HE 232/2014 vp

Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettaviksi rikoslakia, pakkokeinolakia, poliisilakia ja sotilasoikeudenkäyntilakia. Ehdotetuilla laeilla pantaisiin täytäntöön tietojärjestelmiin kohdistuvia hyökkäyksiä koskeva Euroopan parlamentin ja neuvoston direktiivi.

Esityksen mukaan tietoverkkorikosvälineen käyttöön hankkiminen olisi rangaistavaa vaaran aiheuttamisena tietojenkäsittelylle. Lakiin lisättäisiin uusi datavahingontekoa koskeva kriminalisointi sekä datavahingonteon törkeä ja lievä tekomuoto. Datavahingonteon enimmäisrangaistus olisi kaksi vuotta vankeutta. Törkeän datavahingonteon enimmäisrangaistus olisi viisi vuotta vankeutta. Kvalifiointiperusteet liittyvät niin sanottujen bottiverkkojen käyttöön, rikollisjärjestöön, huomattavaan vahinkoon sekä elintärkeään infrastruktuuriin. Syyteoikeutta, toimenpiteistä luopumista ja oikeushenkilön rangaistusvastuuta muutettaisiin vastaamaan edellä mainittua muutosta.

Viestintäsalaisuuden loukkaus kattaisi esityksen mukaan myös tietojärjestelmän sisäisen luottamuksellisen datan siirron. Viestintäsalaisuuden loukkauksen enimmäisrangaistus korotettaisiin kahteen vuoteen vankeutta. Tietojärjestelmän häirinnästä ehdotetaan poistettavaksi toissijaisuuslauseke. Törkeää tietoliikenteen häirintää ja törkeää tietojärjestelmän häirintää koskevaan sääntelyyn lisättäisiin törkeää datavahingontekoa vastaavat kvalifiointiperusteet. Mainittujen törkeiden tekomuotojen enimmäisrangaistus olisi viisi vuotta vankeutta. Tietomurto kattaisi esityksen mukaan myös pääsyn tietojärjestelmässä olevaan dataan ja tiedon hankkimisen siitä. Tietomurron enimmäisrangaistus korotettaisiin kahteen vuoteen vankeutta. Tämän johdosta myös törkeän tietomurron enimmäisrangaistus korotettaisiin kahdesta vuodesta kolmeen vuotta vankeutta. Lakiin lisättäisiin myös uusi säännös, joka sisältäisi direktiivin velvoitteiden mukaiset tietojärjestelmän ja datan määritelmät.

Pakkokeinolakia ja poliisilakia muutettaisiin vastaamaan edellä mainittuja rikoslain muutoksia.

Lisäksi rikoslakiin lisättäisiin uusi identiteettivarkautta koskeva säännös. Identiteettivarkaus olisi asianomistajarikos. Identiteettivarkaus lisättäisiin myös sotilasoikeudenkäyntilaissa tarkoitettujen sotilasoikeudenkäyntiasiana käsiteltävien rikosten listaan.

Lait on tarkoitettu tulemaan voimaan 4 päivänä syyskuuta 2015, jolloin direktiivi on pantava jäsenvaltioissa täytäntöön.

SISÄLLYS

YLEISPERUSTELUT

1 Johdanto

Esityksen tarkoituksena on saattaa Suomen lainsäädäntö vastaamaan vaatimuksia, jotka johtuvat tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta annetusta Euroopan parlamentin ja neuvoston direktiivistä 2013/40/EU, jäljempänä direktiivi tai tietoverkkorikosdirektiivi. Suomen tietoverkkorikoksia koskevaa lainsäädäntöä on viimeksi merkittävästi uudistettu saatettaessa kansallisesti voimaan Budapestissa 23 päivänä marraskuuta 2001 tehty Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (CETS 185), jäljempänä yleissopimus tai tietoverkkorikossopimus (SopS 60/2007, HE 153/2006 vp). Samassa yhteydessä saatettiin lainsäädäntö vastaamaan nyt käsiteltävällä direktiivillä korvattavan Euroopan unionin neuvoston 24 päivänä helmikuuta 2005 hyväksymän puitepäätöksen (2005/222/YOS, EUVL L 69/67, 16.3.2005) tietojärjestelmiin kohdistuvista hyökkäyksistä, jäljempänä puitepäätös, vaatimuksia. Puitepäätöksessä on säännöksiä samoista asioista kuin yleissopimuksessa.

Direktiivi sisältää pitkälti samoja säännöksiä kuin yleissopimus ja puitepäätös. Yleissopimus sisältää kuitenkin vielä kattavammat ja laajemmat määräykset tietoverkkorikoksista kuin puitepäätös ja direktiivi. Se sisältää määräyksiä muun muassa oikeudellisesta yhteistyöstä. Eräs direktiivin tavoitteista onkin saattaa kaikkien jäsenvaltioiden lainsäädäntö vastaamaan tiettyjä yleissopimuksen vaatimuksia. Direktiivissä on kuitenkin joitakin lisäyksiä aiempiin instrumentteihin nähden, sillä se sisältää muun muassa säännöksiä liittyen niin sanottuihin bottiverkkoihin ja identiteettitiedon väärinkäyttöön. Lisäksi direktiivillä harmonisoidaan siinä tarkoitetuista rikoksista seuraavien enimmäisvankeusrangaistusten vähimmäistasoja laajemmin kuin puitepäätöksessä. Tietoverkkorikoksia ja monia asiallisesti direktiiviä vastaavia kysymyksiä on käsitelty laajasti yleissopimusta ja puitepäätöstä koskevassa hallituksen esityksessä 153/2006 vp. Näin ollen aihealueen yleisesittelyn ja monien säännösten osalta voidaan viitata kyseiseen hallituksen esitykseen, eikä toistaminen tässä esityksessä ole tarkoituksenmukaista.

Tässä esityksessä katetaan vain direktiivin edellyttämät lisäykset voimassaolevaan lainsäädäntöön.

Direktiivin noudattamisen edellyttämät säädökset on saatettava voimaan viimeistään 4 päivänä syyskuuta 2015.

2 Nykytila

2.1 Lainsäädäntö

Suomen kansallinen lainsäädäntö on yleissopimuksen voimaansaattamisen ja puitepäätöksen täytäntöönpanotoimien yhteydessä saatettu monilta osin vastaamaan direktiivin vaatimuksia. Direktiivin kannalta merkityksellinen on rikoslain (39/1889) 38 luku tietoja viestintärikoksista. Kyseisessä luvussa ovat muun muassa direktiivin kannalta merkitykselliset säännökset viestintäsalaisuuden loukkauksesta (3 §), törkeästä viestintäsalaisuuden loukkauksesta (4 §), tietoliikenteen häirinnästä (5 §), törkeästä tietoliikenteen häirinnästä (6 §), lievästä tietoliikenteen häirinnästä (7 §), tietojärjestelmän häirinnästä (7 a §), törkeästä tietojärjestelmän häirinnästä (7 b §), tietomurrosta (8 §) ja törkeästä tietomurrosta (8 a §). Direktiivin kannalta olennainen on myös rikoslain 34 luku yleisvaarallisista rikoksista, jossa säädetään muun muassa vaaran aiheuttamisesta tietojenkäsittelylle (9 a §) ja tietoverkkorikosvälineen hallussapidosta (9 b §). Merkityksellisiä ovat myös 35 luvun säännökset vahingonteosta.

2.2 Kansainvälinen kehitys ja EU:n lainsäädäntö

Tietoverkkorikoksiin liittyvä kansainvälinen lainsäädäntö on ollut suhteellisen intensiivisen kehittämisen kohteena. Keskeisimpänä kansainvälisenä instrumenttina voidaan pitää edellä mainittua Euroopan neuvoston

piirissä laadittua tietoverkkorikossopimusta, joka on esikuvana tässäkin esityksessä käsiteltävälle direktiiville. Tietoverkkorikollisuuden maailmanlaajuisen ja korostetusti rajat ylittävän luonteen vuoksi tavoitteena on, että mahdollisimman moni valtio myös Euroopan neuvoston ulkopuolelta liittyisi siihen. Kaikki EU:n jäsenvaltiotkaan eivät ole siihen vielä liittyneet, joten tämän direktiivin voidaan olettaa tukevan myös kyseisten valtioiden liittymistä yleissopimukseen.

Toinen keskeinen instrumentti on aiemmin mainittu EU:n puitepäätös, joka korvattiin tässä esityksessä tarkoitetulla direktiivillä. Puitepäätös sisälsi säännöksiä samoista asioista kuin yleissopimus.

2.3 Nykytilan arviointi

Yleissopimuksen ja puitepäätöksen täytäntöönpanotoimien myötä Suomen rikoslainsäädäntö vastaa jo varsin kattavasti direktiivin vaatimuksia. Direktiivin edellyttämät keskeisimmät muutokset liittyvät enimmäisrangaistustasojen korottamiseen ja eräiden ankaroittamisperusteiden sisällyttämiseen kansalliseen lainsäädäntöön.

3 Esityksen tavoitteet ja keskeiset ehdotukset

Esityksen tarkoituksena on saattaa Suomen lainsäädäntö vastaamaan direktiivin vaatimuksia. Esityksessä ehdotetaan, että rikoslakiin tehdään direktiivin edellyttämät muutokset.

Rikoslain 34 luvun 9 a §:ssä tarkoitettuun vaaran aiheuttamiseen tietojenkäsittelylle ehdotetaan lisättäväksi tekotavaksi tietoverkkorikosvälineen käyttöön hankkiminen. Hallussapito on jo nykyisin rangaistavaa 9 b §:n mukaisesti. Muutos on osin tekninen, koska hallussapidon enimmäisrangaistusta ei olisi aiheellista direktiivistä johtuvista syistä korottaa kuuden kuukauden vankeusrangaistuksesta kahteen vuoteen vankeutta. Lukuun lisättäisiin myös uusi 14 §, jossa 9 a §:ssä tarkoitetun vaaran aiheuttamisen tietojenkäsittelylle ja 9 b §:ssä tarkoitetun tietoverkkorikosvälineen hallussapidon osalta viitattaisiin uuteen ehdotettuun 38 luvun 13 §:ään, joka sisältäisi tietojärjestelmän ja datan määritelmät.

Rikoslain 35 lukuun ehdotetaan lisättäväksi uusi datavahingontekoa koskeva kriminalisointi (3 a §) sekä datavahingonteon törkeä (3 b §) ja lievä (3 c §) tekomuoto. Mainitut muutokset tehdään lähinnä teknisistä syistä sekä sen vuoksi, että muun muassa direktiivin edellyttämää enimmäisrangaistuksen korottamista ei olisi aiheellista ulottaa perinteiseen vahingontekoon. Tämän johdosta luvun 1 §:ssä tarkoitetun vahingonteon 2 ja 3 momentti sekä törkeää vahingontekoa koskevan 2 §:n 1 momentin 2 kohta ehdotetaan kumottavaksi. Myös datavahingonteon tekotapoja täsmennettäisiin. Törkeä datavahingonteko sisältäisi kvalifiointiperusteet, joiden osalta direktiivi edellyttää datavahingonteon enimmäisrangaistuksen vähimmäistasoksi vähintään kolmen ja viiden vuoden vankeutta. Mainitut kvalifiointiperusteet liittyvät niin sanottujen bottiverkkojen käyttöön, rikollisjärjestöihin, huomattavaan vahinkoon ja elintärkeään infrastruktuuriin. Datavahingontekojen erottaminen itsenäisiksi kriminalisoinneikseen edellyttää myös syyteoikeutta koskevan 6 §:n, toimenpiteistä luopumista koskevan 7 §:n ja oikeushenkilön rangaistusvastuuta koskevan 8 §:n teknistä tarkistamista vastaamaan edellä mainittua muutosta. Lukuun lisättäisiin myös uusi 9 §, jossa 3 a §:ssä tarkoitetun datavahingonteon ja 3 b §:ssä tarkoitetun törkeän datavahingonteon osalta viitattaisiin uuteen ehdotettuun 38 luvun 13 §:ään, joka sisältäisi tietojärjestelmän ja datan määritelmät.

Rikoslain 38 luvun 3 §:ssä tarkoitettua viestintäsalaisuuden loukkausta ehdotetaan muutettavaksi niin, että se kattaa direktiivin vaatimusten mukaisesti myös tietojärjestelmän sisäisen luottamuksellisen datan siirron. Lisäksi viestintäsalaisuuden loukkauksen enimmäisrangaistusta ehdotetaan korotetavaksi kahteen vuoteen vankeutta.

Tietojärjestelmän häirintää koskevasta 7 a §:stä ehdotetaan poistettavaksi toissijaisuuslauseke, jotta soveltamistilanteissa ei jouduttaisi epätarkoituksenmukaisiin tilanteisiin direktiivin edellyttämien muiden rikosten rangaistustasojen muutosten vuoksi. Soveltamistilanteet ratkaistaisiin yleisten konkur-

renssia koskevien periaatteiden mukaisesti. Törkeää tietoliikenteen häirintää (RL 38 luvun 6 §) ja törkeää tietojärjestelmän häirintää (7 b §) ehdotetaan myös muutettavaksi siten, että ne sisältäisivät törkeää datavahingontekoa vastaavat direktiivin edellyttämät kvalifiointiperusteet. Mainittujen törkeiden tekomuotojen enimmäisrangaistusta ehdotetaan nostettavaksi viiteen vuoteen vankeutta direktiivin edellyttämällä tavalla. Rikoslain 38 luvun 8 §:ssä tarkoitettua tietomurtoa ehdotetaan myös muutettavaksi niin, että se kattaa direktiivin edellyttämin tavoin myös pääsyn tietojärjestelmässä olevaan dataan ja tiedon hankkimisen siitä. Tietomurron enimmäisrangaistusta ehdotetaan nostettavaksi kahteen vuoteen vankeutta. Tämän johdosta myös törkeän tietomurron (8 a §) enimmäisrangaistusta ehdotetaan korotettavaksi kahdesta vuodesta kolmeen vuotta vankeutta. Rikoslain 38 lukuun ehdotetaan sisällytettäväksi myös direktiivin velvoitteisiin pohjautuvat avoimet tietojärjestelmän ja datan määritelmät (uusi 13 §).

Rikoslain 38 lukuun ehdotetaan direktiivin velvoitteiden täyttämiseksi uutta identiteettivarkautta koskevaa 9 b pykälää. Syyteoikeutta koskevan 10 §:n mukaan identiteettivarkaus olisi asianomistajarikos. Identiteettivarkaus lisättäisiin myös sotilasoikeudenkäyntilain 2 §:ssä tarkoitettujen sotilasoikeudenkäyntiasiana käsiteltävien rikosten listaan.

Rikoslain 38 luvun 11 §:ssä oleva virheellinen pykäläviittaus ehdotetaan korjattavaksi.

Pakkokeinolain 10 luvun 3 §:ään tehtäisiin tarkistus, jossa lakiin lisättäisiin maininta ehdotetusta törkeästä datavahingonteosta. Luvun televalvontaa koskevaan 6 §:ään tehtäisiin tekninen tarkistus johtuen siitä, että eräitä siinä mainittuja rikoksia ei ole enää tarpeen nimenomaisesti listata, johtuen mainittujen rikosten ehdotetuista enimmäisrangaistustasojen nostosta. Vastaava tarkistus tehtäisiin myös poliisilain 5 luvun 8 §:n televalvontaa koskeviin säännöksiin.

4 Esityksen vaikutukset

Rikoslakiin tehtävät uudet säännökset laajentavat sähköisessä muodossa olevan tiedon ja tiedonvälityksen rikosoikeudellista suojaa. Tietoverkkorikollisuuteen liittyvän lainsäädännön lähentäminen Euroopan unionin jäsenvaltioiden välillä saattaa jossain määrin edesauttaa Suomen viranomaisten mahdollisuuksia selvittää sellaisia rajat ylittäviä rikoksia, joiden vahingolliset seuraukset ilmenevät Suomessa. Esityksessä tarkoitettu ympärivuorokautisen päivystyspisteen toiminnan tehostaminen parantaa yhteistyön edellytyksiä rajat ylittävien rikosten selvittämisessä. Päivystyspisteen on edelleen tarkoitus toimia keskusrikospoliisissa. Esityksellä on tältä osin vain vähäisiä poliisiin kohdistuvia organisaatio- ja henkilöstövaikutuksia, jotka eivät edellytä resurssien lisäämistä.

Rikoksista mahdollisesti tuomittavien vankeusrangaistusten enimmäistason nosto saattaa aiheuttaa lisääntyviä täytäntöönpanokuluja. Koska kyseessä ovat kuitenkin teoreettiset enimmäisrangaistukset, ei ole oletettavaa, että kulujen lisäys olisi merkittävää. Esityksessä ehdotettava identiteettivarkaus olisi kuitenkin täysin uusi kriminalisointi. Identiteettivarkaudenkaan osalta ei ole oletettavaa, että täytäntöönpanokulujen lisäys olisi merkittävä. Identiteettivarkaus tapahtunee usein osana muuta rangaistavaa käyttäytymistä, jolloin tuomittava seuraamus olisi usein osa yhteistä rangaistusta. Itsenäisenä rikoksena toteutuessaan seuraamuksena olisi sakkorangaistus. Identiteettivarkaustapaukset eivät todennäköisesti olisi kovin harvinaisia. Näin ollen niiden tutkinta edellyttänee viranomaisten resurssien kohdentamista myös näihin tapauksiin. Tutkittavien tapausten määrään vaikuttaa se, että identiteettivarkaus olisi ehdotuksen mukaan asianomistajarikos.

Tietoverkkorikollisuudella yleisesti voi olettaa olevan merkittävää vaikutusta koko yhteiskuntaan, talous mukaan lukien. Näin ollen tehokkaalla tietoverkkorikollisuuteen puuttumisella kattavien ja toimivien kriminalisointien avulla voidaan olettaa olevan myönteisiä yhteiskunnallisia ja taloudellisia vaikutuksia.

Esityksessä ehdotetuilla rikoslain muutoksilla on vaikutuksia myös joihinkin pakkokeinolaissa (806/2011) tarkoitettuihin toimivaltuuksiin. Tämä johtuu siitä, että nostettaessa enimmäisrangaistuksia, eräät pakkokeinot tulevat sovellettaviksi ilman, että pakkokeinolakia muutetaan.

Esityksessä ehdotetaan tietomurron ja viestintäsalaisuuden loukkauksen enimmäisrangaistuksen nostamista kahteen vuoteen vankeutta. Myös ehdotetun datavahingonteon enimmäisrangaistus olisi kaksi vuotta vankeutta. Tämä merkitsee sitä, että mainittujen tekojen osalta ovat sovellettavissa myös pakkokeinolain 10 luvun 12 §:ssä tarkoitettu suunnitelmallinen tarkkailu, 27 §:n 3 momentissa tarkoitettu tietoverkossa tapahtuva peitetoiminta, sekä 34 §:ssä tarkoitettu valeosto sillä kyseisiä pakkokeinoja on mahdollista käyttää, mikäli henkilöä on syytä epäillä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Luvun 6 §:n 2 momentin 3 kohdan mukaisesti televalvonta on jo nykyisin mahdollista teleosoitetta tai telepäätelaitetta käyttäen tehdyn vahingonteon, viestintäsalaisuuden loukkauksen ja tietomurron osalta vaikka ne eivät nykyisin sisälläkään kahden vuoden vankeuden enimmäisrangaistusta. Näin ollen esityksessä ehdotetut kahden vuoden vankeuden käsittävät enimmäisrangaistukset eivät asiallisesti laajenna 6 §:ssä tarkoitetun televalvonnan käytön mahdollisuutta. Oikeus luvun 7 §:ssä tarkoitettuun teleosoitteen tai telepäätelaitteen haltijan suostumuksella tapahtuvaan televalvontaan sen sijaan laajenisi enimmäisrangaistuksen noston johdosta kattamaan myös ne tilanteet, joissa datavahingontekoa, viestintäsalaisuuden loukkausta tai tietomurtoa ei olisi tehty teleosoitetta tai telepäätelaitetta käyttäen.

Pakkokeinolain 10 luvun 56 §:ssä tarkoitetun ylimääräisen tiedon käytön osalta jatkossa olisi mahdollista pakkokeinolaissa tarkoitetuin edellytyksin käyttää ylimääräistä tietoa myös törkeän tietomurron tutkintaan, sillä esityksen mukaan sen enimmäisrangaistus olisi jatkossa kolme vuotta vankeutta.

Ehdotetuilla rikoslain muutoksilla olisivat pakkokeinolakia vastaavat vaikutukset myös poliisilain (872/2011) toimivaltuuksiin koskien lain 5 luvun 13 pykälässä tarkoitettua suunnitelmallista tarkkailua, 28 §:n 3 momentissa tarkoitettua tietoverkossa tapahtuvaa peitetoimintaa, 35 §:ssä tarkoitettua valeostoa sekä 54 §:ssä tarkoitettua ylimääräisen tiedon käyttöä. Vaikutukset 8 §:ssä tarkoitettuun televalvontaan ja 9 §:ssä tapahtuvaan teleosoitteen tai telepäätelaitteen haltijan suostumuksella tapahtuvaan televalvontaan ovat vastaavat kuin edellä pakkokeinolain osalta.

Esityksellä pannaan täytäntöön kansallisen kyberturvallisuusstrategian toimeenpano-ohjelman toimenpide 62. Turvallisuuskomitea hyväksyi toimeenpano-ohjelman 11 päivänä maaliskuuta 2014.

5 Asian valmistelu

Oikeusministeriö asetti 27 päivänä syyskuuta 2013 työryhmän, jonka tehtäväksi annettiin valmistella ehdotus tietojärjestelmiin kohdistuvia hyökkäyksiä ja neuvoston puitepäätöksen 2005/222/YOS korvaamista koskevan direktiivin 2013/40/EU täytäntöönpanoa koskevaksi kansalliseksi lainsäädännöksi. Ehdotus oli laadittava hallituksen esityksen muotoon. Tehtävässä työssä oli otettava huomioon myös identiteettivarkautta koskeva arviomuistio (OM 4/41/2013) ja siitä saatu lausuntopalaute siltä osin kuin se koskee kysymyksessä olevaa oikeusministeriön toimialaan kuuluvaa rikoslainsäädäntöä.

