaisiin ottamalla käyttöön uusi raskauttava tekijä, toisin sanoen bottiverkon tai vastaavan välineen perustaminen olisi raskauttava tekijä, kun syyllistytään nykyisessä puitepäätöksessä lueteltuihin rikoksiin;

- kun kyseiset hyökkäykset toteutetaan salaamalla rikoksentekijän todellinen henkilöllisyys ja aiheutetaan vahinkoa henkilöllisyyden oikealle haltijalle. Näiden sääntöjen olisi noudatettava laillisuusperiaatetta ja rikoksista määrättävien rangaistusten oikeasuhteisuuden periaatetta ja niiden olisi oltava yhdenmukaiset voimassa olevan henkilötietojen suojaa koskevan lainsäädännön kanssa[13].

C. Direktiivissä määritellään ’viestintäsalaisuuden loukkaaminen (tietojen laiton sieppaus)’ rangaistavaksi teoksi.

D. Direktiivillä otetaan käyttöön toimenpiteitä, joiden tarkoituksena on parantaa rikosoikeudellista yhteistyötä Euroopassa lujittamalla nykyistä ympärivuorokautista yhteyspisteverkostoa[14]:

- ehdotetaan velvollisuutta vastata yhteyspisteiden esittämään avunantopyyntöön (direktiivin 14 artikla) tietyssä määräajassa. Tietoverkkorikollisuutta koskevassa yleissopimuksessa ei ole tämänkaltaista sitovaa määräystä. Toimenpiteen

---

[13] Esimerkiksi Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (EYVL L 201, 31.7.2002, s. 37) (parhaillaan tarkistettavana) sekä yleinen tietosuojadirektiivi 95/46/EY.

[14] Otettu käyttöön yleissopimuksella ja tietojärjestelmiin kohdistuvista hyökkäyksistä tehdyllä puitepäätöksellä 2005/222/YOS.

tarkoituksena on varmistaa, että yhteyspisteet ilmoittavat määräajassa, pystyvätkö ne vastaamaan avunantopyyntöön ja mihin mennessä pyynnön esittänyt yhteyspiste voi odottaa ratkaisua. Ratkaisujen sisältöä ei ole määritelty.

E. Direktiivillä puututaan tarpeeseen saada tilastotietoja tietoverkkorikoksista velvoittamalla jäsenvaltiot varmistamaan, että niillä on asianmukainen järjestelmä, jonka avulla voidaan kirjata, tuottaa ja antaa tilastotietoja nykyisessä puitepäätöksessä mainituista rikoksista sekä direktiiviin lisätystä viestintäsalaisuuden loukkaamisesta.

Direktiivin 3, 4 ja 5 artiklassa lueteltujen rikosten (laiton tunkeutuminen tietojärjestelmään, laiton järjestelmän häirintä ja laiton datan vahingoittaminen) määritelmiin sisältyy säännös, jonka nojalla teot voidaan direktiivin kansallista täytäntöönpanolainsäädäntöä annettaessa säätää rangaistaviksi ”ainakin jos kyse ei ole vähäisestä tapauksesta”. Joustavuuden tarkoituksena on antaa jäsenvaltioille mahdollisuus olla rankaisematta teoista, jotka *in abstracto* kuuluvat perusmääritelmän soveltamisalaan, mutta joiden ei katsota vahingoittavan suojattavaa oikeudellista etua. Tällä tarkoitetaan esimerkiksi tekoja, joiden avulla nuoret IT-harrastajat ovat halunneet osoittaa näppäryyttään. Mahdollisuus rajoittaa rikosoikeudellista vastuuta ei kuitenkaan saa johtaa sellaisten uusien rikoksen tunnusmerkkien käyttöönottoon, jotka eivät sisälly direktiiviin. Se voisi johtaa tilanteeseen, jossa rangaistaviksi katsottaisiin ainoastaan raskauttavien olosuhteiden vallitessa tehdyt teot. Antaessaan direktiivin kansallista täytäntöönpanolainsäädäntöä jäsenvaltioiden olisi erityisesti pidättäydyttävä lisäämästä perustavanlaatuisiin tekoihin uusia rikoksen tunnusmerkkejä, esimerkiksi edellytystä, että teon erityisenä tarkoituksena on saada rikoksesta laitonta hyötyä, tai että teolla on erityinen vaikutus, kuten huomattavan vahingon aiheuttaminen.

