U 50/2010 vp

Valtioneuvoston kirjelmä Eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta

Perustuslain 96 §:n 2 momentin mukaisesti lähetetään ehdotus Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta sekä ehdotuksesta laadittu muistio.

Helsingissä 2 päivänä joulukuuta 2010

Oikeusministeri *Tuija Brax*

Lainsäädäntöjohtaja Asko Välimaa

OIKEUSMINISTERIÖ MUISTIO EU/2010/1522

EHDOTUS EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI TIETOJÄRJESTELMIIN KOHDISTUVISTA HYÖKKÄYKSISTÄ JA NEUVOSTON PUITEPÄÄTÖKSEN 2005/222/YOS KUMOAMISESTA

1 Yleistä

Euroopan komissio on 30 päivänä syyskuuta 2010 tehnyt ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta (KOM(2010) 517 lopullinen). Direktiiviehdotuksen tavoitteena on lähentää tietojärjestelmiin kohdistuvia hyökkäyksiä koskevia jäsenvaltioiden rikosoikeudellisia säännöksiä ja parantaa oikeus- ja muiden toimivaltaisten viranomaisten, jäsenvaltioiden poliisi- ja muut lainvalvontaviranomaiset mukaan luettuina, välistä yhteistyötä.

Ehdotuksessa on kysymys nykyisen tietojärjestelmiin kohdistuvista hyökkäyksistä tehdyn neuvoston puitepäätöksen 2005/222/YOS, jäljempänä puitepäätös, kumoamisesta ja uuden direktiivin säätämisestä sen tilalle. Ehdotettu direktiivi sisältää nykyisen puitepäätöksen vastaavat säännökset pääosin sellaisenaan. Direktiiviin lisättäisiin myös eräitä kriminalisointivelvoitteita, joita vastaavat ovat Euroopan neuvoston tietoverkkorikollisuutta koskevassa yleissopimuksessa (SopS 60/2007), jäljempänä yleissopimus. Lisäksi ehdotuksessa on uusia säännöksiä, joiden tarkoituksena muun muassa puuttua uusiin uhkakuviin kuten laajamittaisiin tietoverkkohyökkäyksiin niin sanottuja bot-verkkoja käyttämällä ja tietoverkkorikoksen yhteydessä tapahtuvaan henkilöllisyyden väärinkäyttöön.

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 komission toimintasuunnitelmassa (KOM (2010) 171 lopullinen). Tarve puuttua tietoverkkorikoksiin Euroopan tasolla todetaan myös Euroopan digitaalistrategiassa, joka on osa Eurooppa 2020 –strategiaa.

Puitepäätöksen täytäntöönpanon ja yleissopimuksen voimaantulon Suomessa edellyttämät lainmuutokset ovat tulleet voimaan 11 päivänä toukokuuta 2007 (HE 153/2006 vp.). Yleissopimus on tullut kansainvälisesti voimaan 1 päivänä heinäkuuta 2004 ja sen on saattanut kansallisesti voimaan 30 valtiota, joista 17 on EU:n jäsenvaltioita.

2 Pääasiallinen sisältö

Ehdotetun direktiivin kumottavaa puitepäätöstä vastaavat säännökset koskevat tietojärjestelmän, datan, oikeushenkilön ja oikeudettomuuden määritelmiä (direktiiviehdotuksen 2 artikla), laitonta tunkeutumista tietojärjestelmään (3 artikla), laitonta järjestelmän häirintää (4 artikla), laitonta datan vahingoittamista (5 artikla), rikokseen yllyttämistä, avunantoa ja rikoksen yritystä (8 artikla), oikeushenkilön vastuuta (11 ja 12 artikla) ja rikosoikeudellista lainkäyttövaltaa (13 artikla). Ehdotuksen säännökset, joita vastaavat sisältyvät yleissopimukseen, mutta puuttuvat puitepäätöksestä, koskevat viestintäsalaisuuden loukkaamista (direktiiviehdotuksen 6 artikla) ja rikoksen tekemisessä käytettyjä välineitä (7 artikla). Direktiiviehdotuksessa ei kuitenkaan ole kaikkia puitepäätöksen ja yleissopimuksen sisältämiä mahdollisuuksia rajoittaa kansallisesti joidenkin edellä mainittujen säännösten soveltamisalaa tai tehdä niihin varaumia.