Työryhmässä oli oikeusministeriön lisäksi edustus sisäministeriöstä, liikenne- ja viestintäministeriöstä, valtakunnansyyttäjänvirastosta, tietosuojavaltuutetun toimistosta ja Suomen Asianajajaliitosta.

Työryhmä kuuli työnsä aikana Tietoturva ry:tä, FISC ry:tä (Finnish Information Security Cluster), Viestintävirastoa ja keskusrikospoliisia.

Esitys perustuu työryhmän mietintöön (Tietoverkkorikosdirektiivin täytäntöönpano, Mietintöjä ja lausuntoja 27/2014) ja mietinnöstä saatuihin lausuntoihin. Lausunto pyydettiin 39 viranomaiselta, järjestöltä tai asiantuntijalta. Lausunnoista on laadittu tiivistelmä (Oikeusministeriö, mietintöjä ja lausuntoja, 35/2014). Yleisesti ottaen lausunnoissa suhtauduttiin myönteisesti työryhmän esityksiin. Lausuntopalautteessa nousi esiin ehdotettu identiteettivarkautta koskeva erillinen kriminalisointi, jota laajasti kannatettiin. Eräät lausunnonantajat kuitenkin toivoivat sisäministeriön työryhmäedustajan eriävän mielipiteen mukaisesti sitä, että pakkokeinolain 10 luvun 6 §:ssä tarkoitettu televalvonta olisi mahdollista myös silloin, kun identiteet-

tivarkaus esiintyy itsenäisenä rikoksena, eikä esimerkiksi teleosoitetta tai telepäätelaitetta käyttäen tehdyn petoksen yhteydessä, jolloin petoksen tutkinnassa voidaan käyttää televalvontaa.

Esityksessä on edellä mainituilta osin pysytty työryhmän mietinnössä esitetyssä. Ensinnäkin identiteettivarkauden yhteydessä on käytettävissä erilaisia tutkintakeinoja ja -valtuuksia tapauksesta riippuen. Identiteettivarkauden tutkinnassa käytettävissä olevia tutkintakeinoja on selostettu esityksen yksityiskohtaisissa perusteluissa. Perusteluissa on tuotu esiin sanavapauden käyttämisestä joukkoviestinnässä säädetyn lain (460/2003) 17 §:n mukaiset mahdollisuudet verkkoviestin tunnistamistietojen selvittämiseen. Edelleen perusteluissa on mainittu mahdollisuudet pakkokeinolain 10 luvun 7 §:ssä tarkoitettuun teleosoitteen tai telepäätelaitteen haltijan suostumuksella tapahtuvaan televalvontaan silloin kun teko on tehty teleosoitetta tai telepäätelaitetta käyttäen. Myös poliisilain 4 luvun 3 §:ssä tarkoitetut tiedonsaantikeinot ovat käytettävissä identiteettivarkauden tutkinnassa.

Tutkinnan kannalta haasteellisia voivat joissain tapauksissa olla tilanteet, joissa rikos on tehty useamman päätelaitteen kautta (HE 14/2013 vp, s. 19). Suostumusperusteisessa televalvonnassa tietojen saanti edellyttää tällöin suostumusta useammalta tiedonvälitysketjussa olevalta taholta. Samoin tulevaisuudessa toimintaympäristön muutokset voivat aiheuttaa uusia ennakoimattomia haasteita, kun perinteiset rikostyypit saattavat siirtyä tietoverkkoon. Nyt ehdotetun identiteettivarkautta koskevan rangaistussäännöksen lisäksi rikoslaissa on kuitenkin nyt ja tulevaisuudessa muitakin suhteellisen vähäisiä rikoksia, joiden osalta poliisilla ei ole käytössään kaikkia salaisia pakkokeinoja muun muassa jäljempänä selostetun perusoikeuksien suojan vuoksi.

Käytettävissä olevien pakkokeinojen tulee olla oikeasuhtaisia. Salaisia telepakkokeinoja tulisi lähtökohtaisesti käyttää vain vakavien rikosten tutkinnassa. Pakkokeinolain 10 luvun 6 §:n mukaisesti yleinen edellytys televalvonnan käyttämiselle on, että rikoksesta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta. Teleosoitetta tai telepäätelaitetta käyttäen tehdyn rikoksen osalta yleinen televalvonnan edellytys on vähintään kahden vuoden enimmäisrangaistus. Identiteettivarkaus itsenäisenä rikoksena esiintyessään on kuitenkin varsin lievä teko, joka helposti täyttää myös jonkun muun törkeämmän rikoksen tunnusmerkistön.

Salaisten telepakkokeinojen käyttöä sakkorikosten tai suhteellisen lievien rikosten osalta esityksessä kuvattua laajemmin rajoittavat myös perustuslain 10 §:n säännökset yksityiselämän ja luottamuksellisen viestinnän suojasta. Perustuslakivaliokunnan vakiintuneessa käytännössä viestin tunnistamistietojen on aikaisemmin katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perustuslain 10 §:ssä tarkoitetun perusoikeuden ydinalueen ulkopuolelle. Perustuslakivaliokunta on kuitenkin antanut tuoreen lausunnon (PeVL 18/2014 vp) ehdotettuun tietoyhteiskuntakaareen ja Unionin tuomioistuimen 8.4.2014 antamaan tuomioon liittyen. Mainitulla tuomiolla Unionin tuomioistuin totesi tunnistamistietojen tallentamista koskevan neuvoston ja parlamentin direktiivin 24/2006/EY kokonaisuudessaan pätemättömäksi. Perustuslakivaliokunta toteaa lausunnossaan (s. 6), että käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen.

Edelleen perustuslakivaliokunnan lausunnossa analysoidaan säilytettävien tietojen käyttämistä todeten niitä voitavan käyttää ainoastaan pakkokeinolain 10 luvun 6 §:ssä tarkoitettujen rikosten tutkimiseksi. Valiokunnan lausunnon mukaan sääntely täyttää tuomiossa tarkoitetun vaatimuksen käyttää niitä vain *vakavien* rikosten yhteydessä.

6 Muita esitykseen vaikuttavia seikkoja

Eduskunnan käsiteltävänä on parhaillaan hallituksen esitys (HE 18/20014 vp.) terrorismirikoksia koskevaksi lainsäädännöksi.

Esityksessä ehdotetaan muutettavaksi muun muassa pakkokeinolain 10 luvun 3 ja 6 §:ää sekä poliisilain 5 luvun 8 §:ää. Nyt käsiteltävässä ehdotuksessa ehdotetaan myös muutettavaksi mainittuja pakkokeinolain ja poliisilain pykäliä. Edellä mainitun vuoksi kyseiset ehdotukset tulisi yhteensovittaa niitä eduskunnassa käsiteltäessä.

YKSITYISKOHTAISET PERUSTELUT

1 Direktiivin sisältö ja sen suhde Suomen lainsäädäntöön

1 artikla. *Kohde.* Artiklan mukaan 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. Artikla ei edellytä lainsäädännön muuttamista.

2 artikla. *Määritelmät.* Artikla sisältää määritelmät. Direktiivin määritelmät vastaavat lähtökohtaisesti asiasisällöltään yleissopimuksen ja puitepäätöksen vastaavia määritelmiä, joita on tarkemmin eritelty hallituksen esityksessä 153/2006 vp. Artiklan a kohdan mukaan tietojärjestelmällä tarkoitetaan 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. Data on määritelty jäljempänä b kohdassa. Määritelmä vastaa tietojärjestelmän osalta sisällöllisesti yleissopimuksen 1 artiklan a kohdassa ja puitepäätöksen 1 artiklan a kohdassa olevaa tietojärjestelmän määritelmää. Direktiivin ja puitepäätöksen sanamuoto poikkeaa yleissopimuksen vastaavasta määritelmästä kuitenkin siten, että yleissopimuksessa tietojärjestelmässä olevaa dataa ei ole erikseen mainittu tietojärjestelmän käsitteeseen kuuluvana osana. Mainitulla tarkennuksella on muun muassa merkitystä direktiivin 3 artiklan osalta, joka määritelmän myötä sisältää kriminalisointivelvoitteen tietojärjestelmään tunkeutumisen ohella myös pääsyn hankkimiseen tietojärjestelmässä olevaan tietoon. Määritelmää käytetäänkin 3—7 artikloissa rajaamaan rangaistaviksi säädettävien rikosten alaa. Yleissopimuksessa oleva tietojärjestelmän määritelmä on saatettu osaksi Suomen kansallista lainsäädäntöä yleissopimuksen voimaansaattamislailla. Puitepäätöksen määritelmiä ei ole nimenomaisesti saatettu osaksi Suomen lainsäädäntöä. Selvyyden vuoksi esityksessä ehdotetaan, että rikoslain 38 lukuun sisällytettäisiin direktiivin 2 artiklan a kohdassa oleva tietojärjestelmän määritelmä niiden rikosten osalta, jotka vastaavat tässä direktiivissä tarkoitettuja kriminalisointivelvoitteita. Määritelmä olisi avoin ja tekniikkaneutraali siten, että tietojärjestelmän käsitettä ei viitattujen rikoslain säännösten osaltakaan rajattaisi direktiivissä tarkoitettuun määritelmään, vaan tietojärjestelmällä tarkoitettaisiin myös sitä mitä direktiivissä tarkoitetaan tietojärjestelmällä ja siinä olevalla datalla. Näin täytettäisiin direktiivin asettamat vaatimukset. Koska kyseessä on direktiivin velvoitteiden täytäntöönpanon varmistamiseksi sisällytettävä avoin määritelmä, esityksessä ehdotetaan, että se kattaa vain ne kriminalisoinnit, joiden on tarkoitettu kattavan direktiivin velvoitteet.

Artiklan b kohdan mukaan 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. Määritelmä vastaa sanatarkasti yleissopimuksen ja puitepäätöksen vastaavia määritelmiä. Datan käsitettä käytetään edellä a kohdassa tietojärjestelmän määritelmässä sekä 4, 5 ja 6 artikloissa rajaamaan rangaistaviksi säädettävien rikosten alaa. Yleissopimuksessa oleva datan määritelmä on saatettu osaksi Suomen kansallista lainsäädäntöä yleissopimuksen voimaansaattamislailla. Selvyyden vuoksi ja datan määritelmän ollessa edellä a kohdassa todetun mukaisesti kiinteässä yhteydessä tietojärjestelmän määritelmään, esityksessä ehdotetaan, että rikoslain 38 lukuun otetaan tietojärjestelmän käsitteen tavoin direktiivin 2 artiklan b kohdan määritelmää vastaava avoin määritelmä, jonka mukaan datalla tarkoitetaan myös direktiivissä tarkoitettua dataa niiden rikosten osalta, jotka vastaavat direktiivissä tarkoitettuja kriminalisointivelvoitteita. Näin täytettäisiin direktiivin vaatimukset. Koska kyseessä on direktiivin velvoitteiden täytäntöönpanon varmistamiseksi sisällytettävä

avoin määritelmä, esityksessä ehdotetaan, että se kattaa vain ne kriminalisoinnit, joiden on tarkoitettu kattavan direktiivin velvoitteet.

Artiklan c kohdan mukaan oikeushenkilöllä tarkoitetaan yksikköä, jolla on sovellettavan lain mukaan oikeushenkilön asema, lukuun ottamatta valtiota tai julkisia elimiä niiden käyttäessä julkista valtaa, tai julkisoikeudellisia kansainvälisiä järjestöjä. Kohta vastaa sanatarkasti puitepäätöksen määritelmää. Määritelmä on vakiomuotoilu, jota käytetään yleisesti Euroopan unionin rikosoikeudellisissa säädöksissä. Määritelmästä seuraa, että oikeushenkilön käsite määräytyy kansallisen lainsäädännön mukaisesti. Määritelmän ainoa sisältö on rajaus, jonka mukaan valtio ja muut vastaavat julkiset elimet jäävät käsitteen ulkopuolelle. Määritelmää käytetään 10 ja 11 artikloissa rajaamaan oikeushenkilöiden vastuuta koskevien määräysten soveltamisalaa sekä 12 artiklan 3 kohdan b alakohdassa, jossa on kyse lainkäyttövaltaa koskevasta erityissäännöksestä. Yleissopimuksessa ei ole vastaavaa määritelmää. Rikoslain 9 luvun 1 §:n 2 momentin mukaan oikeushenkilön rangaistusvastuuta koskevan luvun säännöksiä ei sovelleta julkisen vallan käytössä tehtyyn rikokseen. Kohta ei edellytä lainsäädännön muuttamista.

Artiklan d kohdan mukaan ilmaisulla oikeudettomasti tarkoitetaan 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. Määritelmää käytetään 3—7 artikloissa rajaamaan omistajan luvalla tai muutoin oikeutetut teot artiklojen soveltamisalan ulkopuolelle. Puitepäätöksessä on asiallisesti vastaavankaltainen määritelmä. Siinä ei kuitenkaan mainita laitonta tietojen hankkimista, sillä puitepäätös ei sisällä sitä koskevaa artiklaa. Direktiivin määritelmässä viitataan lisäksi kaikkeen direktiivissä tarkoitettuun toimintaan, johon ei ole lupaa tai joka ei ole sallittua kansallisen lainsäädännön nojalla. Yleissopimuksessa ei ole vastaavaa määritelmää. Rikosoikeuden yleisten perusperiaatteiden mukaisesti oikeudetonta ei ole sellainen toiminta, johon on lupa. Oikeudetonta ei luonnollisesti ole myöskään sellainen toiminta, joka on sallittua kansallisen lainsäädännön nojalla. Kohta ei edellytä lainsäädännön muuttamista.

3 artikla. *Laiton tunkeutuminen tietojärjestelmään.* Artiklan mukaan 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. Artikla vastaa asiasisällöltään puitepäätöksen vastaavaa artiklaa. Puitepäätöksessä turvajärjestelyn murtamista koskeva edellytys on tosin ollut valinnainen mahdollisuus kun taas direktiivissä se on sisällytetty itse perustekomuodon kuvaukseen. Asiallisesti erolla ei ole Suomen kannalta merkitystä. Myös yleissopimus sisältää vastaavan artiklan, joskaan siinä ei ole vähäisiä tapauksia koskevaa nimenomaista poikkeussäännöstä. Lisäksi yleissopimus sallii rajauksen, jonka mukaan rikoksen tulee liittyä sellaiseen tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään. Eroavuuksilla ei ole Suomen kannalta käytännön merkitystä.

Yleissopimuksen ja puitepäätöksen vastaavaa määräystä on käsitelty yksityiskohtaisesti puitepäätöstä ja yleissopimuksen voimaansaattamista koskevassa hallituksen esityksessä (HE 153/2006 vp), joten sen toistaminen vastaavassa laajuudessa ei ole tarkoituksenmukaista tässä yhteydessä. Suomessa voimassa olevat säännökset artiklassa tarkoitetusta laittomasta tunkeutumisesta tietojärjestelmään sisältyvät rikoslain tietomurtoa koskevaan 38 luvun 8 §:ään. Mainitun lainkohdan mukaan tietomurrosta on tuomittava se, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan. Saman pykälän 2 momentin mukaan tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta. Säännös kattaa

siis myös ”dataan” tunkeutumista, joka on oleellista tietojärjestelmän käsitteen määrittelystä johtuen. Pykälän 3 momentin mukaan tietomurron yritys on rangaistava. Pykälän 4 momentin mukaan säännös on toissijainen.

Hallituksen esityksen 153/2006 vp mukaan tuolloin voimassaolevat säännökset vastasivat artiklan velvoitteita. Suomi on yleissopimuksen yhteydessä antanut sen salliman selityksen, jonka mukaan Suomi käyttää hyväkseen oikeutta asettaa rangaistavuuden edellytykseksi sen, että rikos on tehty turvajärjestelyt murtamalla.

Edellä 2 artiklan a kohdan tietojärjestelmän määritelmän yhteydessä todetuin tavoin tietojärjestelmän käsite kattaa myös tietojärjestelmässä olevan datan. Näin ollen artiklan kriminalisointivelvoite kattaa myös tunkeutumisen tietojärjestelmässä olevaan dataan, kun teko on tehty oikeudettomasti ja murtamalla turvajärjestely. Suomenkielisessä direktiivin versiossa oleva käsite ”tunkeutuminen” on osin epäselvä ja harhaanjohtava, sillä tältä osin kyse on asiallisesti rikoslain 38 luvun 8 pykälän 2 momentin tarkoittamasta selon ottamisesta tietojärjestelmässä olevasta tiedosta. (Direktiivin englanninkielisessä versiossa käytetään muotoilua ”access to”). Mainitun 2 momentin mukaan tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta. Mainitussa säännöksessä ei ole teon oikeudettomuutta koskevan kriteerin lisäksi muuta teon rangaistavuuden rajausta kuin se, että teko tehdään teknisellä erikoislaitteella. Tämä on oleellista, sillä 2 momentti täyttää yleissopimuksen ja direktiivin 6 artiklan viestintäsalaisuuden loukkausta koskevat velvoitteet dataa sisältävästä tietojärjestelmästä lähtevän sähkömagneettisen säteilyn osalta. Edellä todetun vuoksi esityksessä ehdotetaan, että tietomurtoa koskevan rikoslain 38 luvun 8 pykälän 2 momenttia täydennettäisiin niin, että se kattaisi teknisen erikoislaitteen käyttämisen lisäksi selon ottamisen tietojärjestelmässä olevasta tiedosta tai datasta myös muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksikäyttäen tai muuten ilmeisen vilpillisin keinoin. Ilmeisen vilpillinen keino voi olla esimerkiksi tietokoneohjelman hyväksikäyttö.

Ehdotetun muutoksen myötä 2 momentissa katettaisiin tekniikkaneutraalisti kaikki sellaiset tilanteet, joissa tietojärjestelmään tunkeutumatta oikeudettomasti ja ilmeisen vilpillisin keinoin otetaan selko tietojärjestelmässä olevasta tiedosta tai datasta. Ehdotetun 2 momentin on siten tarkoitus kattaa muun muassa tilanteet, jossa dataa syöttämällä tietojärjestelmä saadaan toimimaan virheellisesti ja antamaan sen sisältämää tietoa (esimerkiksi ns. SQL -injektio) sekä tilanteet, jossa tietojärjestelmässä olevasta tiedosta tai datasta otetaan selko haittaohjelman avulla.

Tietomurtoa koskevan pykälän 1 momenttiin ehdotetaan lisättäväksi sanan ”tieto” lisäksi sana ”data”, sillä datan käsite kuvaa kattavammin pykälässä säänneltäväksi tarkoitettua seikkaa. Myös direktiivissä käytetään sanaa data, ja käsite esitetään direktiivissä edellytetyin tavoin määriteltäväksi.

On syytä huomioida, että konkreettisesta tapauksesta riippuen kunkin kriminalisoinnin luonne erityissäännöksenä, erityinen tekotapa, kriminalisoinnissa tarkoitetun teon valmisteluluonteisuus suhteessa mahdollisesti muuhun mahdollisesti sovellettavaksi tulevaan kriminalisointiin ja kriminalisoinnilla suojattava oikeushyvä yleensä ratkaisevat sen, mikä rikosnimike kulloinkin tulee sovellettavaksi. Soveltamistilanteet tulee ratkaista tapauskohtaisesti yleisten lainkonkurrenssia koskevien periaatteiden mukaisesti eikä ehdottomia tulkintaohjeita voida antaa tapausten moninaisuuden vuoksi.

Jos esimerkiksi tietojärjestelmään murtautumalla hankittaisiin tieto ulkopuoliselta suojatusta tallennetusta viestistä, tulisi yleensä sovellettavaksi ainoastaan rikoslain 38 luvun 3 pykälässä tarkoitettu viestintäsalaisuuden loukkaus. Teko sinänsä täyttää tietomurron tunnusmerkistön, mutta tietomurtoa voidaan tällöin pitää valmisteluluonteisena tekona suhteessa viestintäsalaisuuden loukkaukseen. Viestintäsalaisuuden loukkaus voi lisäksi olla erityissäännön asemassa suhteessa tietomurtoon. Vaikka tietomurtoa koskevan kriminalisoinnin soveltamisala on melko laaja, voivat siten erityinen tekotapa, suojattava oikeushyvä, säännöksen luonne erityissäännöksenä tai valmisteluluonteisten tekojen väis-

tymistä koskeva periaate johtaa siihen, että muu kriminalisointi tulee sovellettavaksi. Tietomurtoa koskevan pykälän osalta on lisäksi huomattava, että se sisältää toissijaisuuslausekkeen, jota ei ehdoteta kumottavaksi.

Yleisten lainkonkurrenssia koskevien periaatteiden ja tietomurron toissijaisuuslausekkeen tukemana tietomurto voi väistyä, mikäli teko täyttää myös datavahingonteon, tietojärjestelmän häirinnän tai tietoliikenteen häirinnän tunnusmerkistön. Tietomurto on usein näiden suhteen myös valmisteluluonteinen teko. Rikoslain 35 luvun 5 §:ään sisältyvä rajoitussäännös ei ole tässä tapauksessa merkityksellinen, koska tietomurto ei edellytä vahingon aiheuttamista.