- **Oikeusperusta**

Euroopan unionin toiminnasta tehdyn sopimuksen[15] 83 artiklan 1 kohta.

- **Toissijaisuusperiaate**

Euroopan unionin toimiin sovelletaan toissijaisuusperiaatetta. Ehdotuksen tavoitteita ei voida saavuttaa riittävällä tavalla pelkästään jäsenvaltioiden toimin seuraavista syistä:

Tietoverkkorikollisuudella ja erityisesti tietojärjestelmiin kohdistuvilla hyökkäyksillä on huomattava rajatylittävä ulottuvuus, joka on ilmeisintä laajamittaisissa hyökkäyksissä, sillä hyökkäyksen yhdistävät elementit sijaitsevat usein eri paikoissa ja eri maissa. Tämä edellyttää EU:n toimia, erityisesti jotta pysytään ajan tasalla suuntauksesta kohti laajamittaisia hyökkäyksiä sekä Euroopassa että muualla maailmassa. Myös neuvoston päätelmissä[16] marraskuulta 2008 kehotettiin toimimaan EU:n tasolla ja päivittämään puitepäätös 2005/222/YOS, sillä jäsenvaltiot eivät yksin pysty riittävästi suojelemaan tehokkaasti kansalaisia tietoverkkorikollisuudelta.

Ehdotuksen tavoitteet saavutetaan parhaiten Euroopan unionin toimilla seuraavista syistä:

---

15 EUVL C 83, 30.3.2010, s. 49.

16 ”Yhteinen työskentelystrategia ja konkreettiset toimenpiteet tietoverkkorikollisuuden torjumiseksi”, oikeus- ja sisäasioiden neuvoston 2987. kokous, Bryssel, 27.–28. marraskuuta 2008.

Ehdotuksella lähennetään edelleen jäsenvaltioiden aineellista rikosoikeutta ja menettelysääntöjä, millä on myönteinen vaikutus tällaisen rikollisuuden torjuntaan. Ensinnäkin se on tapa estää rikoksentekijöitä muuttamasta sellaisiin jäsenvaltioihin, joissa tietoverkkohyökkäyksiä koskeva lainsäädäntö on lievempi. Toiseksi yhteisten määritelmien ansiosta tietoja voidaan vaihtaa sekä kerätä ja verrata. Kolmanneksi torjuntatoimenpiteiden vaikuttavuus EU:ssa paranee ja kansainvälinen yhteistyö tiivistyy.

Näin ollen ehdotus noudattaa toissijaisuusperiaatetta.

- **Suhteellisuusperiaate**

Ehdotus on suhteellisuusperiaatteen mukainen seuraavasta syystä:

Direktiivissä ei ylitetä sitä, mikä on tarpeen näiden tavoitteiden saavuttamiseksi Euroopan tasolla ottaen huomioon tarpeen varmistaa rikoslainsäädännön täsmällisyys.

- **Sääntelytavan valinta**

Ehdotettu sääntelytapa: direktiivi.

Muut vaihtoehdot eivät soveltuisi seuraavasta syystä:

Oikeusperusta edellyttää direktiiviä.

Muilla kuin lainsäädännöllisillä toimenpiteillä ja itsesääntelyllä tilanne paranisi joillain aloilla, joilla täytäntöönpano on olennaista. Kuitenkin muilla aloilla, joilla uusi lainsäädäntö on olennaista, hyödyt olisivat vaatimattomia.