Ehdotuksessa on myös säännöksiä jäsenvaltioiden viranomaisten välisestä tietojenvaihdosta (14 artikla), jotka ovat puitepää-

töksen ja yleissopimuksen vastaavia määräyksiä velvoittavampia.

Ehdotuksessa on myös säännöksiä, joita vastaavia ei lainkaan sisälly puitepäätökseen tai yleissopimukseen. Raskauttavia olosuhteita koskeviin säännöksiin on lisätty hyökkäysten laajamittaisuus niin sanottuja botverkkoja käyttämällä (10 artiklan 2 kohta) ja tekijän henkilöllisyyden salaaminen siten, että aiheutetaan vahinkoa henkilöllisyyden oikealle haltijalle (10 artiklan 3 kohta). Botverkolla tarkoitetaan haittaohjelmien (tietokonevirusten) saastuttamien tietokoneiden muodostamaa verkkoa, jota hallinnoidaan yhdestä isäntätietokoneesta käsin muiden yleensä sitä tietämättä. Bot-verkko voidaan saada toimimaan halutulla tavalla esimerkiksi hyökkäämään tietojärjestelmiä vastaan (tietoverkkohyökkäykset).

Lisäksi direktiivissä on uusi säännös tilastotietojen keräämisestä (15 artikla).

Säännökset luonnollisille henkilöille rikoksista säädettävistä rangaistuksista ovat puitepäätöstä ja yleissopimusta ankarampia.

3 Vaikutus Suomen lainsäädäntöön

Rikoslain (39/1889) 38 luvussa säädetään tieto- ja viestintärikoksista. Luvussa on säännökset viestintäsalaisuuden loukkauksesta (3 §), törkeästä viestintäsalaisuuden loukkauksesta (4 §), tietojärjestelmän häirinnästä (7 a §), törkeästä tietojärjestelmän häirinnästä (7 b §), tietomurrosta (8 §) ja törkeästä tietomurrosta (8 a §). Rikoslain 34 luvussa säädetään vaaran aiheuttamisesta tietojenkäsittelylle (9 a §) ja tietoverkkorikosvälineen hallussapidosta (9 b §). Rikoslain 35 luvun 1 §:n 2 momentissa säädetään vahingonteosta, joka koskee tietovälineellä olevan tiedon hävittämistä. Tietojärjestelmään kohdistuvia tai tietokoneen avulla tehtyjä tekoja koskevia rangaistussäännöksiä on myös muualla rikoslaissa. Esimerkiksi 28 luvun 7—9 §:ssa säädetään luvattomasta käytöstä, joka koskee myös tietojärjestelmän käyttöä, ja 36 luvun 1 §:n petosta koskevan säännöksen 2 momentissa säädetään taloudellisen vahingon aiheuttamisesta toiselle tietojärjestelmän toimintaan puuttumalla.

Mainitut säännökset täyttävät ne edellä mainitut ehdotetun direktiivin kriminalisointivelvoitteet, joita vastaavat velvoitteet sisältyvät puitepäätökseen ja yleissopimukseen, siltä osin kuin velvoitteiden täytäntöönpanoa ei ole puitepäätöksen tai yleissopimuksen sallimalla tavalla rajoitettu. Myös ehdotuksen edellyttämä yllytyksen, avunannon ja yrityksen rangaistavuus sekä oikeushenkilön rangaistusvastuu täyttyy nykyisen lainsäädännön nojalla (HE 153/2006).