Tietomurron ja rikoslain 28 luvun 7 §:ssä tarkoitetun perustunnusmerkistön mukaisen luvattoman käytön välinen suhde ei enää ratkeaisi tietomurtoa koskevan toissijaisuuslausekkeen perusteella. Luvattoman käytön enimmäisrangaistus on vain yksi vuosi vankeutta ja törkeän tekomuodon kaksi vuotta, kun taas tietomurron enimmäisrangaistus on kaksi vuotta vankeutta ja törkeän tekomuodon kolme vuotta vankeutta. Rikosten suhde määräytyisi yleisten lainkonkurrenssia koskevien periaatteiden mukaisesti, ja tapauksesta riippuen luvattoman käytön lisäksi voitaisiin tuomita myös tietomurrosta. Tämä on perusteltua, koska luvattomalla käytöllä suojellaan omaisuudensuojan ja taloudellisen intressin kaltaisia oikeushyviä kun taas tietomurtokriminalisoinnin suojeluobjektina on ennen kaikkea tietojärjestelmän luottamuksellisuus. Toisaalta on huomattava, että tietomurto voisi tapauskohtaisesti myös väistyä muiden lainkonkurrenssia koskevien yleisten periaatteiden myötä. Luvatonta käyttöä koskeva säännös ei esimerkiksi tulisi sovellettavaksi, jos käyttö jäisi niin vähämerkitykselliseksi, että se olisi käytännössä seurausta tietomurron kattamasta järjestelmään tunkeutumisesta. Selvyyden vuoksi voidaan myös todeta, että 28 luvun 7 §:n 3 momentin mukaisesti luvattomana käyttönä ei pidetä suojaamattoman langattoman tietoverkkoyhteyden kautta muodostetun internet-yhteyden käyttämistä.

Rikoslain 34 luvun 9 b §:ssä tarkoitettu tietoverkkorikosvälineen hallussapito puolestaan voi valmisteluluonteisena tekona väistyä esimerkiksi tietomurron tieltä. Kun sinänsä rangaistava esineen hallussapito liittyy johonkin sitä vakavamman rikoksen tekemiseen, ei oikeuskäytännössä yleensä ole luettu syyksi erillistä hallussapitoa. Näin ollen tietoverkkorikosvälineen hallussapitoa ei yleensä pidettäisi eri rikoksena, jos hallussapitäjä on välinettä käyttäessään syyllistynyt joko tekijänä tai osallisena johonkin muuhun ankarammin rangaistavaan rikokseen. Myös rikoslain 34 luvun 9 a §:ssä tarkoitettu vaaran aiheuttaminen tietojenkäsittelylle on joissakin tapauksissa valmisteluluonteinen teko ja siten väistyy esimerkiksi datavahingonteon, tietojärjestelmän häirinnän ja tietoliikenteen häirinnän tieltä. Mainittu säännös sisältää lisäksi nimenomaisen toissijaisuuslausekkeen, jota ei ehdoteta kumottavaksi. Vaaran aiheuttamisen tietojenkäsittelylle (9 a §) suhde 28 luvun 7 §:ssä tarkoitettuun luvattomaan käyttöön säilyisi entisellään ja sen sekä 28 luvun 7 §:n enimmäisrangaistukset säilyisivät entisellään. Vaikka vaaran aiheuttaminen tietojenkäsittelylle voi tapauskohtaisesti olla valmisteluluonteinen teko, voidaan siitä eräissä tapauksissa rangaista itsenäisesti. Tällainen tilanne voisi olla käsillä esimerkiksi silloin, kun 9 a §:ssä tarkoitettu teko kohdistuu useisiin kohteisiin tai on muuten laajamittainen, ja luvaton käyttö tapahtuisi vain esimerkiksi yhdessä tietojärjestelmässä. Tällöin on perusteltua, että tekijä voidaan tuomita luvattoman käytön lisäksi myös vaaran aiheuttamisesta tietojenkäsittelylle. Tämä on perusteltua, sillä luvattoman käytön kriminalisoinnilla suojellaan taloudellisen intressin kaltaisia oikeushyviä ja yksittäisen järjestelmän tietojenkäsittelyrauhaa kun taas 9 a §:ssä suojellaan ennen kaikkea yleisesti tietojenkäsittelyn ja tietojärjestelmien turvallisuutta ja teko voi vaarantaa useita tietojärjestelmiä.

Vaaran aiheuttaminen tietojenkäsittelylle voi joissain tapauksissa valmisteluluonteisena tekona väistyä myös tietomurron tieltä edellä mainittujen periaatteiden mukaisesti.

Datavahingonteon, tietojärjestelmän häirinnän ja tietoliikenteen häirinnän suhde taas voi tapauskohtaisesti ratketa säännöksen erityisluonteen avulla. Tietoliikenteen häirintää koskevalla kriminalisoinnilla (RL 38 luvun

5 §) suojellaan ennen kaikkea tietoliikennettä. Näin ollen se on erityissäännön asemassa suhteessa tietojärjestelmän häirintään (RL 38 luvun 7 a §), jos häirittävä tietojärjestelmä on olennainen erityisesti tietoliikenteen kannalta. Näiden kahden rikoksen välinen suhde ei siten muutu, vaikka teknisistä syistä tietojärjestelmän häirinnän toissijaisuuslauseke ehdotetaankin kumottavaksi, jotta direktiivin edellyttämien rangaistustasojen muutokset eivät johtaisi epätarkoituksenmukaisin soveltamistilanteisiin esimerkiksi datavahingonteon ja tietojärjestelmän häirinnän välillä niiden enimmäisrangaistusten ollessa jatkossa yhtenevät. Jatkossa soveltamistilanteet ratkaistaisiin yleisten lainkonkurrenssia koskevien periaatteiden mukaisesti. Tietojärjestelmän häirintä olisi erityissäännön asemassa suhteessa datavahingontekoon (RL 35 luvun uusi 3 a §), jos dataa vahingoittamalla esimerkiksi estetään tietojärjestelmän toiminta tai aiheutetaan sille vakavaa häiriötä. Datavahingonteon soveltamismahdollisuuksien osalta tulee huomioida myös 35 luvun 5 §:ssä oleva yleinen rajoitussäännös.

Mikäli henkilön toiminta täyttäisi viestintäsalaisuuden loukkauksen ohella esimerkiksi luvattoman käytön, datavahingonteon, tietojärjestelmän häirinnän tai tietoliikenteen häirinnän tunnusmerkistön, on näistä rikoksista tuomitseminen mahdollista myös viestintäsalaisuuden loukkauksen ohella, sillä niiden suojeluobjektin voi katsoa olevan eri kuin viestintäsalaisuuden loukkauksessa.

Luvaton käyttö voi sisältää vähäisen määrän datan vahingoittamista, jolloin datavahingonteon ei vielä voi katsoa täyttyvän.

Ehdotetussa identiteettivarkautta koskevassa kriminalisoinnissa kyseeseen voi tulla oikeushenkilön yksilöivien tietojen oikeudeton käyttö. Tähän liittyen voidaan todeta, että esimerkiksi eräiden immateriaalioikeusrikosten ja identiteettivarkauden suhde ratkaistaan myös tavanomaisten konkurrenssia koskevien periaatteiden mukaisesti. Esimerkiksi rikoslain 49 luvun 2 §:ssä tarkoitetussa tilanteessa esimerkiksi tavaramerkkiä saatetaan käyttää pykälässä tarkoitetuin tavoin tavaramerkkilain vastaisesti. Tavaramerkkilain (7/1964) mukaisesti oleellista on kuitenkin, että tavaramerkkiä käytettään oikeudettomasti elinkeinotoiminnassa. Mikäli tilanteessa olisi kyse elinkeinotoiminnassa oikeudettomasti käytettävästä yksilöivästä tiedosta eli tavaramerkistä, voi esimerkiksi rikoslain 49 luvun 2 §:ssä tarkoitettu teollisoikeusrikos olla erityissäännön asemassa. Näin ollen vain se tulisi sovellettavaksi. Mikäli oikeushenkilön yksilöivää tietoa käytettäisiin esimerkiksi muualla kuin elinkeinotoiminnassa, voi sovellettavaksi puolestaan tulla ehdotettu identiteettivarkautta koskeva säännös

Edellä kuvatuista syistä ehdottomien konkurrenssisääntöjen kuvaaminen ei ole mahdollista, ja tilanteet tulee ratkaista kunkin yksittäistapauksen olosuhteet huomioiden yleisten lainkonkurrenssia koskevien periaatteiden mukaisesti.

4 artikla. *Laiton järjestelmän häirintä.* Artiklan mukaan 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. Artikla vastaa asiallisesti puitepäätöksen vastaavaa artiklaa. Puitepäätöksessä käytetään ”vakavan” estämisen ja keskeyttämisen sijasta muotoilua ”törkeä” estäminen tai keskeyttäminen. Muotoiluilla ei ole kuitenkaan asiallista eroa ja englanninkielisissä versioissa käytetäänkin samaa käsitettä ”serious”. Yleissopimus sisältää asiasisällöltään vastaavan artiklan. Se eroaa direktiivin ja puitepäätöksen artikloista ainoastaan siinä, että se ei sisällä vähäisiä tapauksia koskevaa nimenomaista poikkeussäännöstä. Muilta osin artiklojen vaatimukset ovat asiallisesti samat. Yleissopimus ei myöskään sisällä muotoilua ”tai saattamalla data käyttökelvottomaksi” toisin kuin direktiivi ja puitepäätös, mutta tällä ei ole Suomen kannalta merkitystä, sillä kansallinen lainsäädäntömme kattaa myös nämä tilanteet muotoilulla ”taikka muulla niihin rinnastettavalla tavalla”.

Hallituksen esityksestä 153/2006 vp ilmenevin tavoin ennen yleissopimuksen ja puitepäätöksen edellyttämiä lainsäädäntömuutoksia artiklassa tarkoitettua laitonta järjestelmän häirintää vastaavat Suomessa voimassa

olleet säännökset sisältyivät lähinnä tietoliikenteen häirintää koskevaan rikoslain 38 luvun 5 §:ään. Kyseisen säännöksen soveltamisala rajautui kuitenkin ainoastaan viestintään eli viestien siirtämiseen paikasta toiseen. Tämän vuoksi yleissopimuksen ja puitepäätöksen velvoitteiden täyttämiseksi rikoslain 38 luvun 7 a §:ään lisättiin tietojärjestelmän häirintää koskeva uusi kriminalisointi. Sitä ja vastaavia artikloita koskevat perustelut sisältyvät hallituksen esitykseen 153/2006 vp. Mainitun pykälän mukaan se, joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Mainitussa 7 a §:ssä ei tekotapoina mainita erikseen tuhoamista ja turmelemista, kuten yleissopimuksessa, puitepäätöksessä ja direktiivissä, mutta kansallisen lainsäädäntömme avoin tekotapaluettelo ”taikka muulla niihin rinnastettavalla tavalla” kattaa myös nämä tekotavat.

Pykälän 2 momentin mukaan yritys on rangaistava. Rikoslain 38 luvun 7 b § sisältää törkeän tietojärjestelmän häirinnän tunnusmerkistön.

Artikla ei edellytä lainsäädännön muuttamista.

Eri rikosten välisistä konkurrenssitilanteista johtuen tietojärjestelmän häirinnän toissijaisuuslauseke ehdotetaan kuitenkin kumottavaksi. Muussa tapauksessa saatettaisiin direktiivin edellyttämien rangaistusasteikkomuutosten myötä päätyä epätarkoituksenmukaisiin soveltamistilanteisiin. Toissijaisuuslausekkeen poiston tarve liittyy muun muassa siihen, että datavahingonteon (RL 35 luvun 3 a §) enimmäisrangaistus olisi jatkossa sama kuin tietojärjestelmän häirinnässä.

5 artikla. *Laiton datan vahingoittaminen.* Artiklan mukaan 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. Artikla vastaa asiasisällöllisesti puitepäätöksen vastaavaa artiklaa. Artikla vastaa asiasisällöllisesti myös yleissopimuksen vastaavaa artiklaa, joskin yleissopimuksessa mainitaan tekotapana myös tuhoaminen. Toisaalta yleissopimuksessa ei mainita erikseen tekotapana käyttökelvottomaksi saattamista. Kyseessä ovat kuitenkin vain erilaiset ilmaisut ja tekotapojen voidaan katsoa kattavan samat tilanteet. Yleissopimuksen artikla eroaa asiallisesti direktiivin ja puitepäätöksen artiklasta ainoastaan siinä, että yleissopimuksessa ei ole vähäisiä tapauksia koskevaa nimenomaista poikkeussäännöstä. Erolla ei ole Suomen kannalta käytännön merkitystä.

Artiklassa tarkoitettujen tilanteiden suhdetta Suomen lainsäädäntöön on selostettu laajemmin puitepäätöstä ja yleissopimuksen voimaansaattamista koskevassa hallituksen esityksessä (HE 153/2006 vp). Suomessa voimassa olevat säännökset tässä tarkoitettua datan vahingoittamista vastaavasta rikoksesta sisältyvät rikoslain vahingontekoa koskevaan 35 luvun 1 §:ään. Pykälän 2 momentin mukaan vahingonteosta on tuomittava se, joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen. Vaikka säännöksen tekotapaluettelo ei sanamuodoltaan vastaa artiklassa olevaa luetteloa, on sääntelyn piirin todettu edellä mainitussa hallituksen esityksessä olevan kuitenkin sama. Turmelemisella tarkoitetaan säännöksessä datan muuttamista sisällöltään toiseksi taikka täysin epäymmärrettävään tai käyttökelvottomaan muotoon. Säännös kattaa siten kaiken sellaisen dataan kajoamisen, jonka seurauksena tallennusalustalla oleva data joko muuttuu tai häviää.

Koska pykälän 2 momentin tekotapaluettelo on kuitenkin tyhjentävä, esityksessä ehdotetaan, että momentissa tarkoitettuun tekotapaluetteloon lisätään tekotavoiksi vahingoittaminen, muuttaminen ja käyttökelvottomaksi saattaminen, sillä mainitut tekotavat eivät välttämättä sisällöllisesti täysin kata nyt momentissa olevia tekotapoja joskin ne koskevat osin samoja tilanteita.

Artiklan sanamuodon mukaan vahingoittamisen kohde on tietojärjestelmässä oleva data. Vahingontekoa koskevassa rikoslain 35 luvun 1 pykälän 2 momentissa käytetään kuitenkin rajoittuneempaa muotoilua tietovälineelle tallennettu tieto tai muu tallennus. Tietojärjestelmässä oleva data voi kuitenkin olla muussakin muodossa kuin pysyväisluonteisesti tallennettuna. Se voi olla esimerkiksi tietojärjestelmän sisällä siirrettävänä. Tämän vuoksi ja direktiivin velvoitteiden täyttämiseksi esityksessä ehdotetaan, että 2 momentissa tarkoitettuun tekotapaluetteloon lisättäisiin vahingoittamisen kohteeksi tietojärjestelmässä oleva data.

Koska 2 momentissa tarkoitettu datavahingonteko on käytännössä itsenäinen, perustekomuotoisesta 1 momentissa tarkoitetusta vahingonteosta erillinen rikos, esityksessä ehdotetaan, että 2 momentissa tarkoitettu datavahingonteko erotettaisiin itsenäiseksi pykäläkseen (uusi 3 a §). Tämä mahdollistaa myös selkeämmän kirjoitusasun ja sääntelyn liittyen rangaistusasteikkoihin ja törkeiden tekomuotojen kvalifiointiperusteisiin. Lisäksi datavahingonteon törkeä tekomuoto ehdotetaan erotettavaksi itsenäiseksi pykäläkseen (uusi 3 b §) samoin kuin datavahingonteon lievä tekomuoto (uusi 3 c §). Edellä mainitun johdosta vahingontekoa koskevan 35 luvun 1 §:n 2 ja 3 momentti ehdotetaan kumottavaksi.

Suomi ei ole tehnyt yleissopimuksen vastaavan artiklan 2 kohdan mahdollistamaa varaumaa, jonka mukaan rangaistavuuden edellytyksenä voi olla se, että yleissopimuksen artiklan 1 kohdassa tarkoitettu teko aiheuttaa huomattavaa vahinkoa.

6 artikla. *Viestintäsalaisuuden loukkaus (tietojen laiton hankkiminen).* Artiklan mukaan 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.

Yleissopimuksen vastaava säännös ei sisällä nimenomaista vähäisiä tapauksia koskevaa poikkeusta. Muuten määräykset ovat asiasisällöltään samanlaiset. Yleissopimus sallii lisäksi sopimuspuolen asettavan rangaistavuuden edellytykseksi sen, että rikos on tehty epärehellisin tarkoituksin tai että se liittyy sellaiseen tietojärjestelmään, joka on kytketty toiseen tietojärjestelmään. Suomi ei ole asettanut rangaistavuudelle artiklassa mainittuja lisäedellytyksiä.

Yleissopimuksen voimaansaattamista koskevassa hallituksen esityksessä (HE 153/2006 vp) on selostettu kattavasti tässä tarkoitetun määräyksen suhdetta Suomen lainsäädäntöön todeten voimassa olevien säännösten vastaavan artiklan velvoitteita. Suomessa voimassa olevat säännökset artiklassa tarkoitettua tekoa vastaavasta rikoksesta sisältyvät rikoslain viestintäsalaisuuden loukkausta koskevan 38 luvun 3 §:ään ja törkeän tekomuodon osalta 4 §:ään sekä luvun 8 §:n 2 momenttiin. Mainitun 3 §:n 1 momentin mukaan viestintäsalaisuuden loukkauksesta on tuomittava se, joka oikeudettomasti avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan-, tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta. Teon katsominen törkeäksi edellyttää 4 §:n mukaan erityisen luottamusaseman hyväksikäyttöä, erityistä suunnitelmallisuutta tai teon kohdistumista erityisen arkaluonteisiin tietoihin. Molempien tekomuotojen yritys on rangaistava.

Rikoslain 38 luvun 8 §:n 2 momenttia, joka koskee hajasäteilyn sieppaamista, on selostettu 3 artiklan yhteydessä.

Yleissopimuksen voimaansaattamista koskevassa hallituksen esityksessä todetaan, että yleissopimuksen selitysmuistion mukaan yleissopimuksen vastaavan artiklan tarkoituksena on turvata yksityisyyden suojaa missä tahansa sähköisessä viestinnässä sen teknisestä toteuttamistavasta riippumatta. Artiklan soveltamisalaan kuuluvat ainoastaan teknisellä keinolla tapahtuvat teot. Teknisellä

keinolla viitataan laitteiden ja ohjelmien lisäksi myös salasanan käyttämiseen. Luottamuksellinen datan siirto tarkoittaa kohdeviestintänä tapahtuvaa viestintää. Ratkaisevaa ei ole kuitenkaan käytetyn viestintävälineen luonne vaan itse viestin luottamuksellisuus. Tämän vuoksi myös joukkoviestintävälineessä välitetty luottamuksellinen viesti voi kuulua artiklan soveltamisalaan. Viestintä voi olla tietokoneiden välistä, yhden tietokoneen eri osien välistä ja myös käyttäjän ja tietokoneen välistä. Viestintä voi tapahtua myös radioaaltojen välityksellä. Artikla kattaa myös niin sanottua hajasäteilyä sieppaamalla tapahtuvat teot. Artiklassa edellytetään, että rangaistavaksi säädettävä teko tapahtuu oikeudettomasti. Teon oikeutus voi perustua esimerkiksi toisen osapuolen suostumukseen tai viranomaisen oikeuteen tutkia rikoksia. Artikla ei koske internetissä käytettävien evästeiden käyttöä käyttäjien seurantaan.

Hallituksen esityksen (HE 153/2006 vp) mukaan rikoslain viestintäsalaisuuden loukkausta koskevan säännöksen soveltamisala on laaja. Säännös kattaa datan muodossa olevien viestien lisäksi myös muut viestit niiden muodosta riippumatta. Datan muodossa olevan viestin pitää kuitenkin olla ulkopuoliselta suljettu tai televerkossa välitettävänä. Siten esimerkiksi sähköpostiviestin saama suoja perustuu säännöksen eri kohtiin viestin sijaintipaikasta riippuen. Sähköpostiviesti saa televerkossa välitettävän viestin suojaa silloin, kun se on televerkossa ja ulkopuolisilta suojatun viestin suojaa silloin, kun se on osapuolen hallinnassa esimerkiksi tietokoneeseen tallennettuna.

Saman hallituksen esityksen mukaan televerkolla tarkoitetaan säännöksessä yleisen televerkon lisäksi myös esimerkiksi yrityksen sisäistä televerkkoa. Televiestillä tarkoitetaan mitä hyvänsä viestiä, joka on säännöksen esimerkkiluettelossa mainitun kaltainen. Vastaavuutta on lain esitöiden mukaan (HE 94/1993 vp) tarkasteltava erityisesti viestin yksityisyyttä silmällä pitäen. Esimerkiksi televerkossa välitettävää joukkoviestintää säännös ei koske. Säännös suojaa viestin sisällön lisäksi myös tietoa viestin lähettämisestä ja vastaanottamisesta. Rangaistavaa on siten esimerkiksi hankkia tieto siitä, mihin numeroon tietystä puhelimesta on soitettu.

Hallituksen esityksen (HE 153/2006 vp) mukaan säännös suojaa myös sellaista viestiä, joka sitä mihinkään siirtämättä tallennetaan tietokoneeseen tietyn henkilöpiirin luettavaksi. Rangaistavuuden edellytyksenä on kuitenkin se, että viesti on teknisin keinoin suojattu ulkopuolisilta ja että tiedon hankkiminen viestistä tapahtuu tämä suojaus murtaen. Hallituksen esityksessä viitataan lain esitöihin (HE 94/1993 vp) todeten, että suojauksen murtaminen voi tapahtua samalla tavalla kuin tietomurron osalta.

Edelleen samassa esityksessä todetaan, että teon tulee tapahtua oikeudettomasti. Teon oikeutus voi perustua esimerkiksi toisen osapuolen suostumukseen tai viranomaisen oikeuteen tutkia rikoksia. Esityksessä viitataan myös rikoslain 38 luvun 8 §:n 2 momenttiin, jonka todetaan koskevan hajasäteilyn sieppaamista. Johtopäätöksenä esityksessä todetaan, että voimassa olevat säännökset vastaavat tältä osin artiklan velvoitteita.