4. TALOUSARVIOVAIKUTUKSET

Ehdotuksen vaikutukset unionin talousarvioon ovat pieniä. Jäsenvaltiot maksaisivat yli 90 prosenttia arvioiduista kustannuksista (5 913 000 euroa), ja lisäksi voidaan hakea EU:n rahoitusta kustannusten vähentämiseksi.

5. LISÄTIEDOT

- **Lainsäädännön kumoaminen**

Ehdotuksesta seuraa, että aiempaa lainsäädäntöä kumotaan.

- **Maantieteellinen soveltamisala**

Tämä direktiivi on osoitettu jäsenvaltioille perussopimusten mukaisesti.

2010/0273 (COD)

Ehdotus

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI

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

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[17],

sen jälkeen, kun ehdotus on toimitettu kansallisille parlamenteille,

ottavat huomioon Euroopan talous- ja sosiaalikomitean lausunnon,

ottavat huomioon alueiden komitean lausunnon,

noudattavat tavallista lainsäätämisjärjestystä,

sekä katsovat seuraavaa:

(1) Tämän direktiivin tavoitteena on lähentää tietojärjestelmiin kohdistuvia hyökkäyksiä koskevia jäsenvaltioiden rikosoikeudellisia säännöksiä ja parantaa oikeus- ja muiden toimivaltaisten viranomaisten, jäsenvaltioiden poliisi- ja muut erikoistuneet lainvalvontaviranomaiset mukaan luettuina, välistä yhteistyötä.

(2) Tietojärjestelmiä vastaan tehdyt hyökkäykset, erityisesti järjestäytyneen rikollisuuden toimesta, ovat kasvava uhka, 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 toteuttamista sekä vapauteen, turvallisuuteen ja oikeuteen perustuvan alueen kehittämistä, niihin on varauduttava Euroopan unionin tasolla.

(3) On todisteita siitä, että pyritään tekemään entistä vaarallisempia ja toistuvia laajamittaisia hyökkäyksiä valtioiden tai julkisen tai yksityisen sektorin tiettyjen toimintojen kannalta elintärkeitä tietojärjestelmiä vastaan. Tähän suuntaukseen liittyvät entistä kehittyneemmät välineet, joita rikoksentekijät voivat käyttää käynnistääkseen erilaisia tietoverkkohyökkäyksiä.

[17] EUVL C […], […], s. […]

(4) Alan yhteiset, erityisesti tietojärjestelmiä ja dataa koskevat määritelmät, ovat tärkeitä sen varmistamiseksi, että jäsenvaltiot soveltavat tätä direktiiviä yhdenmukaisesti.

(5) Rikostunnusmerkistöihin on omaksuttava yhteinen linja antamalla yhteinen rikosmääritelmä laittomista tunkeutumisista tietojärjestelmään, laittomasta järjestelmän häirinnästä, laittomasta datan vahingoittamisesta ja viestintäsalaisuuden loukkaamisesta (tietojen laittomasta sieppauksesta).

(6) Jäsenvaltioiden olisi säädettävä tietojärjestelmiin kohdistuviin hyökkäyksiin syyllistyneille määrättävistä seuraamuksista. Säädettyjen seuraamusten olisi oltava tehokkaita, oikeasuhteisia ja varoittavia.

(7) On tarkoituksenmukaista säätää ankarammista seuraamuksista silloin, kun tietojärjestelmään kohdistuvan hyökkäyksen toteuttaa rikollisjärjestö, sellaisena kuin tämä on määritelty järjestäytyneen rikollisuuden torjunnasta 24 päivänä lokakuuta 2008 tehdyssä neuvoston puitepäätöksessä 2008/841/YOS[18], kun hyökkäys on laajamittainen tai kun teko on tehty salaamalla rikoksentekijän todellinen henkilöllisyys ja henkilöllisyyden oikealle omistajalle on aiheutettu vahinkoa. On myös aiheellista säätää ankarammista seuraamuksista, kun hyökkäys on aiheuttanut vakavia vahinkoja tai vaikuttanut haitallisesti olennaisiin etuihin.