Direktiiviehdotuksen 3 artiklan laitonta tunkeutumista tietojärjestelmään koskeva säännös ei sisältäisi puitepäätöksen ja yleissopimuksen vastaavassa säännöksessä olevaa mahdollisuutta päättää kansallisesti, että menettelystä syytetään vain, jos teko on tehty murtamalla turvajärjestelyt. Rikoslain 38 luvun 8 §:ssä säädetyn tietomurron soveltaminen edellyttää, että tietojärjestelmään tunkeutuminen tehdään tekijälle kuulumatonta käyttäjätunnusta käyttämällä taikka turvajärjestelyn muuten murtamalla. Jos tietojärjestelmään tunkeudutaan ja tietoja käytetään luvatta turvajärjestelyä murtamatta, teko täyttää yleensä rikoslain 28 luvun 7 §:ssä säädetyn luvattoman käytön tunnusmerkistön. Lainsäädäntö ei kuitenkaan ole täysin yhtenevä direktiiviehdotuksen 3 artiklan kanssa.

Direktiiviehdotuksen 8 artiklan 2 kohdan yrityksen rangaistavuutta koskeva säännös vastaa muuten puitepäätöksen sääntelyä, mutta koskee myös 3 artiklassa tarkoitettua laitonta tunkeutumista tietojärjestelmään sekä 6 artiklassa tarkoitettua viestintäsalaisuuden loukkausta. Koska rikoslaissa vastaavien rikosten yritys on jo rangaistavaa, ei säännös edellyttäisi lainsäädännön muuttamista.

Direktiiviehdotuksen 9 artiklan mukaan jäsenvaltioiden olisi toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 3—7 artiklassa tarkoitetuista teoista määrättävä rikosoikeudellinen enimmäisseuraamus on vähintään kaksi vuotta vankeutta. Ehdotettu enimmäisseuraamus on ankarampi kuin puitepäätöksessä, jonka mukaan enimmäisrangaistukseksi siihen sisältyvistä vastaavista teoista riittää yksi vuosi vankeutta (puitepäätöksen 6 artiklan 2 kohta). Yleissopimuksessa edellytetään vain, että rikoksista säädetään tehokkaita, oikeasuhteisia ja riittäviä vapausrangaistuksia (yleissopimuksen 13 artiklan

1 kappale). Direktiiviehdotuksessa edellytettyä vaatimusta enimmäisseuraamuksesta eivät täytä viestintäsalaisuuden loukkaus, tietomurto ja vahingonteko, joista on säädetty enimmäisrangaistukseksi yksi vuosi vankeutta, eikä tietoverkkorikosvälineen hallussapito, josta on säädetty enimmäisrangaistukseksi kuusi kuukautta vankeutta.

Direktiiviehdotuksen 10 artiklassa määritellään raskauttavat olosuhteet, joiden täyttyessä direktiivin alaan kuuluvista rikoksista säädettävän enimmäisseuraamuksen olisi oltava vähintään viisi vuotta vankeutta. Artiklan 1 kohdan mukaan tällainen raskauttava olosuhde olisi ehdotuksen 3—7 artiklassa tarkoitetun rikoksen tekeminen järjestäytyneen rikollisuuden torjunnasta tehdyssä puitepäätöksessä 2008/841/YOS annetun määritelmän mukaisen rikollisjärjestön puitteissa. Mainittu rikollisjärjestön määritelmä vastaa rikoslain 17 luvun 1 a §:n 4 momenttiin sisältyvää järjestäytyneen rikollisryhmän määritelmää.

Artiklan 2 kohdan mukaan raskauttava olosuhde olisi ehdotuksen 3—6 artiklassa tarkoitetun rikoksen tekeminen käyttämällä välinettä, jonka tarkoituksena on käynnistää hyökkäyksiä, jotka vaikuttavat merkittävään määrään tietojärjestelmiä tai aiheuttavat huomattavaa vahinkoa esimerkiksi järjestelmäpalvelujen keskeytyksinä, taloudellisina kustannuksina tai henkilötietojen menetyksinä. Teonkuvauksella tarkoitetaan ehdotuksen perustelujen mukaan erityisesti bot-verkon käyttöä.