Edellä mainitussa hallituksen esityksessä todetusta huolimatta tuli työryhmä siihen tulokseen, että mainitut rikoslain säännökset eivät täysin kata yleissopimuksen, tai nyt direktiivin, tavoitteita ja soveltamisalaa. Ensinnäkin artiklassa edellytetään, että viestintäsalaisuuden loukkaus tehdään teknisin keinoin. Sallittua olisi luonnollisesti säätää teko rangaistavaksi ilman mainittua edellytystä. Rikoslain 38 luvun 3 §:n 1 momentin 1 kohdassa edellytetään kuitenkin suojauksen murtamista. Tämä on rajoittavampi kriteeri kuin ”teknisin keinoin”. Teknisillä keinoilla viitataan yleissopimuksen selitysmuistiossa laitteiden, ohjelmien ja esimerkiksi salasanan käyttämiseen. Kuten edellä on todettu yleissopimuksen voimaansaattamisen yhteydessä esitöissä todettiin suojauksen murtamisen voivan lain esitöiden (HE 94/1993 vp) tapahtua vastaavalla tavalla kuin tietomurron (8 §) osalta. Lisäksi on huomattava, että hajasäteilyä koskeva 8 §:n 2 momentti jo itsessään täyttää artiklassa olevan velvoitteen hajasäteilyn hyväksikäytön osalta. Viestintäsalaisuuden loukkausta koskevan 3 §:n osalta on jossain määrin epäselvää, kattaako se kaikki ”teknisin keinoin” tapahtuvat tilanteet, joita artiklassa on tarkoitettu. Käytännössä on esiintynyt epäselvyyttä siitä, kattaako nykyinen 38 luvun 3 § tilanteet, joissa

tietoa hankitaan silloin, kun data ei ole vielä televerkossa välitettävänä eikä myöskään tallennettuna ja tiedon hankkiminen tapahtuu esimerkiksi haittaohjelman avulla, jonka käyttäjä on tietämättään tai harhaanjohdettuna itse asentanut koneeseensa taikka asentaminen on tapahtunut muuten vilpillisesti. Tällöin tietojärjestelmään ei välttämättä ole tunkeuduttu myöskään tietomurtosäännöksen tarkoittamassa mielessä.

Edellisessä kappaleessa mainitut seikat rikoslain 38 luvun 3 pykälän 1 momentin 1 kohdan ja tallennetun tiedon osalta eivät kuitenkaan ole erityisen merkityksellisiä direktiivin edellyttämien velvoitteiden kannalta, sillä artiklan velvoitteet koskevat tiedon hankkimista tietojärjestelmien välisestä tai sisäisestä datan siirrosta. Kyseessä ei siten ole lähtökohtaisesti tallennettu tieto vaan tiedon hankkiminen silloin kun luottamuksellinen data on siirrettävänä. Direktiivin englanninkielinen teksti tuo selkeämmin esiin tämän edellytyksen. Siinä käytetään muotoilua ”intercepting non-public transmission of computer data”.

Artiklan velvoitteet koskevat sekä tietojärjestelmien välistä että tietojärjestelmän sisäistä viestintää. Edellä esiin nostetut tulkinnanvaraisuudet eivät koske tilanteita, joissa on kyse tietojärjestelmien välisestä datan siirrosta. Tällöin tieto on välitettävänä televerkossa, joten viestintäsalaisuuden loukkausta koskeva 38 luvun 3 §:n 1 momentin 2 kohta tulee sovellettavaksi. Kyseinen 2 kohta ei sisällä mitään lisäkriteereitä sen lisäksi, että tieto datasiirron sisällöstä tai sellaisen lähettämisestä tai vastaanottamisesta on hankittu. Epäselvyydet koskevatkin tietojärjestelmän sisäistä datan siirtoa. Luvun 3 §:n 1 momentin 1 kohta ei nimenomaisesti koske tietojärjestelmän sisäistä datan siirtoa, esimerkiksi käyttäjän (näppäimistö) ja tietojärjestelmän välistä tai tietojärjestelmän eri osien välistä viestintää. Mainittu 1 kohta koskee nimenomaisesti vain tallennettua viestiä, jota artiklan velvoitteiden ei voi katsoa koskevan.

Edellä mainittujen epäselvyyksien poistamiseksi esityksessä ehdotetaan viestintäsalaisuuden loukkausta koskevan 3 §:n 1 momentin 2 kohdan laajentamista koskemaan televerkossa välitettävänä olevan datasiirron lisäksi myös tietojärjestelmän sisäistä datasiirtoa yleissopimuksen ja direktiivin sanamuodon edellyttämällä tavalla. Muutettavan rikoslain 38 luvun 3 §:n 1 momentin 2 kohdan mukaan viestintäsalaisuuden loukkauksesta tuomittaisiin myös se, joka oikeudettomasti hankkii tiedon televerkossa *tai tietojärjestelmässä* välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan-, tai datasiirron tai muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta. Datasiirtoa ja muuta välitettävänä olevaa luottamuksellista viestintää on perusteltua suojata samanlaisesti riippumatta siitä missä kohtaa viestinvälitysketjua kulloinkin tapahtuvasta viestintäsalaisuuden loukkauksesta on kyse. Muutos on perusteltu myös sen vuoksi, että esimerkiksi monet verkkopankkien käyttöön kohdistuvat rikokset tehdään nykyisin kohdistamalla toimet verkkopankkiasiakkaan henkilökohtaisen tietokoneen eli tietojärjestelmän sisäiseen viestintään. Tälle kehityssuunnalle saattaa olla eräänä syynä se, että itse televerkot ja pankkien tietojärjestelmät ovat nykyisin niin hyvin suojatut, että haavoittuvin kohde löytyy asiakaspäästä.

Luottamuksellinen datasiirto voi pykälän 1 momentin 2 kohdassa tarkoitetussa merkityksessä sisältää myös esimerkiksi henkilön hallinnoiman telepäätelaitteen lähettämää tietoa laitteen sijainnista, mikäli data on säännöksessä tarkoitetuin tavoin välitettävänä.

Mainittujen muutosten jälkeen Suomen lainsäädäntö vastaisi artiklan vaatimuksia.

7 artikla. *Rikosten tekemiseen käytettävät välineet.* Artiklan mukaan jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että artiklan kohdissa mainittujen 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. Mainitut välineet ovat artiklan alakohtien mukaan a) tietokoneohjelma, joka on suunniteltu tai muunnettu ensisijaisesti 3—6 artiklassa tarkoitettujen rikosten tekemistä varten ja b) tietojärjestelmän salasana, pääsykoodi tai muu vastaava tieto, joka mahdollistaa pääsyn tietojärjestelmään tai sen osaan.

Yleissopimuksen 6 artiklan 1 kappaleen a kohta sisältää määräykset samasta kysymyksestä. Asiallisena erona on se, että direktiivin säännös ei kata muita välineitä kuin tietokoneohjelmat ja tiedon. Direktiivissä ei siis ole niin sanottuun ”hardwareen” viittaavaa ”välineitä” (device) koskevaa mainintaa, toisin kuin yleissopimuksen 6 artiklan 1 kappaleen a kohdan i alakohdassa. Yleissopimus kuitenkin sallii varauman tekemisen kyseisen artiklan 1 kappaleeseen edellyttäen kuitenkin, että varauma ei koske artiklan 1 kappaleen a kohdan ii alakohdassa tarkoitettujen tuotteiden myyntiä, levittämistä tai muuta saataville asettamista. Kyseinen ii alakohta sisältää samat ”välineet” kuin direktiivin artiklan b kohta eli tietojärjestelmän salasanan, pääsykoodin tai muun vastaavan tiedon. Suomi ei ole tehnyt tässä tarkoitettua varaumaa. Yleissopimus sisältää lisäksi määräyksiä hallussapidon kriminalisoinnista sekä selvyyden vuoksi rikosvastuun poissuljennasta silloin, kun tarkoituksena on tietojärjestelmän luvallinen testaus tai suojelu.

Tässä tarkoitettua säännöstä on selostettu kattavasti yleissopimuksen voimaansaattamista koskevassa hallituksen esityksessä (HE 153/2006 vp). Yleissopimuksen voimaansaattamisen yhteydessä rikoslain 34 luvun 9 a §:ää muutettiin vastaamaan yleissopimuksen vaatimuksia. Suomen voimassaolevassa lainsäädännössä direktiivissä tarkoitettuja tilanteita vastaa rikoslain 34 luvun 9 a §:ssä tarkoitettu vaaran aiheuttaminen tietojenkäsittelylle. Säännöksen mukaan tuomitaan se, joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle 1) tuo maahan, valmistaa, myy tai muuten levittää taikka asettaa saataville a) sellaisen laitteen tai tietokoneohjelman taikka ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa taikka murtamaan tai purkamaan sähköisen viestinnän teknisen suojauksen tai tietojärjestelmän suojauksen taikka b) tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon taikka 2) levittää tai asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseksi. Edellä mainitun 9 a §:n tekotavoista puuttuu direktiivin artiklassa mainittu ”käyttöön hankkiminen”. Tietoverkkorikosvälineen hallussapidosta säädetään rikoslain 34 luvun 9 b §:ssä. Yleissopimuksen voimaansaattamista koskevassa hallituksen esityksessä (HE 153/2006 vp) todetaan 9 b §:n kattavan artiklan velvoitteet siltä osin kuin siinä on kyse tietoverkkorikosvälineen hankinnasta siten, että välinettä ei samalla levitetä tai aseteta saataville. Käytännössä hallussa pitämisen rangaistavuus kattaa myös hankkimisen, koska hankkimisen seurauksena väline päätyy aina myös hankinnan suorittaneen henkilön haltuun.

Direktiivi edellyttää kuitenkin myös ”käyttöön hankkimisen” osalta kahden vuoden enimmäisrangaistusta. Tietoverkkorikosvälineen hallussapidon eli rikoslain 34 luvun 9 b §:ssä tarkoitetun teon enimmäisrangaistus on kuusi kuukautta vankeutta. Pelkän tietoverkkorikosvälineen hallussapidon ei kuitenkaan voi katsoa olevan yhtä moitittava rikos kuin 9 a §:ssä tarkoitettu vaaran aiheuttaminen tietojenkäsittelylle. Näin ollen 9 b §:n enimmäisrangaistuksen nostaminen kahteen vuoteen vankeutta ei olisi perusteltua. Käyttöön hankkimisen voidaan katsoa myös olevan moitittavampaa kuin pelkkä hallussapito eikä se tarkoita samaa asiaa vaikkakin hankkimisen seurauksena väline päätyy hankkijan haltuun. Haittaamis- tai vahingoittamistarkoitusta varten hankkiminen edellyttää aktiivisia toimia välineen haltuun saamiseksi toisin kuin pelkkä hallussapito, jonka osalta tunnusmerkistö voi täyttyä jo sen perusteella, että henkilöllä yksinkertaisesti on väline hallussaan edellyttäen, että säännöksen muut kriteerit kuten haittaamis- tai vahingoittamistarkoitus täyttyvät. Käyttöön hankkiminen puolestaan voi edellyttää muun muassa aktiivista etsimistä, tiedon hankkimista ja sen johdosta esimerkiksi välineen tilaamista internetistä. Oleellista on siten aktiivinen toiminta välineen hankkimiseksi käytettäväksi haittaamis- tai vahingoittamistarkoituksissa.

Rikoslain 34 luvun 9 a ja 9 b § eivät nykyisellään täysin vastaa direktiivin vaatimuksia ”käyttöön hankkimisen” osalta. Edellä mainitun vuoksi esityksessä ehdotetaan, että luvun 9 a §:n 1 momentin 1 kohtaan lisätään tekotavaksi myös ”käyttöön hankkiminen”. Tun-

nusmerkistö käyttöön hankkimisen osalta täyttyisi vasta silloin, kun väline on saatu haltuun. Ehdotetun muutoksen jälkeen lainsäädäntö vastaa direktiivin velvoitteita. Käyttöön hankkimisen kriminalisointi koskisi direktiivin edellyttämin tavoin myös tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon käyttöön hankkimista mikäli muut rangaistavuuden edellytykset kuten erityinen haittaamis- tai vahingoittamistarkoitus täyttyisivät.

Niin sanottuja bottiverkkoja koskevat velvoitteet liittyvät direktiivissä jäljempänä 9 artiklan yhteydessä selostetuin tavoin 4 ja 5 artiklassa tarkoitettujen tekojen ankaroittamisperusteisiin. On syytä kuitenkin todeta, että bottiverkko voi olla myös 34 luvun 9 a ja 9 b §:ssä tarkoitettu laite tai tietokoneohjelma.

8 artikla. *Yllytys, avunanto ja yritys.* Artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että yllytys tai avunanto 3—7 artiklassa tarkoitettuihin rikoksiin on rikosoikeudellisesti rangaistava teko. Vastaavanlainen yllytystä ja avunantoa koskeva määräys sisältyy myös yleissopimukseen ja puitepäätökseen. Suomessa säännökset avunannon ja yllytyksen rangaistavuudesta sisältyvät rikoslain 5 luvun 5 ja 6 §:ään. Yllyttäjä rinnastetaan rangaistusvastuussa tekijään. Avunantaja tuomitaan lievennetyn asteikon perusteella.

Voimassaolevat säännökset vastaavat tältä osin artiklan velvoitteita. Artikla ei edellytä lainsäädännön muuttamista.

Artiklan 2 kohdan mukaan jäsenvaltioiden on varmistettava, että 4 ja 5 artiklassa tarkoitettujen rikosten yritys on rikosoikeudellisesti rangaistava teko. Kyseiset 4 ja 5 artiklat koskevat laitonta järjestelmän häirintää ja laitonta datan vahingoittamista. Puitepäätös ja yleissopimus sisältävät myös yrityksen rangaistavuutta koskevat artiklat. Puitepäätöksen velvoitteet yrityksen rangaistavuuden osalta ovat tosin laajemmat, sillä puitepäätös edellyttää yrityksen rangaistavuutta myös laitonta tunkeutumista tietojärjestelmään koskevan artiklan osalta. Myös yleissopimuksen velvoitteet ovat direktiivin velvoitteita laajemmat, sillä yleissopimuksen velvoitteet yrityksen kriminalisoinnista kattavat myös viestintäsalaisuuden loukkausta koskevan artiklan. Yleissopimus toisaalta sallii varauman tekemisen yrityksen rangaistavuutta koskeviin velvoitteisiin.

Direktiivin 4 artiklaa vastaavat rikoslain säännökset ovat rikoslain 38 luvun 5 §:ssä tarkoitettu tietoliikenteen häirintä, 6 §:ssä tarkoitettu törkeä tietoliikenteen häirintä, 7 §:ssä tarkoitettu lievä tietoliikenteen häirintä, 7 a §:ssä tarkoitettu tietojärjestelmän häirintä ja 7 b §:ssä tarkoitettu törkeä tietojärjestelmän häirintä. Kaikkien edellä mainittujen yritys on rangaistava.

Direktiivin 5 artiklaa vastaava rikoslain säännös on 35 luvun 1 §:n 2 momentissa tarkoitettu vahingonteko, jonka yritys on rangaistava. Myös 35 luvun 2 §:ssä tarkoitetun törkeän vahingonteon yritys on rangaistava. Edellä esitetyin tavoin esityksessä ehdotetaan datavahingontekoa koskevien säännösten erottamista itsenäisiksi pykälikseen. Uudet ehdotetut datavahingontekoa (3 a §) ja törkeää datavahingontekoa (3 b §) koskevat säännökset vastaisivat tältä osin edellä mainittuja sisältäen yrityksen rangaistavuuden. Rikoslain 35 luvun 3 §:ssä tarkoitetun lievän vahingonteon yritys ei ole rangaistava. Myöskään uuden ehdotetun lievää datavahingontekoa koskevan 3 c §:n yritys ei olisi rangaistava. Direktiivin 5 artiklan mukaiset velvoitteet eivät kuitenkaan koske vähäisiä tapauksia, joten yrityksen rangaistavuutta ei ole tarpeen ulottaa lievään datavahingontekoon. Vastaavanlainen ratkaisu on omaksuttu puitepäätöksen osalta, jonka laitonta datan vahingoittamista koskeva artikla ei sisällä vähäisiä tapauksia koskevia velvoitteita. Yleissopimuksen voimaansaattamisen yhteydessä Suomi on myös tehnyt varauman, jonka mukaan se ei sovella yrityksen kriminalisointiin liittyvää velvoitetta lievään vahingontekoon.

Artikla ei edellytä lainsäädännön muuttamista muilta osin kuin yrityksen rangaistavuuden sisällyttämistä uuteen ehdotettuun datavahingontekoon (38 luvun 3 a §) ja törkeään datavahingontekoon (38 luvun 3 b §).

9 artikla. *Seuraamukset.* Artiklan 1 kohdan mukaan jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 3—8 artiklassa tarkoitetuista rikoksista voidaan määrätä tehokkaat, oikeasuhtaiset ja varoittavat seuraamukset. Artiklan 1 kohta on standardimuotoinen seuraamussäännös eikä

edellytä tiettyjen erityisten rangaistustasojen säätämistä. Käytännössä se kuitenkin kohdistuu vain 8 artiklaan eli yllytyksen, avunannon ja yrityksen rangaistavuuteen, sillä 3—7 artikloiden osalta edellytetään jäljempänä esitetyin tavoin tiettyjä enimmäisrangaistusten vähimmäistasoja.

Perustekomuodot

Artiklan 2 kohdan mukaan 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. Vähäisiä tapauksia koskeva rajaus on tässä lähinnä informatiivinen lisäys, sillä sama vähäisiä tapauksia koskeva rajaus mainitaan itsenäisesti kaikissa tässä tarkoitetuissa artikloissa (3—7 artiklat). Näin ollen vähimmäistasoa koskeva edellytys kohdistuu artikloihin 3—7 kokonaisuudessaan.

Edellä 3 artiklan yhteydessä todetuin tavoin 3 artiklassa tarkoitettua tekoa vastaa Suomessa rikoslain 38 luvun 8 §:ssä tarkoitettu tietomurto. Tietomurron enimmäisrangaistus on enintään yksi vuosi vankeutta. Näin ollen tietomurron rangaistustaso joudutaan korottamaan kahteen vuoteen vankeutta. Tietomurron perustekomuodon rangaistustason nostamisella kahteen vuoteen on merkitystä myös rikoslain 38 luvun 8 a §:ssä tarkoitetun törkeän tietomurron osalta. Nykyisin törkeän tietomurron enimmäisrangaistus on kaksi vuotta vankeutta. Jotta perustekomuodon ja törkeän tekomuodon enimmäisrangaistukset eivät olisi identtiset, esityksessä ehdotetaan törkeän tietomurron rangaistustason nostamista kolmeen vuoteen vankeutta. Tietomurron törkeän tekomuodon enimmäisrangaistuksen korottaminen on edellä mainitun lisäksi perusteltua sen vuoksi, että tietoverkkorikoksien vakavuuteen suhtauduttaisiin johdonmukaisesti samalla tavalla kuin muihin direktiivissä tarkoitettuihin rikostyyppeihin. Direktiivin 9 artiklan 2 kohta edellyttää siten lainsäädännön muuttamista tietomurtoa koskevien säännösten osalta.

Edellä 4 artiklan yhteydessä todetuin tavoin 4 artiklassa tarkoitettua tekoa vastaavat säännökset sisältyvät rikoslain 38 luvun 5 §:ssä tarkoitettuun tietoliikenteen häirintään ja 38 luvun 7 a §:ssä tarkoitettuun tietojärjestelmän häirintään. Kyseisten tekojen enimmäisrangaistus on jo nykyisin kaksi vuotta vankeutta, joten 9 artiklan 2 kohdan edellyttämä enimmäisrangaistustaso täyttyy. Direktiivin 9 artiklan 2 kohta ei siten edellytä lainsäädännön muuttamista tietoliikenteen häirinnän ja tietojärjestelmän häirinnän osalta.

Edellä 5 artiklan yhteydessä todetuin tavoin 5 artiklassa tarkoitettua tekoa vastaavat säännökset sisältyvät vahingontekoa koskevaan rikoslain 35 luvun 1 §:n 2 momenttiin (datavahingonteko). Vahingonteon enimmäisrangaistus on yksi vuosi vankeutta. Direktiivin vaatimusten täyttämiseksi datavahingonteon enimmäisrangaistusta olisi lähtökohtaisesti nostettava kahteen vuoteen vankeutta. Vahingontekokriminalisoinnin 1 momentissa tarkoitettu yleinen tekomuoto kattaa kuitenkin niin laajan joukon tilanteita, että ei ole tarkoituksenmukaista korottaa rangaistustasoa laajemmin kuin direktiivi edellyttää. Datavahingonteko ilmentää monissa tapauksissa suurempaa tahallisuutta eli edellyttää usein tietynasteista suunnitelmallisuutta. Tämän vuoksi on perusteltua, että datavahingon osalta on käytettävissä korkeampi enimmäisrangaistus kuin perustekomuotoisessa vahingonteossa. Kahden vuoden enimmäisrangaistuksen tulisi näin ollen koskea vain 2 momentissa tarkoitettuja datavahingontekoja. Datavahingonteko ehdotetaan edellä kuvatulla tavalla erotettavaksi omaksi itsenäiseksi pykäläkseen muun muassa kirjoitusteknisen selkeyden vuoksi. Mainitun erottamisen johdosta perustekomuotoisen rikoslain 35 luvun 1 §:ssä tarkoitetun vahingonteon rangaistusasteikkoa ei ole tarpeen korottaa kahteen vuoteen vankeutta, vaan riittävää on, että uuden 3 a §:ssä ehdotetun datavahingonteon enimmäisrangaistus on kaksi vuotta vankeutta.

Vahingontekoa vastaavasti myös uuden datavahingonteon osalta ehdotetaan uutta lievää tekomuotoa eli lievää datavahingontekoa (3 c §), jonka enimmäisrangaistus olisi lievää vahingontekoa vastaavasti sakkoa. Lievän tekomuodon säätäminen myös uuden ehdotetun datavahingonteon osalta on perusteltua, jotta suhteellisen ankarasti rangaistavaa data-

vahingonteon perusmuotoa ei olisi tarvetta soveltaa kaikkein lievimpiin tapauksiin. Direktiivin velvoitteet eivät koske vähäisiä tapauksia, joten lievän datavahingonteon enimmäisrangaistus voidaan päättää kansallisesti.

Direktiivin 9 artiklan 2 kohta edellyttää siten lainsäädännön muuttamista vahingonteon osalta.