(8) Neuvoston 27 ja 28 päivänä marraskuuta 2008 antamien päätelmien mukaan jäsenvaltioiden ja komission kanssa olisi luotava uusi strategia ottaen huomioon tietoverkkorikollisuutta koskevan Euroopan neuvoston vuonna 2001 tekemän yleissopimuksen sisältö. Kyseinen yleissopimus on oikeudellinen viitekehys torjuttaessa tietoverkkorikollisuutta, tietojärjestelmiin kohdistuvat hyökkäykset mukaan luettuina. Tämä direktiivi pohjautuu mainittuun yleissopimukseen.

(9) Kun otetaan huomioon hyökkäysten toteuttamistavat ja laitteistojen ja ohjelmistojen nopea kehitys, tässä direktiivissä tarkoitetaan ’välineillä’ sellaisia välineitä, joita voidaan käyttää tässä direktiivissä tarkoitettujen rikosten tekemiseen. Välineillä tarkoitetaan esimerkiksi haittaohjelmia, mukaan lukien bottiverkot, joita käytetään tietoverkkohyökkäysten tekemiseen.

(10) Tämän direktiivin tarkoituksena ei ole asettaa rikosvastuuta silloin, kun teko on tehty ilman rikollista tarkoitusta, vaan tarkoituksena on tietojärjestelmien luvallinen testaus tai suojelu.

(11) Tässä direktiivissä vahvistetaan verkostojen, kuten G8:n tai Euroopan neuvoston ympärivuorokautisen, seitsemän päivää viikossa käytettävissä olevan yhteyspisteverkoston, merkitystä tietojenvaihdossa, jotta voidaan varmistaa välitön avunanto tutkimuksissa tai menettelyissä, jotka koskevat tietojärjestelmiin ja dataan liittyviä rikoksia, tai sähköisessä muodossa olevien todisteiden keräämisessä rikostapauksissa. Kun otetaan huomioon, miten nopeasti laajamittaisia hyökkäyksiä voidaan toteuttaa, jäsenvaltioiden olisi voitava vastata ripeästi yhteyspisteverkoston esittämiin kiireellisiin pyyntöihin. Tähän avunantoon olisi kuuluttava avustaminen seuraavissa toimenpiteissä tai niiden toteuttaminen: tekninen neuvonta, tietojen säilyttäminen, todisteiden kerääminen, oikeudellisten tietojen antaminen ja epäiltyjen paikantaminen.

---

[18] EUVL L 300, 11.11.2008, s. 42.

(12) On tarpeen kerätä tässä direktiivissä tarkoitetuista rikoksista tietoja, jotta saadaan täydellisempi kuva ongelmasta unionin tasolla ja voidaan suunnitella tehokkaampia vastatoimia. Lisäksi tiedot auttavat erityisvirastoja, kuten Europolia ja Euroopan verkko- ja tietoturvavirastoa, arvioimaan paremmin tietoverkkorikollisuuden laajuutta ja verkko- ja tietoturvallisuuden tilaa Euroopassa.

(13) Jäsenvaltioiden tietojärjestelmiin kohdistuviin hyökkäyksiin liittyvien lainsäädäntöjen merkittävät puutteet ja lainsäädäntöjen väliset erot 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 rikoslainsäädäntöä tällä alalla. Lisäksi rikosoikeudenkäyntejä koskevien toimivaltaristiriitojen ehkäisemisestä ja ratkaisemisesta annetun neuvoston puitepäätöksen 2009/948/YOS pitäisi helpottaa tietojärjestelmiin kohdistuvia hyökkäyksiä koskevien syytetoimien koordinointia.