Artiklan 1 ja 2 kohdan ehdotettuja velvoitteita lähinnä vastaavat säännökset ovat törkeä viestintäsalaisuuden loukkaus, törkeä tietojärjestelmän häirintä, törkeä tietomurto ja törkeä vahingonteko. Edellä mainituissa tunnusmerkistöissä ei törkeää tietomurtoa ja törkeää vahingontekoa lukuun ottamatta ole mainittu teon toteuttamista osana järjestäytynyttä rikollisryhmää. Lisäksi vain osassa säännöksistä on sellaisia soveltamisperusteita, että niitä mahdollisesti voitaisiin soveltaa 2 kohdassa tarkoitettuun laajamittaiseen tekoon.

Mainitut säännökset eivät myöskään kata kaikkia ehdotuksen 3—7 artiklassa tarkoitettuja rikoksia, joita 1 ja 2 kohdan raskauttavat olosuhteet koskevat. Esimerkiksi vaaran aiheuttamisesta tietojenkäsittelylle tai tietoverkkorikosvälineen hallussapidosta ei ole säädetty törkeää tekomuotoa. Lisäksi teoista on säädetty enimmäisrangaistukseksi kolme tai neljä vuotta vankeutta, mikä ei vastaa ehdotettua vähintään viiden vuoden enimmäisvankeusrangaistusta.

Artiklan 3 kohdan mukaan raskauttava olosuhde olisi ehdotuksen 3—6 artiklassa tarkoitetun rikoksen tekeminen salaamalla rikoksentekijän todellinen henkilöllisyys aiheuttaen henkilöllisyyden oikealle omistajalle vahinkoa. Ehdotuksen sisältö ei ole kovin selkeä. Siinä ei esimerkiksi määritellä, mitä tarkoitetaan henkilöllisyydellä tai sen salaamisella. Myöskään vahingon laatua ei määritellä. Epäselvyydestä huolimatta ehdotuksen perusteluissa todetaan, että näiden sääntöjen olisi noudatettava laillisuusperiaatetta ja henkilötietojen suojaa koskevaa lainsäädäntöä (s. 7).

Suomen lainsäädännössä ei ole 3 kohdan raskauttavaa olosuhdetta vastaavaa säännöstä.

Direktiiviehdotuksen 13 artiklan lainkäyttövaltaa koskeva säännös vastaa puitepäätöksen vastaavaa sääntelyä. Puitepäätöksessä jätetään kuitenkin jäsenvaltioille mahdollisuus jättää ulottamatta lainkäyttövaltaansa muun muassa tapauksiin, joissa teko on tehty sellaisen oikeushenkilön hyväksi, jonka kotipaikka on kyseisen jäsenvaltion alueella. Koska Suomen lainsäädännön mukaan lainkäyttövaltaa ei ole tällaisissa tilanteissa, on käytetty mahdollisuutta olla soveltamatta puitepäätöksen kyseistä säännöstä (HE 153/2006, s. 54). Direktiiviehdotukseen ei sisälly vastaavaa poikkeamismahdollisuutta. Direktiiviehdotuksen 13 artikla edellyttäisi sen vuoksi lainsäädännön muuttamista.

Direktiiviehdotuksen 14 artiklan tietojenvaihtoa koskevaan säännökseen on puitepäätöksen ja yleissopimuksen vastaaviin säännöksiin nähden lisätty velvoite, jonka mukaan jäsenvaltioiden olisi varmistettava, että niillä on käytössä menettely, jonka avulla niiden kaikkina viikonpäivinä ympärivuorokautisesti toimivat yhteyspisteet voivat vastata kiireellisiin pyyntöihin enintään kahdeksan tunnin kuluessa. Vastauksesta olisi ilmettävä, vastataanko avunpyyntöön ja missä muodossa ja milloin se tehdään. Suomessa tällaisena

yhteyspisteenä toimii keskusrikospoliisi. Artikla ei edellyttäisi lainsäädännön muuttamista.