Edellä 6 artiklan yhteydessä todetuin tavoin 6 artiklassa tarkoitettua tekoa vastaavat säännökset sisältyvät viestintäsalaisuuden loukkausta koskevaan rikoslain 38 luvun 3 §:ään ja tietomurtoa koskevaan 8 §:n 2 momenttiin. Viestintäsalaisuuden loukkauksen enimmäisrangaistus on nykyisin yksi vuosi vankeutta. Edellä todetuin tavoin nykyisin myös tietomurron enimmäisrangaistus on yksi vuosi vankeutta. Direktiivin 9 artiklan 2 kohdan vaatimusten täyttämiseksi tietomurron enimmäisrangaistuksen lisäksi myös viestintäsalaisuuden loukkauksen enimmäisrangaistus joudutaan nostamaan kahteen vuoteen vankeutta.

Edellä 7 artiklan yhteydessä todetuin tavoin 7 artiklassa tarkoitettua tekoa vastaavat säännökset sisältyvät vaaran aiheuttamista tietojenkäsittelylle koskevaan rikoslain 34 luvun 9 a §:ään sekä ”käyttöön hankkimisen” osalta rikoslain 34 luvun 9 b §:ssä tarkoitettuun tietoverkkorikosvälineen hallussapitoon. Vaaran aiheuttamista tietojenkäsittelylle koskevan kriminalisoinnin enimmäisrangaistus on jo nykyisin kaksi vuotta vankeutta, joten sen osalta ei ole tarvetta korottaa enimmäisrangaistuksen tasoa. Tietoverkkorikosvälineen hallussapidon enimmäisrangaistus on kuusi kuukautta vankeutta. Esityksessä ehdotetaan kuitenkin ”käyttöön hankkimisen” sisällyttämistä vaaran aiheuttamista tietojenkäsittelylle koskevan kriminalisoinnin alaisuuteen. Näin ollen Direktiivin 9 artiklan 2 kohdan enimmäisrangaistuksen vähimmäistasoa koskevat vaatimukset eivät mainitun muutoksen myötä edellytä muutoksia lainsäädäntöön.

Kolmen vuoden enimmäisrangaistus

Artiklan 3 kohdan mukaan jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 4 ja 5 artiklassa tarkoitetuista rikoksista säädetään vankeusrangaistus, jonka enimmäiskesto on vähintään kolme vuotta vankeutta, 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.

Artiklan 3 kohdassa on kyse muun muassa tilanteista, joiden on tarkoitettu kattavan niin sanotut bottiverkkoja koskevat tilanteet. Direktiivin tavoitteena on ollut kattaa niin bottiverkkojen luominen kuin niiden käyttäminenkin, vaikka esimerkiksi bottiverkkoa hyödyntävä palvelunestohyökkäys kohdistuisikin vain yhteen kohteeseen. Mainitussa 3 kohdassa tarkoitetuissa 4 ja 5 artiklassa on edellä esitetyin tavoin kansallisessa lainsäädännössä kyse rikoslain 38 luvun 5 §:ssä tarkoitetusta tietoliikenteen häirinnästä ja 38 luvun 7 a §:ssä tarkoitetusta tietojärjestelmän häirinnästä sekä rikoslain 35 luvun 1 §:n 2 momentissa tarkoitetusta datavahingonteosta tai uudesta tässä esityksessä ehdotettavasta datavahingonteosta (3 a §). Direktiivin 7 artiklassa tarkoitetuilla välineillä puolestaan tarkoitetaan välineitä, joita tarkoitetaan rikoslain 34 luvun 9 a §:n 1 kohdassa.

Joiltain osin 3 kohdan mukaisissa tilanteissa voisi olla kyse törkeää tietojärjestelmän häirintää koskevan rikoslain 38 luvun 7 b §:n 1 momentin 2 kohdassa tarkoitetusta erityisen suunnitelmallisesti tehdystä rikoksesta. Tällaista erityistä suunnitelmallisuutta koskevaa kvalifiointiperustetta ei kuitenkaan sisälly luvun 6 §:ssä tarkoitettuun törkeään tietoliikenteen häirintään eikä 35 luvun 2 §:ssä tarkoitettuun törkeään vahingontekoon tai uuteen ehdotettavaan 35 luvun 3 b §:ssä tarkoitettuun törkeään datavahingontekoon. Tämän vuoksi ja koska törkeiden tekomuotojen kvalifiointiperusteita on lähtökohtaisesti tulkittava suppeasti, esityksessä ehdotetaan, että direktiivin vaatimusten täyttämiseksi rikoslain 38 luvun 6 §:ssä tarkoitettuun törkeään tietoliikenteen häirintään, rikoslain 38 luvun 7 b §:ssä tarkoitettuun törkeään tietojärjestelmän häirintään ja rikoslain 35 luvun uudessa 3 b §:ssä tarkoitettuun törkeään datavahingontekoon sisällytettäisiin uusi direktiivin 9 artiklan 3 kohtaa vastaava tekomuoto, joka kvalifioisi kyseiset teot törkeiksi. Teko voisi kvalifioitua törkeäksi, jos rikos

tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa.

Direktiivin 9 artiklan 3 kohdassa edellytetty kolmen vuoden enimmäisrangaistuksen vähimmäistasoa koskeva vaatimus ei edellytä kansallisen lainsäädännön rangaistustasojen nostamista, sillä edellä mainittujen nykyisin voimassa olevien rikosten törkeiden tekomuotojen enimmäisrangaistus on jo nykyisin Suomen lainsäädännössä neljä vuotta vankeutta. Törkeä datavahingonteko (38 luvun 3 b §) olisi uusi kriminalisointi, mutta myös törkeän vahingonteon enimmäisrangaistus on jo nykyisin neljä vuotta vankeutta. Jäljempänä tässä esityksessä selostetuista syistä johtuen kyseisten törkeiden tekomuotojen enimmäisrangaistuksia joudutaan kuitenkin korottamaan.

Viiden vuoden enimmäisrangaistus

Artiklan 4 kohdan mukaan 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.

Kohdassa tarkoitetuissa 4 ja 5 artiklassa on edellä esitetyin tavoin kansallisessa lainsäädännössä kyse rikoslain 38 luvun 5 §:ssä tarkoitetusta tietoliikenteen häirinnästä ja 38 luvun 7 a §:ssä tarkoitetusta tietojärjestelmän häirinnästä sekä rikoslain 35 luvun 1 §:n 2 momentissa tarkoitetusta datavahingonteosta tai jatkossa 3 a §:ssä tarkoitetusta datavahingonteosta. Kohdassa tarkoitetut tekotavat on nykyisin vain osittain katettu kansallisessa lainsäädännössä edellä mainittujen rikosten törkeissä tekomuodoissa eli rikoslain 38 luvun 6 §:ssä tarkoitetussa törkeässä tietoliikenteen häirinnässä, 38 luvun 7 b §:ssä tarkoitetussa törkeässä tietojärjestelmän häirinnässä ja 35 luvun 2 §:ssä tarkoitetussa törkeässä vahingonteossa. Direktiivin vaatimusten täyttämiseksi esityksessä ehdotetaan uusien 4 kohtaa vastaavien kvalifiointiperusteiden sisällyttämistä edellä mainittujen rikosten törkeisiin tekomuotoihin. Datavahingonteon osalta törkeä datavahingonteko erotettaisiin aiemmin esityksessä tarkoitetuin tavoin itsenäiseksi törkeästä vahingonteosta erilliseksi pykäläkseen (3 b §). Lisäksi mainittujen törkeiden tekomuotojen enimmäisrangaistus kansallisessa lainsäädännössä on nykyisin neljä vuotta vankeutta. Direktiivin vaatimusten täyttämiseksi mainittujen törkeiden tekomuotojen enimmäisrangaistukseksi ehdotetaan viittä vuotta vankeutta. Koska törkeä datavahingonteko erotettaisiin omaksi pykäläkseen, ei rikoslain 35 luvun 2 §:n törkeän vahingonteon enimmäisrangaistusta tarvitsisi nostaa.

Rikollisjärjestö

Rikoslain 35 luvun 2 §:n 1 momentin 2 kohta sisältää nykyisin asiasisällöltään direktiivin velvoitteita vastaavan, nimenomaan datavahingontekoon rajautuvan rikollisjärjestöä koskevan kvalifiointiperusteen. Kyseinen kvalifiointiperuste on sisällytetty säännökseen puitepäätöksen kansallisten täytäntöönpanotoimien yhteydessä. Törkeän datavahingonteon osalta a alakohta ei siten edellyttäisi lainsäädännön muuttamista muuten kuin enimmäisrangaistuksen osalta, joka olisi nostettava direktiivin edellyttämään viiteen vuoteen vankeutta. Esityksessä kuitenkin edellä mainituin tavoin ehdotetaan uutta törkeää datavahingontekoa koskevaa 3 b §:n säätämistä, joka sisältäisi 2 kohtaa vastaavan kvalifiointiperusteen. Uuden ehdotetun 3 b §:n enimmäisrangaistus olisi viisi vuotta vankeutta. Nykyisen 35 luvun 2 §:n 1 momentin 2 kohta tulisi vastaavasti kumottavaksi.

Rikoslain 38 luvun 6 §:ssä tarkoitettu törkeä tietoliikenteen häirintä ja 7 b §:ssä tarkoitettu törkeä tietojärjestelmän häirintä eivät sisällä vastaavaa rikollisjärjestöön liittyvää kvalifiointiperustetta. Direktiivin vaatimusten täyttämiseksi kyseisiin säännöksiin ehdotetaan lisättäväksi vastaava kvalifiointiperuste, joka nykyisin sisältyy törkeään datavahin-

gontekoon. Näin ollen teko voisi kvalifioitua törkeäksi, jos rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa. Lisäksi mainittujen rikosten enimmäisrangaistus ehdotetaan nostettavaksi viiteen vuoteen vankeutta.

Vakava vahinko

Direktiivin johdanto-osan 5 kappaleessa todetaan, että jäsenvaltiot voivat määritellä vakavan vahingon kansallisen lakinsa ja käytäntönsä mukaisesti.

Törkeää vahingontekoa koskevassa rikoslain 35 luvun 2 §:n 1 momentin 1 kohdassa tarkoitetut tilanteet kattavat laajasti direktiivissä tarkoitetun vakavan vahingon. Vahingonteko voidaan kvalifioida törkeäksi, jos vahingonteolla aiheutetaan a) erittäin suurta taloudellista vahinkoa, b) rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa vahinkoa tai c) historiallisesti tai sivistyksellisesti erityisen arvokkaalle omaisuudelle huomattavaa vahinkoa. Esityksessä ehdotetaan, että törkeä datavahingonteko erotetaan omaksi itsenäiseksi pykäläkseen (3 b §) ja siihen sisällytettäisiin alla mainittu 38 luvun 7 b §:ää vastaava kvalifiointiperuste. Uuden ehdotetun törkeän datavahingonteon enimmäisrangaistus olisi viisi vuotta vankeutta.

Rikoslain 38 luvun 7 b §:ssä tarkoitetun törkeän tietojärjestelmän häirinnän 1 momentin 1 kohta sisältää jo nykyisin kvalifiointiperusteen, joka kattaa tilanteet, jossa aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa. Direktiivi ei siten tältä osin edellytä törkeää tietojärjestelmän häirintää koskevan kriminalisoinnin muuttamista lukuun ottamatta enimmäisrangaistuksen nostamista viiteen vuoteen vankeutta.

Rikoslain 38 luvun 6 §:ssä tarkoitettu törkeä tietoliikenteen häirintä ei sisällä nykyisin vakavaa vahinkoa koskevaa kvalifiointiperustetta. Esityksessä ehdotetaan, että mainittuun säännökseen lisättäisiin, samoin kuin edellä törkeän datavahingonteon osalta (35 luvun 3 b §), törkeää tietojärjestelmän häirintää koskevan 7 b §:n 1 momentin 1 kohtaa vastaava kvalifiointiperuste, jonka mukaan teko voi kvalifioitua törkeäksi, jos aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa. Kriteeri ”erityisen tuntuvaa” koskee myös taloudellista vahinkoa (HE 153/2006 vp, s. 66). Tämän lisäksi enimmäisrangaistusta ehdotetaan korotettavaksi viiteen vuoteen vankeutta.

Elintärkeä infrastruktuuri

Elintärkeää infrastruktuuria ei ole direktiivissä määritelty, joten tämä jää jäsenvaltioiden omaan harkintaan. Johdanto-osan 4 kappaleessa on kuitenkin annettu tämän osalta harkinnanvaraista osviittaa. Sen mukaan ”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 ja 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.”.

Artikloissa 4 ja 5 tarkoitettujen rikosten eli käytännössä tietoliikenteen häirinnän, tietojärjestelmän häirinnän ja datavahingonteon kohdistuessa elintärkeään infrastruktuuriin kuuluvaan tietojärjestelmään, saattaa useissa tapauksissa täyttyä myös rikoslain 34 luvun 1 §:ssä tarkoitetun tuhotyön tunnusmerkistö. Kyseisen 1 §:n 2 momentin mukaan tuhotyöstä tuomitaan myös se, joka omaisuutta vahingoittamalla tai tuhoamalla taikka tuotanto-, jakelu- tai tietojärjestelmän toimintaan oikeudettomasti puuttumalla aiheuttaa vakavan vaaran energiahuollolle, yleiselle terveydenhuollolle, maanpuolustukselle, oikeudenhoidolle tai muulle näihin rinnastettavalle yhteiskunnan tärkeälle toiminnolle. Tuhotyötä koskeva kriminalisointi ei kuitenkaan riitä täyttämään direktiivin vaatimuksia tältä osin. Ensinnäkin tuhotyön tunnusmerkistössä edellytetään vakavan vaaran aiheuttamista. Direktiivin säännökset eivät tätä rajausta näyttäisi sallivan, vaan kansallisesti on kriminalisoitava, että 4 ja 5 artiklassa tarkoitettu rikos on ylipäänsä kohdistunut elintärkeään infrastruktuuriin kuuluvaan tietojärjestelmään. Toiseksi tuhotyön neljän vuoden enimmäisrangaistus ei täytä vaatimusta vii-

den vuoden enimmäisrangaistuksen vähimmäistasosta.

Koska direktiivin velvoitteiden täyttämiseksi törkeän tietoliikenteen häirinnän, törkeän tietojärjestelmän häirinnän ja törkeän datavahingonteon enimmäisrangaistusta ehdotetaan nostettavaksi viiteen vuoteen vankeutta ja jotta kriminalisoitava toiminta katettaisiin selkeästi direktiivin vaatimusten ja sen tarkoittamalla tavalla, esityksessä ehdotetaan, että edellä mainittujen rikosten törkeisiin tekomuotoihin sisällytettäisiin uusi kvalifiointiperuste, joka vastaa osin tuhotyön tunnusmerkistöä siltä osin kuin siinä on kyse elintärkeästä infrastruktuurista. Törkeän tietojärjestelmän häirinnän osalta ehdotetaan siten lisättäväksi uusi kvalifiointiperuste, jonka mukaan teko olisi törkeä, jos rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon.

Edellä mainittu olennainen tietojärjestelmä voi olla esimerkiksi hallituksen esityksessä (HE 54/2013 vp) laiksi julkisen hallinnon turvallisuusverkkotoiminnasta tarkoitettu turvallisuusverkko. Mainitun esityksen mukaan tällaisen turvallisuusverkon käyttövelvoite koskisi sellaista valtion johtamiseen ja turvallisuuteen, maanpuolustukseen, yleiseen järjestykseen ja turvallisuuteen, rajaturvallisuuteen, pelastustoimintaan, meripelastustoimintaan, hätäkeskustoimintaan, maahanmuuttoon ja ensihoitopalveluun liittyvää viranomaisten sisäistä, välistä ja ulkoista yhteistoimintaa ja viestintää, joissa noudatetaan korkean varautumisen tai turvallisuuden vaatimuksia. Olennaisia voivat olla myös järjestelmät, jotka liittyvät huoltovarmuuden turvaamiseen. Valtioneuvoston päätöksessä huoltovarmuuden tavoitteista (5.12.2013) mainitaan kriittisen infrastruktuurin osa-alueina energian tuotanto-, siirto- ja jakelujärjestelmät; tieto- ja viestintäjärjestelmät, -verkot ja –palvelut; finanssialan palvelut; liikenne ja logistiikka; vesihuolto; infrastruktuurin rakentaminen ja kunnossapito sekä jätehuolto erityistilanteissa. Nyt ehdotetussa säännöksessä tarkoitettu tärkeä toiminto voi olla myös esimerkiksi elintarvikehuolto. Valtioneuvoston periaatepäätöksessä (16.12.2010) yhteiskunnan turvallisuusstrategiasta puolestaan todetaan, että elintärkeät toiminnot ovat poikkihallinnollisia, yhteiskunnalle välttämättömiä toimintokokonaisuuksia, jotka on oltava turvattuna kaikissa tilanteissa. Suomalaisen yhteiskunnan elintärkeitä toimintoja ovat periaatepäätöksen mukaan valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky sekä henkinen kriisinkestävyys. Myös valtioneuvoston periaatepäätöksessä Suomen kyberturvallisuusstrategiasta (24.1.2013) viitataan edellä mainittuihin valtioneuvoston periaatepäätöksessä (16.12.2010) mainittuihin suomalaisen yhteiskunnan elintärkeisiin toimintoihin sekä valtioneuvoston päätökseen (5.12.2013) huoltovarmuuden tavoitteista.

Törkeään tietoliikenteen häirintään ehdotetaan puolestaan lisättäväksi tietoliikenteen häirinnän perustekomuodossa tarkoitetut häirittävät kohteet kattaen uusi kvalifiointiperuste, jonka mukaan teko olisi törkeä, jos tietoliikenteen häirinnässä rikos kohdistuu laitteeseen, tietojärjestelmään tai viestintään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon.

Edellä selostetun mukaisesti törkeään datavahingontekoon ehdotetaan puolestaan sisällytettäväksi peruste, joka kvalifioisi teon törkeäksi, jos rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon.

Edellä mainittujen rikosten nyt ehdotetut törkeät tekomuodot saattavat joskus olla päällekkäisiä tuhotyötä koskevan kriminalisoinnin kanssa. Joissakin tilanteissa mainitut kriminalisoinnit ovat kattavampia kuin tuhotyö ja joissakin tilanteissa puolestaan tuhotyön tunnusmerkistö voi täyttyä vaikka edellä mainittujen kriminalisointien tunnusmerkistö ei täyttyisikään. Mikäli tietojärjestelmän toimintaan on tuhotyötä koskevassa rikoslain 34 luvun 1 §:n 2 momentissa tarkoitetuin tavoin oikeudettomasti puututtu

aiheuttaen vakavaa vaaraa, ei törkeän datavahingonteon tunnusmerkistö välttämättä täyty, mikäli rikoslain 35 luvun 3 b §:ssä edellytetty vahingoittamistarkoitus ei täyty. Vastaavasti tuhotyön tunnusmerkistö olisi tietyissä tilanteissa osin päällekkäinen törkeää tietoliikenteen häirintää ja törkeää tietojärjestelmän häirintää koskevan kriminalisoinnin kanssa. Myös voimassa olevassa laissa tuhotyön ja törkeän tietoliikenteen häirinnän sekä törkeän tietojärjestelmän häirinnän tunnusmerkistöt ovat osin päällekkäiset. Datavahingonteko, tietojärjestelmän häirintä ja tietoliikenteen häirintä ovat kuitenkin erityissäännöksiä suhteessa tuhotyöhön, sillä ne edellyttävät erityistä tahallisuutta tai tekotapaa. Ne voivat siten tulla sovellettavaksi tuhotyön sijasta vaikka vakavaa vaaraa olisi aiheutunutkin. Tuhotyö puolestaan voi tulla sovellettavaksi tilanteissa, joissa edellä mainittu erityinen tahallisuus tai tekotapa ei ole käsillä, mutta teosta aiheutuu kuitenkin vakavaa vaaraa. Ehdottomien konkurrenssisääntöjen kuvaaminen ei ole mahdollista, ja tilanteet tulee ratkaista kunkin yksittäistapauksen olosuhteet huomioiden yleisten lainkonkurrenssia koskevien periaatteiden mukaisesti.

Henkilötietojen väärinkäyttö

Artiklan 5 kohdan mukaan jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että jos 4 ja 5 artiklassa tarkoitetut teot on tehty käyttämällä väärin toisen henkilötietoja tarkoituksena voittaa kolmannen osapuolen luottamus ja aiheuttaen näin vahinkoa henkilöllisyyden oikealle omistajalle, tätä voidaan kansallisen lain ja säännösten mukaisesti pitää raskauttavana asianhaarana, jolleivät nämä asianhaarat jo kuulu jonkin muun kansallisen lainsäädännön mukaisesti rangaistavan teon tunnusmerkistöön.

Suomen kansallisessa lainsäädännössä ei ole säännöksiä, jotka nimenomaisesti kattaisivat 5 kohdassa tarkoitetut tilanteet. Siinä tarkoitetuissa tilanteissa on kyse niin sanotuista identiteettivarkauksista tai toisen identiteettitietojen väärinkäytöstä silloin kun on kyse 4 artiklassa (laiton järjestelmän häirintä) tai 5 artiklassa (laiton datan vahingoittaminen) tarkoitettujen rikosten tekemisestä. Tyypillisesti tällaisissa tilanteissa voi olla kyse tekijän tietoteknisten jälkien peittämisestä. Tällöin myös tutkintatoimet ja epäilyt saattavat kohdistua siihen henkilöön, jonka identiteetti- , yksilöimis- tai tunnistamistietoja on käytetty. Tässä tarkoitettua identiteettitietoa voi olla myös esimerkiksi henkilön tietokoneen IP-osoite.