(14) Koska jäsenvaltiot eivät voi riittävällä tavalla toteuttaa direktiivin tavoitteita eli sitä, että tietojärjestelmiin kohdistuvista hyökkäyksistä määrätään kaikissa jäsenvaltioissa tehokkaat, oikeasuhteiset ja varoittavat rikosoikeudelliset seuraamukset ja että oikeudellista yhteistyötä tehostetaan ja siihen kannustetaan poistamalla mahdolliset hankaluudet, sillä sääntöjen on oltava yhteiset ja yhteensopivat, ja ne voidaan tämän vuoksi saavuttaa paremmin unionin tasolla, unioni voi toteuttaa toimenpiteitä Euroopan unionista tehdyn sopimuksen 5 artiklassa vahvistetun toissijaisuusperiaatteen mukaisesti. Tässä direktiivissä ei ylitetä sitä, mikä on tarpeen kyseisten tavoitteiden saavuttamiseksi.

(15) Tämän direktiivin täytäntöönpanon yhteydessä käsiteltäviä henkilötietoja olisi suojeltava niiden sääntöjen mukaisesti, jotka on vahvistettu rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta 27 päivänä marraskuuta 2008 tehdyssä neuvoston puitepäätöksessä 2008/977/YOS[19] niiden käsittelytoimintojen osalta, jotka kuuluvat sen soveltamisalaan, ja yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annetussa Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 45/2001[20].

(16) Tässä direktiivissä kunnioitetaan erityisesti Euroopan unionin perusoikeuskirjassa tunnustettuja perusoikeuksia ja periaatteita, mukaan lukien henkilötietojen suoja, sananvapaus ja tiedonvälityksen vapaus, oikeus oikeudenmukaiseen oikeudenkäyntiin, syyttömyysolettama ja puolustautumisoikeus sekä laillisuusperiaate ja rikoksista määrättävien rangaistusten oikeasuhteisuuden periaate. Erityisesti tässä direktiivissä pyritään varmistamaan näiden oikeuksien ja periaatteiden noudattaminen täysimääräisesti ja ne on pantava täytäntöön vastaavasti.

(17) [Euroopan unionin toiminnasta tehtyyn sopimukseen liitetyn, Yhdistyneen kuningaskunnan ja Irlannin asemasta vapauden, turvallisuuden ja oikeuden alueen osalta tehdyn pöytäkirjan 1, 2, 3 ja 4 artiklan mukaisesti Yhdistynyt kuningaskunta ja Irlanti ovat ilmoittaneet haluavansa osallistua tämän direktiivin antamiseen ja

---

19 EUVL L 350, 30.12.2008, s. 60.
20 EYVL L 8, 12.1.2001, s. 1.

soveltamiseen] TAI [Vaikuttamatta Yhdistyneen kuningaskunnan ja Irlannin asemasta vapauden, turvallisuuden ja oikeuden alueen osalta tehdyn pöytäkirjan 4 artiklan soveltamiseen, Yhdistynyt kuningaskunta ja Irlanti eivät osallistu tämän direktiivin antamiseen, se ei sido Yhdistynyttä kuningaskuntaa ja Irlantia eikä sitä sovelleta Yhdistyneeseen kuningaskuntaan ja Irlantiin].

(18) Euroopan unionin toiminnasta tehtyyn sopimukseen liitetyn, Tanskan asemasta tehdyn pöytäkirjan 1 ja 2 artiklan mukaisesti Tanska ei osallistu tämän direktiivin antamiseen, se ei sido Tanskaa eikä sitä sovelleta Tanskaan,

OVAT HYVÄKSYNEET TÄMÄN DIREKTIIVIN:

1 artikla

Kohde

Tässä direktiivissä määritellään tietojärjestelmiin kohdistuvien hyökkäysten alalla tehdyt rikokset ja vahvistetaan vähimmäissäännöt näistä rikoksista langetettavista seuraamuksista. Sen tavoitteena on myös vahvistaa yhteiset säännökset tällaisten hyökkäysten torjumiseksi ja parantaa tämän alan rikosoikeudellista yhteistyötä Euroopassa.