Direktiiviehdotuksen 15 artiklassa on säännös seurannasta ja tilastoista. Vastaavaa säännöstä ei sisälly puitepäätökseen tai yleissopimukseen. Jäsenvaltioilla on säännöksen mukaan oltava järjestelmä, jonka avulla voidaan kirjata, tuottaa ja antaa tilastotietoja direktiiviehdotuksen 3—8 artiklassa tarkoitetuista rikoksista. Tilastot on julkaistava ja niiden tiedot on toimitettava komissiolle. Suomessa artiklan tarkoittamista tilastoista vastaa tilastokeskus. Säännös ei edellyttäisi lainsäädännön muuttamista.

4 Ahvenanmaan toimivalta

Ahvenanmaan itsehallintolain (1144/1991) 27 §:n 22 kohdan mukaan valtakunnan lainsäädäntövaltaan kuuluvat rikosoikeutta koskevat asiat 18 §:n 25 kohdassa säädetyin poikkeuksin. Viimeksi mainitun kohdan mukaan maakunnalla on lainsäädäntövalta asioissa, jotka koskevat teon rangaistavaksi säätämistä ja rangaistuksen määrää, kun kysymys on maakunnan lainsäädäntövaltaan kuuluvasta oikeudenalasta. Tietokonerikoksia koskeva lainsäädäntö ei 18 §:n muiden kohtien perusteella kuulu maakunnan lainsäädäntövaltaan.

5 Ehdotuksen vaikutukset

Direktiivillä lähennettäisiin jäsenvaltioiden lainsäädäntöä edellyttämällä rangaistavaksi tietojärjestelmiin kohdistuvat vahingolliset teot ja määrittelemällä niistä säädettävät vähimmäisrangaistukset. Tällainen yhtenäistäminen voi olla omiaan edistämään myös jäsenvaltioiden yhteistyötä direktiivin alaan kuuluvien rikosten torjunnassa.

Direktiivillä myös tehostettaisiin rikosten tutkintaa tehostamalla ja nopeuttamalla kaikkina viikonpäivinä ympärivuorokautisesti toimivien yhteyspisteiden toimintaa. Uudet velvoitteet tilastoinnista myös edistäisivät tietoverkkorikollisuuden seurantaa koko EU:ssa.

Ehdotukseen liittyvässä komission vaikutusarvioinnissa on arveltu, että ympärivuorokautisesti toimivien yhteyspisteiden toiminnan tehostaminen aiheuttaisi jäsenvaltioille lisäkustannuksia. Koska keskusrikospoliisissa olevan yhteyspisteen toiminta täyttää jo ehdotetut lisävelvoitteet, ei direktiivi aiheuttaisi Suomelle tältä osin lisäkustannuksia.

6 Oikeusperusta

Sopimus Euroopan unionin toiminnasta 83 artiklan 1 kohta.

7 Toissijaisuusperiaate

Tietoverkkorikollisuudella on rajat ylittävä ulottuvuus. Ehdotuksella lähennettäisiin edelleen kansainvälisen yhteistyön menettelysääntöjä, millä on myönteinen vaikutus tällaisen rikollisuuden torjuntaan. Valtioneuvosto pitää ehdotusta toissijaisuusperiaatteen mukaisena.

8 Toisten jäsenvaltioiden kannat

Ehdotuksen käsittelyä ei ole vielä aloitettu työryhmässä.

9 Instituutioiden ja muut kannat

Euroopan parlamentti ei ole vielä käsitellyt direktiiviehdotusta.