Direktiivin velvoitteiden täyttämiseksi voidaan arvioida useita eri toteuttamisvaihtoehtoja. Ensimmäinen vaihtoehto olisi tehdä 5 kohdassa tarkoitetusta toisen identiteetin käyttämisestä kvalifiointiperuste, joka tyypillisesti tekisi ehdotetusta datavahingonteosta (RL 35:3 a), tietoliikenteen häirinnästä (RL 38:5) tai tietojärjestelmän häirinnästä (RL 38:7 a) törkeän. Kyseisen vaihtoehdon ei kuitenkaan voi katsoa olevan optimaalinen, sillä esimerkiksi jälkien peittäminen tässä tarkoitetulla tavalla lienee hyvin tyypillistä edellä mainittujen rikosten osalta. Arvioinnissa on merkitystä myös sillä, että edellä mainittujen rikosten törkeiden tekomuotojen rangaistustasoa ehdotetaan direktiivin velvoitteiden vuoksi nostettavaksi viiteen vuoteen vankeutta. Myöskään direktiivin mainitussa 5 kohdassa tarkoituksena ei ole ollut, että siinä tarkoitetuissa tilanteissa soveltuisi jokin tietty ankara enimmäisrangaistuksen vähimmäistaso, kuten viisi vuotta vankeutta.

Rikoslain 6 luvun 5 §:ssä tarkoitetuista yleisistä koventamisperusteista pykälän 1 kohdassa tarkoitettu rikollisen toiminnan suunnitelmallisuus vastaisi lähinnä artiklan 5 kohdassa tarkoitettua toisen identiteettitietojen väärinkäyttöä. Tämä onkin toinen vaihtoehto täyttää direktiivin velvoitteet. Itse artiklan 5 kohdassakin todetaan, että kohdassa tarkoitettuja tilanteita on voitava ”kansallisen lain mukaisesti pitää raskauttavana asianhaarana”. Mainittu kirjaus antaa varsin laajan liikkumavaran kansalliselle täytäntöönpanolle. Kansallista liikkumavaraa painotetaan edelleen myös johdanto-osan kappaleessa 19, jonka mukaan ”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 rikok-

sentekijöitä. Tuomari voi harkita näitä asianhaaroja yhdessä tietyn tapauksen muiden tosiseikkojen kanssa". On kuitenkin perusteltua, että osin kansallisista tarpeista johtuen identiteettivarkauksiin liittyvän 5 kohdan velvoitteet pannaan tästä huolimatta täytäntöön ottamalla aihetta koskevat nimenomaiset säännökset kansalliseen lainsäädäntöön.

Kolmas toteuttamisvaihtoehto olisi lisätä 5 kohdassa tarkoitetut tilanteet rikoslain 6 luvun 5 §:ään uudeksi yleiseksi koventamisperusteeksi. Tässä tarkoitetussa 5 kohdassa olevan tilanteen voidaan kuitenkin katsoa olevan liian spesifi, eikä sen lisääminen uudeksi yleiseksi koventamisperusteeksi olisi perusteltua.

Neljäs toteuttamisvaihtoehto olisi se, että kyseisen kohdan osalta viitattaisiin rikoslain 6 luvun 4 §:ään jonka mukaan rangaistus on mitattava niin, että se on oikeudenmukaisessa suhteessa rikoksen vahingollisuuteen ja vaarallisuuteen, teon vaikuttimiin sekä rikoksesta ilmenevään muuhun tekijän syyllisyyteen. Voidaan kuitenkin arvioida, että tämä toteuttamisvaihtoehto ei olisi optimaalinen kansalliset tarpeet huomioon ottaen.

Direktiivin velvoitteet voidaan 5 kohdasta ilmi käyvin tavoin täyttää myös siten, että kohdassa tarkoitetut tilanteet katetaan jonkin muun rikoksen tunnusmerkistössä eli niiden osalta laaditaan itsenäinen kriminalisointi (viides toteuttamisvaihtoehto). Esityksessä ehdotetaankin lisättäväksi rikoslain 38 lukuun uusi 9 b §, joka vastaisi direktiivin määräyksiä rajautumatta kuitenkaan direktiivin 4 ja 5 artiklassa tarkoitettujen rikosten tilanteisiin. Sen mukaan "Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon". Tällöin direktiivin 5 kohdassa edellytetyin tavoin rangaistus 4 ja 5 artiklassa tarkoitetuista teoista voisi tarvittaessa koventua yhteisen rangaistuksen myötä, mikäli henkilö tuomittaisiin myös uudessa 9 b §:ssä tarkoitetusta teosta. Uudessa 9 b §:ssä tarkoitetussa teossa suojeluobjektina on identiteetin loukkaamattomuus (sen, jonka henkilötietoja on käytetty), kun taas direktiivin 4 ja 5 artiklassa tarkoitetuissa teoissa ja niitä vastaavissa kansallisissa kriminalisoinneissa suojellaan tietojärjestelmää tai dataa. Näin ollen konkurrenssiopillisesti molemmista rikoksista tuomitseminen on mahdollista. Toisaalta direktiivi ei edes edellytä rangaistuksen ankaroitumista, mikäli 5 kohdassa tarkoitettu teko on katettu jollain kansallisen lain kriminalisoinnilla, jollaista esityksessä nyt ehdotetaan.

Toisen henkilötietoja hyväksikäyttäen on saatettu syyllistyä esimerkiksi rikoslain 36 luvun 1 §:ssä tarkoitettuun petokseen. Tällöin erehdyttämisen kohteena on henkilö, joka esimerkiksi määrää taloudellisesta edusta ja suojeluobjektina keskeisesti erehdytettävän henkilön omaisuuden suoja. Nyt ehdotetussa identiteettivarkautta koskevassa kriminalisoinnissa suojeluobjektina puolestaan on sen henkilön identiteetin loukkaamattomuus, jonka henkilötietoja on käytetty petosrikoksen tekemisessä. Näin ollen tekijä voidaan tuomita molemmista rikoksista. Tekijä voidaan toisaalta tuomita identiteettivarkaudesta, vaikka henkilöä ei tuomittaisikaan petoksesta, mikäli identiteettivarkaudesta tuomitsemisen edellytykset täyttyvät. Vastaavasti esimerkiksi tietojärjestelmän häirinnässä (RL 38:7 a) suojeluobjektina on keskeisesti tietojärjestelmän häiriötön toiminta. Myös rikoksen uhri on usein eri henkilö. Näin ollen myös tietojärjestelmän häirinnästä ja identiteettivarkaudesta voitaisiin tuomita samanaikaisesti. Sama koskee myös esimerkiksi datavahingontekoa (RL 35:3 a), jossa suojeluobjektina on datan eheys ja uhrina usein eri henkilö kuin identiteettivarkaudessa. Ehdotettu uusi identiteettivarkautta koskeva kriminalisointi selkeyttää esimerkiksi petosrikosten osalta sen henkilön asianomistajaasemaa, jonka henkilötietoja on käytetty.

Direktiivin vaatimusten täyttämiseksi riittäisi, että edellä mainitussa kriminalisoinnissa rajauduttaisiin vain tilanteisiin, joissa olisi syyllistytty samalla rikoslain 38 luvun 5 §:ssä tarkoitettuun tietoliikenteen häirintään, 6 §:ssä tarkoitettuun törkeään tietoliikenteen häirintään, 7 a §:ssä tarkoitettuun tietojärjestelmän häirintään, 7 b §:ssä tarkoitettuun törkeään tietojärjestelmän häirintään, 35 luvun 3 a §:ssä tarkoitettuun datavahingontekoon tai sen 35 luvun 3 b §:ssä tarkoitettuun törke-

ään tekomuotoon taikka niiden rangaistavaan yritykseen. Tällainen rajaus ei kuitenkaan ole perusteltu, sillä vastaavanlaiseen ja asiallisesti yhtä moitittavaan jälkien peittelyyn ja siten haitan aiheuttamiseen sille, jota identiteettitieto koskee, voidaan turvautua myös muissa rikoksissa. Artiklan 5 kohdassa ja nyt ehdotettavassa uudessa 9 b:ssä keskitytään siihen henkilöön, jonka identiteettitietoja on käytetty väärin. Tällainen henkilö on tässä tapauksessa identiteettivarkauden uhri, jonka asemaa ehdotetulla uudella säännöksellä on tarkoitus parantaa. Mikäli toisen identiteettitietojen väärinkäyttämistä koskeva kriminalisointi kytkettäisiin tiettyjen muiden listattujen rikosten täyttyneisiin tekomuotoihin, voisi tietyissä tapauksissa syntyä ongelmia siitä, että kyseisten listarikosten asianomistajat eivät syystä tai toisesta haluaisi syytettä nostettavaksi. Tällöin myöskään ehdotetusta 9 b §:stä ei voitaisi nostaa syytettä vaikka sille, jonka henkilötietoja on käytetty väärin, olisi aiheutunut haittaa. Tällainen tilanne voisi syntyä muun muassa sen vuoksi, että ehdotettu rikoslain 35 luvun 3 a §:ssä tarkoitettu datavahingonteko ja 38 luvun 7 a §:ssä tarkoitettu tietojärjestelmän häirintä ovat asianomistajarikoksia. Ehdotetussa 9 b §:ssä ei voitaisi direktiivin vaatimusten täyttämiseksi rajautua myöskään pelkästään internet–ympäristöön tai televerkossa tapahtuvaan viestintään, sillä tietojärjestelmää ja tietoliikennettä voidaan häiritä tai dataa vahingoittaa myös fyysisesti ja reaalimaailmassa. Uutta ehdotettua 9 b §:ää puoltaa direktiivin vaatimusten täyttämisen lisäksi myös se, että kansallisesti identiteettivarkauden kattavaan kriminalisointiin ja erityisesti identiteettivarkauksien uhrin, eli sen henkilön asemaan jonka identiteettitietoja on käytetty, on viime aikoina kiinnitetty huomiota (ks. esimerkiksi henkilöllisyyden luomista koskeva hanke (identiteettiohjelma), työryhmän loppuraportti, sisäasiainministeriön julkaisuja 32/2010 sekä oikeusministeriön identiteettivarkauksia koskeva arviomuistio OM 4/41/2013 ja sitä koskevista lausunnoista tehty tiivistelmä, Mietintöjä ja lausuntoja 47/2013.).

Ehdotettu uusi kriminalisointi olisi rajattu tilanteisiin joissa on aiheutunut taloudellista vahinkoa taikka muuta vähäistä suurempaa haittaa. Tällainen rajaus on direktiivin sallima, sillä direktiivin 4 ja 5 artiklassa tarkoitettu kriminalisointivelvoite koskee vain tilanteita, jotka eivät ole vähäisiä. Näin ollen direktiivin 9 artiklan 5 kohdassa tarkoitettu toisen identiteettitietojen väärinkäyttöä koskeva ankaroittamisperuste voi rajautua kattamaan tilanteet jotka ovat muita kuin vähäisiä.

Artikla 10. *Oikeushenkilön vastuu.* Artiklan 1 kohdan mukaan 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.

Artiklan 2 kohdan mukaan 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 oikeushenkilön hyväksi.

Artiklan 3 kohdan mukaan 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.

Artikla on standardimuotoinen oikeushenkilöiden vastuuta koskeva artikla, jollainen sisältyy useisiin Euroopan unionin säädöksiin. Puitepäätös sisältää asiasisällöltään vastaavan artiklan, jota on selostettu yleissopimuksen voimaansaattamista ja puitepäätöstä koskevassa hallituksen esityksessä (HE 153/2006 vp), eikä oikeushenkilön rangaistusvastuun yleisten edellytysten analysointi tässä yhteydessä ole tarkoituksenmukaista. Yleissopimus sisältää myös asiasisällöltään vastaavankaltaiset määräykset.

Suomessa voimassa olevat yleiset säännökset oikeushenkilön rangaistusvastuusta sisältyvät rikoslain 9 lukuun. Yksittäisen rikossäännöksen osalta oikeushenkilön rangais-

tusvastuun soveltuminen edellyttää, että rikoslaissa on asiaa koskeva rangaistussäännös.

Rikoslain 9 luvun 2 §:n 1 momentin mukaan oikeushenkilö tuomitaan yhteisösakkoon, jos sen lakisääteiseen toimielimeen tai muuhun johtoon kuuluva taikka oikeushenkilössä tosiasiallista päätösvaltaa käyttävä on ollut osallinen rikokseen tai sallinut rikoksen tekemisen taikka, jos sen toiminnassa ei ole noudatettu vaadittavaa huolellisuutta ja varovaisuutta rikoksen ehkäisemiseksi. Saman pykälän 2 momentin mukaan yhteisösakkoon tuomitaan, vaikkei rikoksentekijää saada selville tai muusta syystä tuomita rangaistukseen. Luvun 3 §:n mukaan rikos katsotaan oikeushenkilön toiminnassa tehdyksi, jos sen tekijä on toiminut oikeushenkilön puolesta tai hyväksi ja hän kuuluu oikeushenkilön johtoon tai on virka- tai työsuhteessa oikeushenkilöön taikka on toiminut oikeushenkilön edustajalta saamansa toimeksiannon perusteella.

Oikeushenkilön rangaistusvastuu ulottuu nykyään seuraaviin direktiivissä tarkoitettuihin rikoksiin:

1. vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9 a)
2. (data)vahingonteko (RL 35:1.2) ja ehdotettu uusi datavahingonteko (RL 35:3 a)
3. törkeä (data)vahingonteko (RL 35:2) ja ehdotettu uusi törkeä datavahingonteko (RL 35:3 b)
4. viestintäsalaisuuden loukkaus (RL 38:3)
5. törkeä viestintäsalaisuuden loukkaus (RL 38:4)
6. tietoliikenteen häirintä (RL 38:5)
7. törkeä tietoliikenteen häirintä (RL 38:6)
8. tietojärjestelmän häirintä (RL 38:7 a)
9. törkeä tietojärjestelmän häirintä (RL 38:7 b)
10. tietomurto (RL 38:8)
11. törkeä tietomurto (RL 38:8 a)

Oikeushenkilön rangaistusvastuu ei kata lievää vahingontekoa, lievää tietoliikenteen häirintää, lievää tietojärjestelmän häirintää eikä tietoverkkorikosvälineen hallussapitoa. Se ei kattaisi myöskään ehdotettua lievää datavahingontekoa (RL 35:3 c). Edellä mainittuihin lieviin tekomuotoihin ei ole perusteltua ulottaa oikeushenkilön rangaistusvastuuta. Järjestely on direktiivin mukainen, koska kansainvälinen velvoite ei koske vähäisiä tapauksia. Sen sijaan direktiivin velvoitteiden täyttämiseksi oikeushenkilön rangaistusvastuu olisi ulotettava tietoverkkorikosvälineen hallussapitoon (RL 34:9 b) mikäli ”käyttöön hankkimista” ei katettaisi tyhjentävästi RL 34 luvun 9 a §:ssä nykyisen 9 b §:n sijaan. Esityksessä ehdotetaan kuitenkin ”käyttöön hankkimisen” kattamista 9 a §:ssä. Oikeushenkilön rangaistusvastuun ulottaminen tietoverkkorikosvälineen hallussapitoon ei ollut välttämätöntä vielä yleissopimuksen voimaansaattamista ja puitepäätöstä koskevan hallituksen esityksen (HE 153/2006 vp, s. 27) yhteydessä, sillä yleissopimuksen mukaan vastuu saattoi olla myös yksityisoikeudellista vahingonkorvausvastuuta. Puitepäätös sen sijaan edellytti rikosoikeudellisia tai muita sakkoja, mutta sen soveltamisalaan eivät kuuluneet rikosten tekemiseen käytettävät välineet.

Artikla edellyttää oikeushenkilön rangaistusvastuun ulottamista esityksessä ehdotettuihin uusiin datavahingontekoon (RL 35:3 a) ja törkeään datavahingontekoon (RL 35:3 b), joiden myötä datavahingonteko ja törkeä datavahingonteko erotetaan perusmuotoisen vahingonteon tunnusmerkistöstä.

Artikla 11. *Oikeushenkilöille määrättävät seuraamukset.* Oikeushenkilöihin kohdistettavia seuraamuksia koskeva artikla on myös standardimuotoinen. Se vastaa puitepäätöksen artiklaa. Artiklan mukaan jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että 10 artiklan 1 kohdan mukaisesti vastuulliseksi todettua oikeushenkilöä voidaan rangaista tehokkain, oikeasuhtaisin ja varoittavin seuraamuksin, joihin kuuluvat rikosoikeudelliset tai muut sakot. Edellisessä artiklassa kuvatuin tavoin Suomessa oikeushenkilön vastuu on direktiivissä tarkoitettujen rikosten osalta katettu ja tarkoitus kattaa oikeushenkilön rikosoikeudellisella vastuulla ja rikoslain 9 luvun mukaisella yhteisösakolla.

Artiklan 1 kohdassa on myös esimerkkiluettelo vaihtoehtoisista seuraamuksista, joista osa on Suomen oikeusjärjestelmälle vieraita. Asialla ei kuitenkaan ole merkitystä, koska säännös ei ole tältä osin velvoittava. Artiklan 2 kohdassa on lisäksi säännös, jonka

mukaan 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 oikeasuhtaisia ja varoittavia.

Artikla ei edellytä muutoksia lainsäädäntöön.

Artikla 12. *Lainkäyttövalta.* Artiklan 1 kohdan mukaan 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. Artiklan 2 kohdan mukaan 1 kohdan a alakohdassa tarkoitetuissa tapauksissa jäsenvaltion on varmistettava, että sillä on lainkäyttövalta, kun a) rikoksentekijä tekee rikoksen olleessaan 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.

Artiklan 3 kohdan mukaan 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.

Myös yleissopimus ja puitepäätös sisältävät määräykset lainkäyttövallasta, joskin niiden velvoitteiden laajuus poikkeaa hieman direktiivin velvoitteista.

Suomessa voimassaolevat säännökset rikoslain soveltamisalasta ovat rikoslain 1 luvussa.

Artiklan 1 kohdan a alakohtaa vastaava säännös on luvun 1 §, jonka mukaan Suomessa tehtyyn rikokseen sovelletaan Suomen lakia. Artiklan 2 kohtaa vastaava säännös on 10 §:n 1 momentti, jonka mukaan rikos katsotaan tehdyksi sekä siellä, missä rikollinen teko suoritettiin, että siellä, missä rikoksen tunnusmerkistön mukainen seuraus ilmeni.

Artiklan 1 kohdan b alakohtaa vastaava säännös on 6 §, jonka mukaan Suomen kansalaisen Suomen ulkopuolella tekemään rikokseen sovelletaan Suomen lakia. Luvun 11 § sisältää lisäedellytyksenä myös niin sanotun kaksoisrangaistavuuden vaatimuksen.

Artiklan 3 kohdalla ei ole välitöntä merkitystä lainsäädännön kannalta, sillä se sisältää vain informointivelvoitteen mahdollisten laajempien lainkäyttövaltuuksien osalta. Kohdan a alakohdan osalta merkityksellinen on kuitenkin rikoslain 1 luvun 6 §:n 3 momentin 1 kohta, jonka mukaan Suomen kansalaiseen rinnastetaan henkilö, joka rikoksen tekohetkellä asui tai oikeudenkäynnin alkaessa asuu pysyvästi Suomessa. Kyseisestä säännöksestä tulisi informoida komissiota täytäntöönpanoilmoituksen yhteydessä. Artiklan 3 kohdan b alakohdan ja oikeushenkilön hyväksi tehdyn rikoksen osalta ei Suomessa ole vastaavaa toimivaltasäännöstä.

Voimassa olevat säännökset vastaavat artiklan velvoitteita. Artikla ei edellytä lainsäädännön muuttamista.

Artikla 13. *Tietojenvaihto.* Artiklan 1 kohdan mukaan 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 tiedonvaihtoa varten. Jäsenvaltioiden on myös huolehdittava siitä, että niillä on käytettävissä menettelyt, jotta toimivaltainen viranomainen voi kiireellisten avunpyyntöjen osalta ilmoittaa kahdeksan tunnin kuluessa pyynnön vastaanottamisesta ainakin sen, vastataanko pyyntöön sekä missä muodossa ja milloin tällainen vastaus arviolta toimitetaan.

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

Artiklassa tarkoitetusta yhteyspisteestä ja verkostosta on määräykset jo yleissopimuksen 35 artiklassa ja puitepäätöksen 11 artiklassa. Yleissopimus on saatettu Suomessa voimaan tasavallan presidentin asetuksella 768/2007. Artiklassa velvoitetaankin vain varmistamaan tällaisen yhteyspisteen olemassaolo ja se, että nykyistä verkostoa hyödynnetään. Direktiivin artiklan 1 kohta vastaa

asiallisesti puitepäätöksen artiklaa. Ainoa merkityksellinen lisäys on se, että direktiivin 1 kohdan mukaan kiireellisissä tapauksissa kontaktipisteiden on pystyttävä indikoimaan kahdeksan tunnin sisällä pyynnön vastaanottamisesta, tullaanko avunpyyntöön vastaamaan samoin kuin vastauksen muoto ja arvioitu aika. Yhteyspisteenä Suomessa toimii nykyisin keskusrikospoliisi. Direktiivin täytäntöönpanoilmoitusten yhteydessä tästä ilmoitetaan komissiolle artiklan 2 kohdan mukaisesti. Artiklassa mainittu kahdeksan tunnin sääntö ei edellytä säädösmuutoksia. Poliisin sisäistä ohjeistusta päivitetään niin, että kuittaus voidaan antaa kahdeksan tunnin kuluessa.

Artiklan 3 kohdan mukaan 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.

Kohta on yleisluonteinen kehotus eikä asianmukaisia ilmoituskanavia määritellä tarkemmin. On käytännössä selvää, että rikosten ilmoittamista varten on olemassa ilmoituskanavat. Niiden asianmukaisuus puolestaan määrittyy kansallisesti. Suomessa kohdassa tarkoitettuja ilmoituskanavia ovat muun muassa rikosilmoitus, joka joissakin tapauksissa voidaan tehdä myös sähköisesti, sähköposti-ilmoitukset tai puhelinsoitto viranomaisille, ns. ”sininen nappi” poliisin verkkosivulla eli nettivinkki sekä Viestintäviraston kyberturvallisuuskeskukselle (cert-fi) ilmoittaminen, jota varten Viestintäviraston verkkosivulla on muun muassa linkki ”ilmoita tietoturvaloukkauksesta”. Kohta ei edellytä säädösmuutoksia.