2 artikla

Määritelmät

Tässä direktiivissä käytetään seuraavia määritelmiä:

a) ’tietojärjestelmällä’ tarkoitetaan laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten, sekä dataa, jota niissä varastoidaan, käsitellään, haetaan tai välitetään niiden toimintaa, käyttöä, suojausta tai huoltoa varten;

b) ’datalla’ tarkoitetaan 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’ tarkoitetaan yksikköä, jolla on sovellettavan lain mukaan oikeushenkilön asema, lukuun ottamatta valtioita tai muita julkisia elimiä niiden käyttäessä julkista valtaa, tai julkisoikeudellisia kansainvälisiä järjestöjä;

d) ilmaisulla ’oikeudettomasti’ tarkoitetaan järjestelmään tunkeutumista tai sen häirintää, johon ei ole järjestelmän tai sen osan omistajan tai muun oikeudenhaltijan lupaa tai joka ei ole sallittua kansallisen lainsäädännön mukaan.

3 artikla

Laiton tunkeutuminen tietojärjestelmään

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että tahallinen ja oikeudeton tunkeutuminen tietojärjestelmään tai sen osaan on rikosoikeudellisesti rangaistava teko, ainakin jos kyse ei ole vähäisestä tapauksesta.

4 artikla

Laiton järjestelmän häirintä

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että tahallinen ja oikeudeton tietojärjestelmän toiminnan vakava estäminen tai keskeyttäminen dataa syöttämällä, siirtämällä, vahingoittamalla, tuhoamalla, turmelemalla, muuttamalla tai poistamalla tai 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 tahallinen ja oikeudeton tietojärjestelmässä olevan datan tuhoaminen, vahingoittaminen, turmeleminen, muuttaminen, poistaminen tai saattaminen käyttökelvottomaksi on rikosoikeudellisesti rangaistava teko, ainakin jos kyse ei ole vähäisestä tapauksesta.

6 artikla

Viestintäsalaisuuden loukkaus (tietojen laiton sieppaus)

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että tahallinen ja oikeudeton teknisin keinoin tapahtuva tiedon hankkiminen tietojärjestelmän sisäisestä tai tietojärjestelmien välisestä luottamuksellisesta datan siirrosta, sekä tällaista dataa sisältävästä tietojärjestelmästä lähtevästä sähkömagneettisesta säteilystä on rikosoikeudellisesti rangaistava teko.

7 artikla

Rikosten tekemisessä käytetyt välineet

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että seuraavien tahallinen ja oikeudeton tuottaminen, myynti, hankkiminen, tuonti, hallussapito, levittäminen tai muu saataville asettaminen on rangaistava teko, kun tarkoituksena on käyttää niitä 3–6 artiklassa rangaistaviksi säädettyjen rikosten tekemiseen.

a) väline, mukaan luettuna tietokoneohjelma, joka on suunniteltu tai muutettu ensisijaisesti 3–6 artiklan mukaisesti rangaistaviksi säädettyjen 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 tekoihin on rikosoikeudellisesti rangaistava teko.

2. Jäsenvaltioiden on varmistettava, että 3–6 artiklassa tarkoitettujen tekojen yritys on rikosoikeudellisesti rangaistava teko.

9 artikla

Seuraamukset

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

2. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 3–7 artiklassa tarkoitetuista teoista määrättävä rikosoikeudellinen enimmäisseuraamus on vähintään kaksi vuotta vankeutta.

10 artikla

Raskauttavat olosuhteet

1. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 3–7 artiklassa tarkoitetuista teoista määrättävä rikosoikeudellinen enimmäisseuraamus on vähintään viisi vuotta vankeutta, kun teot on tehty puitepäätöksessä 2008/841/YOS annetun määritelmän mukaisen rikollisjärjestön puitteissa.

2. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 3–6 artiklassa tarkoitetuista teoista määrättävä rikosoikeudellinen enimmäisseuraamus on vähintään viisi vuotta vankeutta, kun teot on tehty käyttämällä välinettä, jonka tarkoituksena on käynnistää hyökkäyksiä, jotka vaikuttavat merkittävään määrään tietojärjestelmiä tai aiheuttavat huomattavaa vahinkoa esimerkiksi järjestelmäpalvelujen keskeytyksinä, taloudellisina kustannuksina tai henkilötietojen menetyksinä.

3. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 3–6 artiklassa tarkoitetuista teoista määrättävä rikosoikeudellinen enimmäisseuraamus on vähintään viisi vuotta vankeutta, kun teot on tehty salaamalla rikoksentekijän todellinen henkilöllisyys ja henkilöllisyyden oikealle omistajalle on aiheutettu vahinkoa.

11 artikla

Oikeushenkilöiden vastuu

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

   a) valtaan edustaa oikeushenkilöä;

   b) valtuuteen tehdä päätöksiä oikeushenkilön puolesta;

   c) valtuuteen 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 valvonnan alaisena toimiva henkilö on tehnyt kyseisen oikeushenkilön hyväksi 3–8 artiklassa tarkoitettuja tekoja.

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

12 artikla

Oikeushenkilöihin kohdistettavat seuraamukset

1. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 11 artiklan 1 kohdan mukaisesti vastuulliseksi todettua oikeushenkilöä voidaan rangaista tehokkain, oikeasuhteisin ja varoittavin seuraamuksin, joihin kuuluvat rikosoikeudelliset tai muut sakot ja joihin voi kuulua myös muita seuraamuksia, kuten:

   a) oikeuden menettäminen julkisista varoista myönnettyjen etuuksien tai tuen saamiseen;

   b) tilapäinen tai pysyvä kielto harjoittaa liiketoimintaa;

   c) oikeudelliseen valvontaan asettaminen;

   d) oikeudellinen määräys lopettaa toiminta;

   e) rikoksen tekemiseen käytettyjen laitosten sulkeminen väliaikaisesti tai pysyvästi.

2. Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet, jotta 11 artiklan 2 kohdan mukaisesti vastuulliseksi todettua oikeushenkilöä voidaan rangaista tehokkain, oikeasuhteisin ja varoittavin seuraamuksin tai toimenpitein.

13 artikla

Lainkäyttövalta

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

   a) teko on tehty kokonaan tai osittain kyseisen jäsenvaltion alueella; tai

   b) teon on tehnyt niiden kansalainen tai henkilö, jonka kotipaikka on kyseisen jäsenvaltion alueella; tai

   c) teko on tehty sellaisen oikeushenkilön hyväksi, jonka kotipaikka on kyseisen jäsenvaltion alueella.

2. Ulottaessaan lainkäyttövaltansa 1 kohdan a alakohdan mukaisesti jäsenvaltioiden on varmistettava, että niiden lainkäyttövaltaan kuuluvat tapaukset, joissa:

   a) rikoksentekijä tekee teon ollessaan fyysisesti kyseisen jäsenvaltion alueella, riippumatta siitä, kohdistuuko teko sen alueella sijaitsevaan tietojärjestelmään; tai

   b) teko kohdistuu kyseisen jäsenvaltion alueella sijaitsevaan tietojärjestelmään, riippumatta siitä, tekeekö rikoksentekijä teon ollessaan fyysisesti sen alueella.