10 Ehdotuksen kansallinen käsittely ja käsittely Euroopan unionissa

Direktiiviehdotus on ollut oikeus- ja sisäasiat -jaoston (jaosto 7) kirjallisessa menettelyssä.

Komissio on esitellyt direktiiviehdotuksen oikeus- ja sisäasiain neuvostossa 8 päivänä marraskuuta 2010 sekä neuvoston työryhmässä 13 päivänä lokakuuta 2010. Varsinainen käsittely työryhmässä aloitetaan esitetyn arvion mukaan Unkarin puheenjohtajuuskaudella.

Euroopan parlamentissa vastuuvaliokunta on kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta (LIBE). Raportoijaa ei ole vielä nimetty.

11 Valtioneuvoston kanta

Valtioneuvosto suhtautuu myönteisesti Euroopan unionin yhteiseen toimintaan vakavien tietojärjestelmiin kohdistuvien rikosten torjunnassa. Rikokset tapahtuvat nopeasti muuttuvassa toimintaympäristössä ja ne ovat varsin usein valtioiden rajat ylittäviä. Sen vuoksi on tärkeää, että rikoslainsäädäntö on ajantasaista ja kattavaa kaikissa EU:n jäsenvaltioissa. Ehdotettujen kriminalisointivelvoitteiden ala vastaa pääosin nykyisen puitepäätöksen, Euroopan neuvoston yleissopimuksen ja Suomen nykyisen lain sääntelyä. Ehdotusta voidaan valtioneuvoston näkemyksen mukaan pitää yleisellä tasolla tarpeellisena ja kannatettavana huolimatta vastaavasta Euroopan neuvoston yleissopimuksesta, koska toistaiseksi 10 EU:n jäsenvaltiota ei ole saattanut sopimusta kansallisesti voimaan.

Ehdotuksen uudet säännökset botverkkojen käytöstä ja henkilöllisyyden väärinkäytöstä heijastavat viimeaikaista kehitystä. Nämä säännökset eivät kuitenkaan laajentaisi rangaistavuuden alaa vaan ne koskisivat tällaisista teoista säädettäviä enimmäisrangaistuksia. Säännökset olisi Suomessa johdonmukaista panna täytäntöön siten, että ne olisivat rikosten törkeiden tekomuotojen soveltamisperusteita. Sen vuoksi säännökset olisi ehdotuksen jatkovalmistelussa pyrittävä muotoilemaan niin, että ne voidaan panna kansallisesti täytäntöön rikosoikeudellisen laillisuusperiaatteen edellyttämällä tavalla.

Ehdotetut enimmäisrangaistukset ovat nykyistä ankarampia ja rikoslain yleiseen ankaruustasoon verrattuna varsin korkeat. Enimmäisrangaistusvelvoitteita ei myöskään ole eritelty niin, että otettaisiin huomioon direktiivin rikosten erilaiset vakavuusasteet. Ongelmallista on esimerkiksi se, että vähintään kahden vuoden enimmäisvankeusrangaistus olisi säädettävä sekä oikeudettomasta tunkeutumisesta tietojärjestelmään että pelkästään sellaiseen tekoon käytettävän välineen hallussapidosta, kun hallussapidon tarkoituksena on käyttää välinettä direktiivissä tarkoitettuihin rikoksiin.

Teon rangaistusarvon ja rangaistusasteikkojen olisi oltava suhteellisuusperiaatteen mukaisesti oikeassa suhteessa tavoitteeseen ja rikoksen vakavuuteen. Kiinnijäämisriskin lisääminen, esimerkiksi kansainvälistä viranomaisyhteistyötä tehostamalla, toimii rikosten ennaltaehkäisyssä paremmin kuin rangaistusasteikkojen koventaminen. On tärkeää, että EU:n rikosoikeudessa otetaan riittävästi huomioon yksittäisen jäsenvaltion rangaistusasteikkokäytäntö eikä vaaranneta jäsenvaltion rikosoikeuden johdonmukaisuutta.