Artikla 14. *Seuranta ja tilastot.* Artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että niillä on järjestelmä, jonka avulla voidaan kirjata, tuottaa ja antaa tilastotietoja 3—7 artiklassa tarkoitetuista rikoksista. Artiklan 2 kohdan mukaan 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.

Artiklan 3 kohdan mukaan 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.

Direktiivissä tarkoitetut olemassa olevat tiedot ovat saatavissa ja toimitettavissa direktiivin edellyttämällä tavalla ilman säädösmuutoksia. Tilastointia edesauttaa lisäksi se, että esityksessä ehdotetaan uutta itsenäistä datavahingonteon kriminalisointia, eikä kansainvälisten velvoitteiden täyttäminen enää sen myötä perustuisi vahingonteon perustekomuodon 2 momenttiin. Tämä on merkityksellistä, sillä tilastoinnissa oleellista on rikosnimike. Mikäli datavahingontekoa ei eriytettäisi omaksi rikokseen, tilastoituisi vahingontekokriminalisoinnin alaisuuteen huomattava määrä vahingontekoja, joilla ei ole liityntää tietoverkkorikoksiin.

Artiklat 15—19. Artiklat 15—19 sisältävät tavanomaiset loppumääräykset aiemman puitepäätöksen 2005/222/YOS korvaamisesta, direktiivin velvoitteiden saattamisesta osaksi kansallista lainsäädäntöä, raportoinnista, voimaantulosta ja osoituksesta.

2 Lakiehdotusten perustelut

2.1 Rikoslaki

34 luku **Yleisvaarallisista rikoksista**

9 a §. *Vaaran aiheuttaminen tietojenkäsittelylle.* Edellä yksityiskohtaisissa perusteluissa 7 artiklan kohdalla selostetuin tavoin niin sanottuja tietoverkkorikosvälineitä koskevan kriminalisoinnin 1 momentin 1 kohtaan ehdotetaan lisättäväksi uusi *käyttöön hankkimista* koskeva tekotapa. Pykälän 1 momentin 1 kohdan mukaan vaaran aiheuttamisesta tietojenkäsittelylle voitaisiin tuomita myös se, joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle

1) tuo maahan, *hankkii käyttöön*, valmistaa, myy tai muuten levittää taikka asettaa saataville

a) sellaisen laitteen tai tietokoneohjelman taikka ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa taikka murtamaan tai purkamaan sähköisen viestinnän teknisen suojauksen tai tietojärjestelmän suojauksen taikka

b) tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon.

Lisäys on tarpeen direktiivin rikosten tekemiseen käytettäviä välineitä koskevan 7 artiklan, vähintään kahden vuoden enimmäisrangaistusta edellyttävän 9 artiklan 2 kohdan ja oikeushenkilön vastuuta koskevan 10 artiklan täytäntöönpanemiseksi. Tietoverkkorikosvälineen hallussapito on nykyisin kriminalisoitu tietoverkkorikosvälineen hallussapitoa koskevassa luvun 9 b §:ssä. Mainittu kriminalisointi ei kuitenkaan täytä direktiivin vaatimuksia sen vuoksi, että direktiivissä tarkoitettu käyttöön hankkiminen ja toisaalta hallussapito ovat yksityiskohtaisissa perusteluissa 7 artiklan osalta ja alla selostetuin tavoin osin eri tekotapoja ja mainitut tekotavat on myös yleissopimuksessa erotettu toisistaan. Nykyiseen 9 b §:ään ei luvun 13 §:n mukaisesti sovelleta myöskään oikeushenkilön rangaistusvastuuta toisin kuin 9 a §:ssä tarkoitettuun vaaran aiheuttamiseen tietojenkäsittelylle.

Direktiivi edellyttää ”käyttöön hankkimisen” osalta kahden vuoden enimmäisrangaistusta. Tietoverkkorikosvälineen hallussapidon eli rikoslain 34 luvun 9 b §:ssä tarkoitetun teon enimmäisrangaistus on kuusi kuukautta vankeutta. Pelkän tietoverkkorikosvälineen hallussapidon ei kuitenkaan voi katsoa olevan yhtä moitittava rikos kuin 9 a §:ssä tarkoitettu vaaran aiheuttaminen tietojenkäsittelylle. Näin ollen 9 b §:n enimmäisrangaistuksen nostaminen kahteen vuoteen vankeutta ei olisi perusteltua. Käyttöön hankkimisen voidaan katsoa myös olevan moitittavampaa kuin pelkkä hallussapito eikä se tarkoita samaa asiaa vaikkakin hankkimisen seurauksena väline päätyy hankkijan haltuun. Haittaamis- tai vahingoittamistarkoitusta varten hankkiminen edellyttää aktiivisia toimia välineen haltuun saamiseksi toisin kuin pelkkä hallussapito, jonka osalta tunnusmerkistö voi täyttyä jo sen perusteella, että henkilöllä yksinkertaisesti on väline hallussaan, edellyttäen, että säännöksen muut kriteerit kuten haittaamis- tai vahingoittamistarkoitus täyttyvät. Käyttöön hankkiminen puolestaan voi edellyttää muun muassa aktiivista etsimistä, tiedon hankkimista ja sen johdosta esimerkiksi välineen tilaamista internetistä. Oleellista on siten aktiivinen toiminta välineen hankkimiseksi käytettäväksi haittaamis- tai vahingoittamistarkoituksissa. Tunnusmerkistö käyttöön hankkimisen osalta täyttyisi vasta silloin, kun väline on saatu haltuun.

14 §. *Määritelmät.* Lukuun ehdotetaan yksityiskohtaisissa perusteluissa 2 artiklan kohdalla ja jäljempänä 38 luvun 13 §:n perusteluissa selostetuista syistä lisättäväksi uusi määritelmäsäännös, johon sisältyy 34 luvun 9 a ja 9 b pykälien osalta viittaus 38 luvun ehdotetussa 13 §:ssä olevaan tietojärjestelmän määritelmään.

35 luku Vahingonteosta

1 §. *Vahingonteko.* Vahingontekoa koskevan pykälän niin sanottua datavahingontekoa koskevat 2 ja 3 momentti ehdotetaan yksityiskohtaisissa perusteluissa 5 artiklan kohdalla esitetyistä syistä kumottaviksi. Vastaava sääntely siirrettäisiin direktiivin edellyttämillä muutoksilla tarkennettuna itsenäiseksi datavahingontekoa koskevaksi 3 a pykäläksi. Näin tavallisen vahingonteon enimmäisrangaistusta ei tarvitse direktiivin 9 artiklan 2 kohdan vaatimusten vuoksi korottaa. Ehdotetulla ratkaisulla pyritään myös selkeyttämään säännösten kirjoitustekniikkaa, sillä sääntelytavalla on vaikutus myös vahingonteon törkeää tekomuotoa koskevaan sääntelyyn. Edelleen vahingonteon ja datavahingonteon eriyttämisellä mahdollistetaan datavahingontekojen parempi tilastointi 14 artiklan edellyttämällä tavalla.

2 §. *Törkeä vahingonteko.* Törkeää vahingontekoa koskevan pykälän 1 momentin datavahingontekoon liittyvä 2 kohta ehdotetaan kumottavaksi. Sitä koskeva sääntely direktiivin edellyttämillä lisäyksillä täydennettynä ehdotetaan siirrettäväksi yksityiskohtaisissa perusteluissa 5 artiklan sekä 9 artiklan 3 ja 4 kohdan osalta selostetuin tavoin uuteen törkeää datavahingontekoa koskevaan

3 b pykälään. Ratkaisu vastaa vahingonteon perustekomuodon osalta omaksuttua.

3 a §. *Datavahingonteko.* Lukuun lisättäisiin edellä 1 §:n kohdalla ja yksityiskohtaisissa perusteluissa 5 artiklan kohdalla esitetyistä syistä uusi datavahingontekoa koskeva pykälä, jolloin datavahingonteot siirrettäisiin nykyisestä vahingontekoa koskevasta 1 §:stä. Pykälän 1 momentin mukaan tietovälineelle tallennetun tiedon tai muun tallennuksen taikka tietojärjestelmässä olevan datan vahingoittamistarkoituksessa ja oikeudettomasti tehty hävittäminen, turmeleminen, kätkeminen, vahingoittaminen, muuttaminen, käyttökelvottomaksi saattaminen tai salaaminen olisi kriminalisoitu datavahingontekona.

Asiallisesti uusi pykälä olisi lähtökohtaisesti sisällöllisesti sama kuin kumottavat 1 §:n 2 ja 3 momentit. Direktiivin 5 artiklan vaatimusten täyttämiseksi tekotavoiksi lisättäisiin kuitenkin vahingoittaminen, muuttaminen ja käyttökelvottomaksi saattaminen. Lisäksi direktiivin vaatimusten mukaisesti teko voisi kohdistua tietovälineelle tallennetun tiedon tai muun tallennuksen lisäksi tietojärjestelmässä olevaan dataan. Edellä mainittu lisäys on oleellinen, sillä tietojärjestelmässä oleva data voi olla muussakin muodossa kuin pysyväisluonteisesti tallennettuna. Se voi olla esimerkiksi tietojärjestelmän sisällä siirrettävänä. Direktiivin vaatimusten mukaisesti ehdotetun uuden datavahingonteon rangaistusasteikko olisi sakkoa tai enintään kaksi vuotta vankeutta. Datavahingonteko ilmentää monissa tapauksissa suurempaa tahallisuutta eli edellyttää usein tietynasteista tai suurempaa suunnitelmallisuutta kuin perustekomuotoinen vahingonteko. Tämän vuoksi on perusteltua, että datavahingonteossa on käytettävissä korkeampi enimmäisrangaistus kuin vahingonteon perustunnusmerkistössä.

Hallituksen esityksen 153/2006 vp yhteydessä 1 §:ssä tarkoitetun vahingonteon perustunnusmerkistön enimmäisrangaistusta ehdotettiin puitepäätöksen vaatimusten täyttämiseksi nostettavaksi kahteen vuoteen vankeutta. Tuolloin lakivaliokunta totesi mietinnössään (LaVM 23/2006 vp), että puitepäätöksen 7 artiklassa asetettu velvoite säätää vähintään kahden vuoden enimmäisrangaistus ei koske muita vahingontekorikoksia kuin käsillä olevan pykälän 2 momentissa tarkoitettua ns. tietovahingontekoa. Lisäksi tuolloin puitepäätöksen velvoitteet koskivat vain tapauksia, joissa rikos on tehty osana järjestäytyneen rikollisryhmän toimintaa. Valiokunta ei pitänyt perusteltuna, että puitepäätöksen alaltaan hyvin suppean velvoitteen täytäntöönpanemiseksi olisi tehty ehdotetun kaltainen olennainen muutos vahingonteon rangaistusasteikkoon. Valiokunnan mukaan ehdotetulla muutoksella olisi saattanut olla ennakoimattomia kriminaalipoliittisia vaikutuksia, kun otetaan huomioon vahingontekorikosten yleisyys ja se, että kysymys on tyypillisestä nuorisorikollisuuden lajista. Valiokunnan mukaan tuolloin ehdotettua enimmäisrangaistuksen korottamista vastaan puhui myös se, että sen myötä vahingonteosta tulisi ankarammin rangaistava rikos kuin varkaudesta. Rikoslain kokonaisuudistuksen ensimmäisessä vaiheessa omaisuusrikoksia koskevaa sääntelyä uudistettaessa on todettu, että vahingontekorikokset keskimäärin osoittavat vähäisempää syyllisyyttä kuin useimmat muut omaisuusrikokset eikä niihin ole perusteltua suhtautua yhtä ankarasti kuin esimerkiksi varkausrikoksiin (HE 66/1988 vp, s. 22/I). Valiokunta piti tätä käsitystä edelleen ajankohtaisena. Edellä mainitut näkökohdat ovat yhä merkityksellisiä myös tämän direktiivin täytäntöönpanotoimien yhteydessä. Tämän vuoksi esityksessä ehdotetaan datavahingonteon erottamista itsenäiseksi rikoksekseen.

Pykälän toisen momentin mukaan datavahingonteon yritys olisi rangaistavaa, kuten nykyisinkin 1 §:n 3 momentissa. Tätä edellyttää myös direktiivin 8 artikla.

3 b §. *Törkeä datavahingonteko.* Lukuun lisättäisiin edellä 1, 2 ja 3 a pykälien yhteydessä sekä yksityiskohtaisissa perusteluissa 5 artiklan sekä 9 artiklan 3 ja 4 kohdan osalta selostetuin tavoin uusi törkeää datavahingontekoa koskeva pykälä. Datavahingonteko kvalifioituisi törkeäksi ensinnäkin, jos datavahingonteossa aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa. Mainitulla perusteella täytetään direktiivin 9 artiklan 4 kohdan b luetelmakohdan vaatimukset liittyen vakavan vahingon aiheuttamiseen. Kvalifiointiperuste vastaa nykyisen tietojärjestelmän häirinnän (38 luvun 7 b §) 1 momentin 1 kohdassa olevaa kvalifiointiperus-

tetta. Vastaavaa perustetta ehdotetaan direktiivin velvoitteiden täyttämiseksi myös tietoliikenteen häirinnän törkeään tekomuotoon (38 luvun 6 §). Kvalifiointiperuste poikkeaa yksityiskohtien osalta hieman nykyisestä 2 §:n 1 momentin 1 kohdassa olevista törkeää vahingontekoa koskevista kvalifiointiperusteista, mutta niiden sisältö on pitkälti sama ja nyt ehdotettu ja nykyisin törkeässä tietojärjestelmän häirinnässä olevan muotoilun kanssa yhdenmukaisen kvalifiointiperusteen voi katsoa soveltuvan paremmin datavahingontekoon. Törkeää datavahingontekoa koskevassa kvalifiointiperusteessa ei nyt mainittaisi nimenomaisesti historiallisesti tai sivistyksellisesti erityisen arvokkaalle omaisuudelle aiheutettua huomattavaa vahinkoa. Käytännössä mikäli datavahingonteko aiheuttaisi tällaiselle erityisen arvokkaalle omaisuudelle huomattavaa vahinkoa, tulisi yleensä nyt ehdotettu erityisen tuntuvaa haittaa tai taloudellista vahinkoa koskeva kvalifiointiperuste sovellettavaksi.

Törkeään datavahingontekoon sisältyisi myös edellä yksityiskohtaisissa perusteluissa 9 artiklan kohdalla ja yksityiskohtaisissa perusteluissa 2 §:n kohdalla selostetuin tavoin rikollisjärjestöä koskeva kvalifiointiperuste. Täysin vastaava peruste sisältyy jo nykyisin kumottavaksi ehdotettuun 2 §:n 2 kohtaan. Sen mukaan rikos voi kvalifioitua törkeäksi, jos rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa. Direktiivin vaatimusten täyttämiseksi vastaava peruste ehdotetaan lisättäväksi myös törkeään tietoliikenteen häirintään (38 luvun 6 §) ja törkeään tietojärjestelmän häirintään (38 luvun 7 b §).

Törkeään datavahingontekoon sisältyisi myös yksityiskohtaisissa perusteluissa 9 artiklan 3 kohdan osalta esitetyin tavoin niin sanottuja bottiverkkoja koskeva kvalifiointiperuste. Sen mukaan teko voisi kvalifioitua törkeäksi, jos rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa. Vastaava kvalifiointiperuste sisällytettäisiin myös törkeään tietoliikenteen häirintään ja törkeään tietojärjestelmän häirintään.

Törkeään datavahingontekoon sisältyisi myös direktiivin vaatimusten mukaisesti ja yksityiskohtaisissa perusteluissa 9 artiklan kohdalla selostetuin tavoin niin sanottuja elintärkeitä infrastruktuureita koskeva kvalifiointiperuste. Sen mukaan teko voisi kvalifioitua törkeäksi, jos rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon. Vastaava kvalifiointiperuste sisällytettäisiin myös törkeään tietoliikenteen häirintään ja törkeään tietojärjestelmän häirintään.

Direktiivin 8 artiklan vaatimusten mukaisesti yritys olisi rangaistava, kuten törkeässä vahingonteossa nykyisinkin.

3 c §. *Lievä datavahingonteko.* Tavallisen vahingonteon kriminalisointia vastaavasti lukuun ehdotetaan lisättäväksi uusi lievää datavahingontekoa koskeva pykälä yksityiskohtaisissa perusteluissa 5 artiklan osalta selostetun mukaisesti. Pykälä olisi sisällöllisesti yhdenmukainen nykyisen lievää vahingontekoa koskevan kriminalisoinnin kanssa. Se tulisi sovellettavaksi, jos datavahingonteko, huomioon ottaen vahingon vähäisyys tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen. Seuraamuksena olisi sakkorangaistus.

6 §. *Syyteoikeus.* Pykälään ehdotetaan lisättäväksi viittaukset uuteen ehdotettuun datavahingontekoon (3 a §) ja lievään datavahingontekoon (3 c §). Kyseessä on tekninen muutos, joka on seurausta datavahingonteon ja lievän datavahingonteon erottamisesta itsenäisiksi kriminalisoinneikseen. Myös näiden rikosten osalta, jos rikoksen kohteena on ollut ainoastaan yksityinen omaisuus, syyttäjä saisi nostaa syytteen vain, jos asianomistaja on ilmoittanut rikoksen syytteeseen pantavaksi. Pykälän teknistä kirjoitusasua korjattaisiin lisäksi vastaamaan nykysuosituksia.

7 §. *Toimenpiteistä luopuminen.* Pykälään ehdotetaan lisättäväksi viittaukset uusiin ehdotettuihin datavahingontekoon (3 a §) ja lievään datavahingontekoon (3 c §). Kyseessä on tekninen muutos, joka on seurausta datavahingonteon ja lievän datavahingonteon

erottamisesta itsenäisiksi kriminalisoinneikseen. Myös näiden rikosten osalta voidaan jättää ilmoitus tekemättä, syyte ajamatta tai rangaistus tuomitsematta, jos rikoksen tekijä on korvannut vahingon ja vahingonkorvaus harkintaan riittäväksi seuraamukseksi.

8 §. *Oikeushenkilön rangaistusvastuu.* Oikeushenkilön rangaistusvastuuta koskevaa pykälää ehdotetaan muutettavaksi teknisesti niin, että se vastaa muutosta, jolla datavahingonteko ja törkeä datavahingonteko erotetaan itsenäisiksi pykälikseen. Nykyisin oikeushenkilön rangaistusvastuu liittyy kumottavaksi ehdotettuun 1 §:n 2 momenttiin. Direktiivin 10 artikla edellyttää yleisperusteluissa selostetuin tavoin oikeushenkilön rangaistusvastuun ulottamista datavahingontekoon ja törkeään datavahingontekoon.

9 §. *Määritelmät.* Lukuun ehdotetaan yksityiskohtaisissa perusteluissa 2 artiklan osalta ja jäljempänä 38 luvun 13 §:n perusteluissa selostetuista syistä lisättäväksi uusi määritelmäsäännös, johon sisältyy 35 luvun ehdotetun 3 a ja 3 b pykälien osalta viittaus 38 luvun ehdotetussa uudessa 13 §:ssä oleviin tietojärjestelmän ja datan määritelmiin.

38 luku Tieto- ja viestintärikoksista

3 §. *Viestintäsalaisuuden loukkaus.* Pykälän 1 momentin 2 kohtaan ehdotetaan direktiivin vaatimusten täyttämiseksi lisättäväksi yksityiskohtaisissa perusteluissa 6 artiklan osalta selostetuin tavoin viittaus tietojärjestelmässä välitettävänä olevaan datasiirtoon. Direktiivi edellyttää kriminalisoimaan teknisin keinoin ja oikeudettomasti tapahtuvan tahallisen tietojen hankkimisen (interception) tietojärjestelmän sisäisestä tai tietojärjestelmien välisestä luottamuksellisesta datan siirrosta. Nykyisin pykälän 1 momentin 2 kohta kattaa tietojärjestelmien välisen luottamuksellisen datan siirron, mutta ei tietojärjestelmän sisäistä luottamuksellista datan siirtoa. Pykälän 1 momentin 1 kohta kattaa vain tallennetun viestin ja senkin osalta teon täyttymisen edellytyksenä oleva suojauksen murtamista koskeva kriteeri on liian rajaava, jotta direktiivin vaatimukset täyttyisivät. Direktiivin vaatimusten ei kuitenkaan voi katsoa koskevan tallennettua viestiä. Ehdotetun muutoksen myötä lainsäädäntö vastaisi direktiivin vaatimuksia ja kattaisi esimerkiksi tilanteet, jossa hankitaan tieto tietojärjestelmän sisäisestä luottamuksellisesta datan siirrosta, esimerkiksi käyttäjän näppäimistöllä syöttämästä viestistä.

Viestintäsalaisuuden loukkauksen enimmäisrangaistus ehdotetaan direktiivin vaatimusten mukaisesti nostettavaksi kahteen vuoteen vankeutta nykyisestä yhdestä vuodesta.

6 §. *Törkeä tietoliikenteen häirintä.* Pykälään ehdotetaan yksityiskohtaisissa perusteluissa 9 artiklan osalta ja edellä törkeän datavahingonteon (35 luvun 3 b §) perusteluissa selostetuin tavoin lisättäväksi vastaavat bottiverkkojen käyttöä, järjestäytynyttä rikollisryhmää, vakavaa vahinkoa ja elintärkeää infrastruktuuria koskevat kvalifiointiperusteet kuin törkeään datavahingontekoon. Tietoliikenteen törkeän häirinnän enimmäisrangaistus ehdotetaan direktiivin 9 artiklan vaatimusten mukaisesti nostettavaksi neljästä viiteen vuoteen vankeutta.