14 artikla

Tietojenvaihto

1. Jäsenvaltioiden on hyödynnettävä nykyistä kaikkina viikonpäivinä ja ympärivuorokautisesti toimivien yhteyspisteiden verkostoa 3–8 artiklassa tarkoitettuja tekoja koskevaa tietojenvaihtoa varten ja tietosuojasäännösten mukaisesti. Jäsenvaltioiden on myös varmistettava, että niillä on käytössä menettely, jonka avulla ne voivat vastata kiireellisiin pyyntöihin enintään kahdeksan tunnin kuluessa. Vastauksesta on ilmettävä, vastataanko avunpyyntöön ja missä muodossa ja milloin se tehdään.

2. Jäsenvaltioiden on ilmoitettava komissiolle 3–8 artiklassa tarkoitettuja tekoja koskevaa tietojenvaihtoa varten nimeämänsä yhteyspisteen yhteystiedot. Komissio toimittaa tiedot muille jäsenvaltioille.

15 artikla

Seuranta ja tilastot

1. Jäsenvaltioiden on varmistettava, että niillä on järjestelmä, jonka avulla voidaan kirjata, tuottaa ja antaa tilastotietoja 3–8 artiklassa tarkoitetuista teoista.

2. Edellä 1 kohdassa tarkoitettujen tilastotietojen on katettava vähintään 3–8 artiklassa tarkoitettujen, jäsenvaltioille ilmoitettujen tekojen lukumäärä ja ilmoitusten johdosta

toteutetut jatkotoimenpiteet ja niihin on sisällyttävä vuosittain tutkittujen ilmoitettujen tapausten lukumäärä, syytteeseen asetettujen henkilöiden lukumäärä sekä 3–8 artiklassa tarkoitetuista teoista tuomittujen henkilöiden lukumäärä.

3. Jäsenvaltioiden on toimitettava tämän artiklan mukaisesti kerätyt tiedot komissiolle. Niiden on myös varmistettava, että tilastollisista kertomuksista julkaistaan konsolidoitu selvitys.

16 artikla

Puitepäätöksen 2005/222/YOS kumoaminen

Kumotaan puitepäätös 2005/222/YOS, sanotun kuitenkaan rajoittamatta jäsenvaltioiden velvollisuutta noudattaa määräaikoja, joihin mennessä säädös on saatettava osaksi kansallista lainsäädäntöä.
Viittauksia kumottuun puitepäätökseen pidetään viittauksina tähän direktiiviin.

17 artikla

Saattaminen osaksi kansallista lainsäädäntöä

1. Jäsenvaltioiden on saatettava tämän direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset voimaan viimeistään [kahden vuoden kuluttua sen hyväksymisestä]. Niiden on viipymättä toimitettava komissiolle kirjallisina nämä säännökset sekä kyseisiä säännöksiä ja tätä direktiiviä koskeva vastaavuustaulukko.

   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.

2. Jäsenvaltioiden on toimitettava tässä direktiivissä tarkoitetuista kysymyksistä antamansa keskeiset kansalliset säännökset kirjallisina komissiolle.

18 artikla

Raportointi

1. Komissio antaa Euroopan parlamentille ja neuvostolle kertomuksen tämän direktiivin soveltamisesta jäsenvaltioissa ja mahdollisesti tarvittavat ehdotukset viimeistään [NELJÄN VUODEN KULUTTUA DIREKTIIVIN HYVÄKSYMISESTÄ] ja sen jälkeen kolmen vuoden välein.

2. Jäsenvaltioiden on toimitettava komissiolle kaikki 1 kohdassa tarkoitetun kertomuksen laatimiseen tarvittavat tiedot. Niiden mukana on toimitettava yksityiskohtainen kuvaus tämän direktiivin täytäntöönpanemiseksi toteutetuista lainsäädännöllisistä ja muista toimenpiteistä.

19 artikla

Voimaantulo

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

20 artikla

Osoitus

Tämä direktiivi on osoitettu jäsenvaltioille perussopimusten mukaisesti.

Tehty Brysselissä

Euroopan parlamentin puolesta	*Neuvoston puolesta*
Puhemies	*Puheenjohtaja*