7 a §. *Tietojärjestelmän häirintä.* Eri rikosten välisistä konkurrenssitilanteista johtuen tietojärjestelmän häirinnän toissijaisuuslauseke ehdotetaan kumottavaksi. Rangaistusasteikkomuutosten myötä saatettaisiin muuten päätyä epätarkoituksenmukaisiin soveltamistilanteisiin. Toissijaisuuslausekkeen poiston tarve liittyy muun muassa siihen, että datavahingonteon (RL 35 luvun 3 a §) enimmäisrangaistus olisi jatkossa sama kuin tietojärjestelmän häirinnässä. Eri rikosten välisiä konkurrenssitilanteita on selostettu yksityiskohtaisissa perusteluissa laitonta tunkeutumista tietojärjestelmään koskevan 3 artiklan yhteydessä.

7 b §. *Törkeä tietojärjestelmän häirintä.* Pykälään ehdotetaan yksityiskohtaisissa perusteluissa 9 artiklan osalta esitetyin tavoin lisättäväksi vastaavat bottiverkkoja, järjestäytynyttä rikollisryhmää ja elintärkeää infrastruktuuria koskevat kvalifiointiperusteet kuin edellä on ehdotettu törkeän datavahingonteon (35 luvun 3 b §) ja törkeän tietoliikenteen häirinnän osalta. Törkeä tietojärjestelmän häirintä sisältää jo nykyisin vakavaa vahinkoa koskevan kvalifiointiperusteen (”aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa”), jota vastaavaa kvalifiointiperustetta ehdotetaan törkeään datava-

hingontekoon ja törkeään tietoliikenteen häirintään.

Direktiivin 9 artiklan vaatimusten mukaisesti enimmäisrangaistus ehdotetaan nostettavaksi neljästä vuodesta viiteen vuoteen vankeutta.

8 §. *Tietomurto.* Pykälän toista momenttia ehdotetaan yksityiskohtaisissa perusteluissa 3 artiklan osalta selostetuin tavoin muutettavaksi niin, että se kattaa teknisin keinoin hankittavan pääsyn tietojärjestelmässä olevaan dataan tai tiedon hankkimisen tällaisesta datasta laajemmin kuin nykyisin. Nykyisin pykälän toinen momentti kattaa selon ottamisen tietojärjestelmässä olevasta tiedosta vain tilanteissa, joissa se tapahtuu teknisen erikoislaitteen avulla. Mainitulla nykyisellä 2 momentilla on pantu täytäntöön yleissopimuksen 3 artiklan viestintäsalaisuuden loukkausta koskeva määräys tietojärjestelmästä lähtevästä sähkömagneettisesta säteilystä. Vastaava velvoite sisältyy myös direktiivin 6 artiklaan.

Ehdotuksen mukaan tietomurrosta tuomittaisiin nykyisen teknisellä erikoislaitteen avulla tehtävän tekotavan lisäksi myös tilanteessa, jossa tietojärjestelmään tai sen osaan tunkeutumatta muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin otettaisiin oikeudettomasti selko 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta.

Ehdotettu 2 momentti on tekniikkaneutraali. Ehdotetun 2 momentin on siten tarkoitus kattaa muun muassa tilanteet, jossa dataa syöttämällä tietojärjestelmä saadaan toimimaan virheellisesti ja antamaan sen sisältämää tietoa (muun muassa SQL-injektio) sekä tilanteet, jossa tietojärjestelmässä olevasta tiedosta tai datasta otetaan selko haittaohjelman avulla, joka tietojärjestelmän haltija on esimerkiksi harhautettu asentamaan. Ehdotetun 2 momentin 2 kohdan täyttymisen kriteerit ja toiminnan ilmeinen vilpillisyys tulee arvioitavaksi tapauskohtaisesti. Selvää on, että käytännössä vahingossa tapahtuvaa tiedon saamista säännös ei kata. Tunnusmerkistö ei myös useinkaan täyttyisi, mikäli dataan pääsy ei edellyttäisi erityistä tietoteknistä osaamista tai tilanteessa, jossa dataa ei ole suojattu erityisellä turvajärjestelyllä. Vilpillisyyden tulisi myös olla ilmeistä. Näin ollen esimerkiksi tavanomaisen internetissä tapahtuvan asioinnin ja käyttämisen yhteydessä tapahtuva kokeileminen tai tiedon kysyminen ei kuuluisi kohdan soveltamisalaan. Kohdassa tarkoitetun vilpillisen toiminnan tulisi tekijän toimesta kohdistua suoraan komennettavaan tai käytettävään tietojärjestelmään. Jos teossa on kysymys tietojärjestelmän käyttämisestä, tulisi vilpillisyyden yleensä ilmetä välittömästi tietojärjestelmän rajapinnassa. Selvyyden vuoksi voidaan todeta, että esimerkiksi tietojärjestelmän käyttäminen Tor-verkon kautta taikka muiden käyttäjän yksityisyyden suojaa parantavien menettelyiden tai ohjelmistojen käyttö ei lähtökohtaisesti merkitsisi vilpillisyyttä.

Vilpillisyyden tulisi muutenkin kohdistua yleensä suoraan tietojärjestelmään taikka sen haltijaan tai ylläpitoon. Tietojärjestelmän käyttäjien erehdyttäminen tulisi yleensä arvioitavaksi muina rikoksina. Esimerkiksi cross site scripting -haavoittuvuuden (XSS) hyödyntäminen tai cross site request forgery -hyökkäys (CSRF) eivät yleensä myöskään merkitsisi selon ottamista tietojärjestelmässä olevasta tiedosta tai datasta, joten ne tulisivat arvioitavaksi tietomurron asemesta tapauskohtaisesti esimerkiksi vaaran aiheuttamisena tietojenkäsittelylle, luvattomana käyttönä, datavahingontekona, petoksena tai maksuvälinepetoksena.

Pykälän 2 momentissa tarkoitettu oikeudettomuus liittyy tietojärjestelmän käyttöön. Pelkästään se, että tiedot olisivat jollain muulla tavalla saatavilla, esimerkiksi siksi, että ne ovat julkisia, ei vielä tee käytöstä oikeutettua.

Tietomurtoa koskevan pykälän 1 momenttiin ehdotetaan lisäksi lisättäväksi sanan ”tieto” lisäksi sana ”data”, sillä datan käsite kuvaa kattavimmin pykälässä säänneltäväksi tarkoitettua seikkaa. Myös direktiivissä käytetään sanaa data, ja datan käsite ehdotetaan direktiivin edellyttämin tavoin määriteltäväksi. Pykälän 1 momentti ei tietojärjestelmän määritelmän myötä kuitenkaan merkitse yleistä salauksen purkamisen kriminalisointia. Esimerkiksi salauksen purku ei ole osa mainitun teon tunnusmerkistöä. Pykälän 1 momentti koskee kuitenkin 13 pykälän

määritelmäsäännöksen nojalla myös ”dataan tunkeutumista” direktiivin teknisten vaatimusten täyttämiseksi. Pykälän 1 momenttiin sisällytettävän sanan ”data” on tarkoitus selventää myös sitä, että asianomistajana voi olla myös datan haltija eikä vain laitteen omistaja.

Tietomurron enimmäisrangaistus ehdotetaan direktiivin 9 artiklan vaatimusten mukaisesti nostettavaksi yhdestä vuodesta kahteen vuoteen vankeutta.

8 a §. *Törkeä tietomurto.* Törkeän tietomurron enimmäisrangaistus on nykyisin kaksi vuotta vankeutta. Direktiivin edellyttämällä tavalla tietomurron perustunnusmerkistön enimmäisrangaistus on nostettava kahdeksi vuodeksi vankeutta. Tästä johtuen myös törkeän tietomurron enimmäisrangaistusta on korotettava. Esityksessä ehdotetaan uudeksi enimmäisrangaistukseksi kolmea vuotta vankeutta. Enimmäisrangaistuksen korottaminen on muutenkin perusteltua ottaen huomioon muiden vastaavan kaltaisten tietoverkkorikosten enimmäisrangaistustasojen ankaroituminen. Enimmäisrangaistuksen on kuitenkin perusteltua olla alempi kuin esimerkiksi törkeässä datavahingonteossa, törkeässä tietoliikenteen häirinnässä tai törkeässä tietojärjestelmän häirinnässä kuten nykyisinkin. Lisäksi matalampi enimmäisrangaistus on perusteltu, koska tietomurtoa koskeva kriminalisointi kattaa myös niin sanotusti urheilumielessä tehdyt oikeudettomat teot. Mikäli tietojärjestelmään tunkeutumisen jälkeen vahingoitetaan dataa, estetään tietojärjestelmän toimintaa tai estetään viestintää, voivat muut ja mahdollisesti ankarammin rangaistavat kriminalisoinnit tulla sovellettaviksi.

9 b §. *Identiteettivarkaus.* Lukuun ehdotetaan lisättäväksi uusi identiteettivarkautta koskeva pykälä. Ehdotusta on selostettu tarkemmin yksityiskohtaisissa perusteluissa 9 artiklan 5 kohdan yhteydessä. Ehdotuksen mukaan identiteettivarkaudesta tuomittaisiin se, joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee. Seuraamukseksi ehdotetaan sakkorangaistusta.

Ehdotettu 9 b § edellyttäisi ensinnäkin sitä, että identiteettitiedon käytön osalta tekijän tarkoituksena on ollut erehdyttää kolmatta osapuolta. Kyseinen kriteeri sisältyy myös direktiiviin. Erehdytetty voi olla myös henkilöiden luoma tai ylläpitämä tietojärjestelmä. Erehdyttämisen osalta olennaista on, että kolmatta erehdytetään nimenomaan henkilöllisyyden tai identiteetin osalta. Rangaistavuuden edellytyksenä olisi myös se, että henkilö toimii oikeudettomasti. Henkilö ei toimisi oikeudettomasti, jos hänellä on esimerkiksi oikeus käyttää kyseessä olevaa IP-osoitetta, taikka hän käyttäisi nimeään, joka on myös hänen omansa. Ehdotetussa kriminalisoinnissa edellytetään toisen henkilötietojen, tunnistamistietojen tai muun vastaavan yksilöivän tiedon käyttöä. Tarkoituksena on ollut kattaa kaikki tiedot, joiden perusteella kolmas osapuoli voi erehtyä luulemaan tiedon käyttäjää siksi, jota tieto koskee. Esimerkiksi henkilötiedolla tarkoitetaan henkilötietolain (523/1999) 3 §:n 1 kohdan mukaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. Tunnistamistiedoilla tarkoitetaan esimerkiksi pakkokeinolain (806/2011) 10 luvun 6 §:n mukaan tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkossa käsitellään viestin siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Tällaista tietoa on muun muassa IP-osoite. Mitkä tahansa irralliset tiedot eivät kuitenkaan tulisi kyseeseen, vaan oleellista on, että tiedot ovat tunnistamiseen liittyviä tai kytkeytyviä ja mahdollistavat henkilön tunnistamisen ja siten erehtymisen. Vaikka tieto sinänsä olisi henkilötietoa, se ei kuitenkaan olisi tässä tarkoitetussa tilanteessa merkityksellinen, ellei se esiintyisi sellaisessa yhteydessä tai sellaisen muun tiedon kanssa, joka mahdollistaisi tunnistamisen.

Pykälässä tarkoitettu ”toinen” voi olla myös oikeushenkilö. Vaikka henkilötiedoilla tarkoitetaan henkilötietolaissa tarkoitettua henkilöön tunnistettavissa olevaa luonnollisen henkilön henkilötietoa, ehdotetussa säännöksessä olevalla kirjauksella muusta yksi-

löivästä tiedosta on tarkoitettu kattaa myös esimerkiksi oikeushenkilön yksilöivät tiedot.

Selvää kuitenkin on, että rikos ei täyttyisi, jos toisen tietojen käyttö on niin vähäistä tai koskee kokonaisuudessa niin irrallista seikkaa tai on muuten sellaista, ettei erehtymisen vaaraa tosiasiassa ole. Erehtymisen vaaraa ei esimerkiksi olisi, jos toiminta olisi selkeästi tunnistettavissa satiiriksi.

Mikäli kyseeseen tulisi pseudonyymillä, kuten ”Matti Meikäläisenä” esiintyminen, on selvää, että välttämättä kyseisessä tilanteessa henkilö ei käytä omaa nimeään ja kyseessä on varsin todennäköisesti myös jonkun muun henkilön nimi. Teko ei kuitenkaan ole rangaistava, jos erehdyttämistarkoitus puuttuu tai kyseessä on pikemminkin tarkoitus esittää jokin kommentti anonyymisti. Tunnusmerkistön täyttymisen kannalta oleellista on myös se, että kolmatta on tarkoitus erehdyttää luulemaan tietojen käyttäjää tietyksi toiseksi tai toisiksi henkilöiksi. Oleellista rangaistusvastuun kannalta on aiemmin esitetyin tavoin myös sen arviointi, onko konkreettisessa tilanteessa erehtymisen vaaraa.

Pykälässä tarkoitettu henkilötietojen käyttäminen ei myöskään koskisi valmisteluluonteista henkilötietojen käsittelyä.

Lisäksi teon on tullut aiheuttaa taloudellista vahinkoa tai muuta vähäistä suurempaa haittaa. Taloudellista vahinkoa voi syntyä esimerkiksi selvittelykuluina tilanteen korjaamiseksi. Vähäisiä tilanteita koskeva rajoitus koskee vain muita kuin taloudellisen vahingon tilanteita eli haittaa. Käytännössä haitta on osin päällekkäinen taloudellisen vahingon edellytyksen kanssa, mutta kattaa myös tilanteet, joissa ei olisi syntynyt suoranaista taloudellista vahinkoa. Tällaista haittaa voisi syntyä esimerkiksi tilanteissa, joissa asian selvittäminen ja oikaiseminen vaatii paljon vaivannäköä tai ei onnistu lainkaan. Esimerkiksi tilanteessa, jossa toisen henkilötiedoilla on tehty petoksia, saattaa tilanteen ja aiheettomien laskujen selvittäminen vaatia huomattavaa vaivannäköä siltä, jonka henkilötietoja on käytetty. Haittaan liittyy myös sen suojaaminen, että henkilöllä on oikeus omissa nimissään käyttää sananvapauttaan. Tällainen tilanne saattaisi joissakin tapauksissa olla käsillä esimerkiksi silloin, kun internetin sosiaaliseen mediaan on luotu valeprofiili toisen henkilötiedoilla. Joissakin tapauksissa tällaisen profiilin poistaminen saattaa olla vaikeaa. Lisäksi tilanne saattaa edellyttää yhteydenottoja lukuisiin henkilöihin, jotka ovat kuvitelleet kommunikoivansa sen henkilön kanssa, jota identiteettitieto koskee. Nimenomaan internetissä tapahtuvien tekojen osalta korostuu tilanne, jossa internetiin ladattujen tietojen saaminen poistetuksi on haasteellista ja aiheuttaa haittaa. Toisaalta yksittäisen ja onnistuneen reklamaatiosähköpostin lähettäminen ei yleensä aiheuttaisi vähäistä suurempaa haittaa. Jos erehdyttämiset muodostaisivat motivaatioperustaltaan yhtenäisen ajallisen ja asiallisen kokonaisuuden, jossa on käytetty saman henkilön identiteettitietoja, teko katsottaisiin vain yhdeksi identiteettivarkaudeksi, vaikka sillä olisikin erehdytetty useita kolmansia osapuolia. Tämä merkitsee sitä, että vaikka henkilö joutuisikin esimerkiksi lähettämään vain yhden reklamaatiosähköpostin kullekin kolmannelle erehdytetylle taholle, ei kyse enää olisi edellä mainitusta yksittäisestä onnistuneesta reklamaatiosta. Yksittäinenkin reklamaatio voi toisaalta olosuhteet huomioiden aiheuttaa vähäistä suurempaa haittaa, jos esimerkiksi henkilö joutuu useiden yksittäisten identiteettivarkauksien kohteeksi useiden tekijöiden toimesta. Asia on näin ollen arvioitava tapauskohtaisesti.

Rikoksen tutkimisessa tulevat sovellettaviksi kulloinkin kyseeseen tulevat tutkinta- ja pakkokeinot. Esimerkiksi sanavapauden käyttämisestä joukkoviestinnässä säädetyn lain (460/2003) 17 §:n mukaisesti on mahdollisuus selvittää verkkoviestin tunnistamistiedot, jos on todennäköisiä syitä epäillä viestin olevan sisällöltään sellainen, että sen toimittaminen yleisön saataville on säädetty rangaistavaksi. Tällainen tilanne voi olla kyseessä esimerkiksi silloin, kun ehdotetussa pykälässä tarkoitettu identiteettivarkaus tapahtuisi blogikirjoittelun muodossa. Identiteettivarkauden tutkinnassa tulee sovellettavaksi myös pakkokeinolain 10 luvun 7 §:ssä tarkoitettu teleosoitteen tai telepäätelaitteen haltijan suostumuksella tapahtuvaan televalvonta silloin kun teko on tehty teleosoitetta tai telepäätelaitetta käyttäen. Myös poliisilain 4 luvun 3 §:ssä tarkoitetut tiedonsaantikeinot ovat käytettävissä identiteettivarkauden tutkinnassa. Mainitun pykälän 2 momentin mu-

kaan poliisilla on yksittäistapauksessa oikeus pyynnöstä saada teleyritykseltä ja yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen poliisille kuuluvan tehtävän suorittamiseksi.

On kuitenkin huomattava, että teko voi konkreettisesta tekotavasta riippuen täyttää jonkin muun rikoksen, kuten kunnianloukkauksen tai yksityiselämää loukkaavan tiedon levittämisen, jolloin niihin sovellettavat pakkokeinot tulevat kyseeseen. Edelleen on syytä huomioida, että ehdotetussa pykälässä tarkoitettu identiteettivarkaus voi usein tapahtua jonkin muun vakavamman rikoksen kuten petoksen yhteydessä. Tällöin petoksen tutkinnassa ovat käytettävissä sen tutkinnassa mahdolliset pakkokeinot. Tältä osin merkityksellistä onkin se ehdotuksen tavoite, jonka mukaan identiteettivarkautta koskevalla kriminalisoinnilla on tarkoitus selkeyttää identiteettivarkauden uhrin asianomistaja-asemaa esimerkiksi petosrikoksissa.

10 §. *Syyteoikeus.* Pykälään lisättäisiin uusi 4 momentti, jonka mukaan syyttäjä saa nostaa syytteen identiteettivarkaudesta vain, jos asianomistaja ilmoittaa rikoksen syytteeseen pantavaksi. Uudessa ehdotetussa identiteettivarkautta koskevassa 9 b §:ssä suojataan ennen kaikkea sen henkilön identiteetin loukkaamattomuutta, jonka henkilötietoja on käytetty. Mikäli asianomistaja ei koe identiteettiään loukatun tai muusta syystä ei toivo asian käsittelyä ja syytteen nostamista, ei ole perusteltua ryhtyä tähän vastoin asianomistajan tahtoa. On mahdollista, että suhteellisen vähäisissä tapauksissa asianomistaja saattaisi myös kokea syyteasian käsittelyn enemmän haittaa aiheuttavaksi kuin itse rikos.

11 §. *Menettämisseuraamus.* Pykälässä oleva viittaus 8 a §:ssä tarkoitettuun suojauksen purkujärjestelmään muutettaisiin viittamaan 8 b §:ään. Ehdotus ei liity direktiivin täytäntöönpanoon. Kyseessä on kirjoitusvirheen korjaus, sillä nykyisin 8 b §:ssä oleva suojauksen purkujärjestelmärikos on aiemmin sijainnut 8 a §:ssä. Aiemman pykälien numerointia koskevan muutoksen yhteydessä on jäänyt muutamatta 11 §:ssä oleva viittaus.

13 §. *Määritelmät.* Lukuun lisättäisiin uusi pykälä, joka sisältäisi yksityiskohtaisissa perusteluissa 2 artiklan osalta selostetuin tavoin tietojärjestelmän ja datan määritelmät. Nyt ehdotettuun pykälään viitattaisiin myös 34 ja 35 luvussa edellä esitetyin tavoin.

Ehdotetun pykälän 1 momenttiin sisällytettäisiin direktiivin 2 artiklan a kohdassa oleva tietojärjestelmän määritelmä niiden rikosten osalta, jotka vastaavat tässä direktiivissä tarkoitettuja kriminalisointivelvoitteita. Määritelmä olisi avoin ja tekniikkaneutraali siten, että tietojärjestelmän käsitettä ei viitattujen rikoslain säännösten osaltakaan rajattaisi direktiivissä tarkoitettuun määritelmään, vaan tietojärjestelmällä tarkoitettaisiin myös sitä mitä direktiivissä tarkoitetaan tietojärjestelmällä ja siinä olevalla datalla. Näin täytettäisiin direktiivin vähimmäisvaatimukset. Määritelmän sisällyttäminen pykälään on olennaista, sillä direktiivissä tietojärjestelmällä tarkoitetaan myös tietojärjestelmässä olevaa dataa. Koska kyseessä on vain direktiivin velvoitteiden täytäntöönpanon varmistamiseksi säädettävä avoin määritelmä, esityksessä ehdotetaan, että se kattaa vain ne kriminalisoinnit, joiden on tarkoitettu kattavan direktiivin vähimmäisvelvoitteet.

Ehdotetun 1 momentin mukaan sovellettaessa 3, 6, 7 a, 7 b ja 8 §:ää, tietojärjestelmällä tarkoitetaan myös tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta annetun Euroopan parlamentin ja neuvoston direktiivin 2013/40/EU 2 artiklan a kohdassa tarkoitettua:

1) laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten; sekä

2) dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään sen tai niiden toimintaa, käyttöä, suojausta tai huoltoa varten.

Selvyyden vuoksi ja datan määritelmän ollessa edellä a kohdassa todetun mukaisesti kiinteässä yhteydessä tietojärjestelmän määritelmään, esityksessä ehdotetaan, että 2 momenttiin otetaan tietojärjestelmän käsitettä vastaavasti avoin direktiivin 2 artiklan b kohdan määritelmää vastaava määritelmä, jonka mukaan datalla tarkoitetaan myös direktiivissä tarkoitettua dataa niiden rikosten

osalta, jotka vastaavat direktiivissä tarkoitettuja kriminalisointivelvoitteita. Näin täytettäisiin direktiivin vähimmäisvaatimukset. Koska kyseessä on vain direktiivin velvoitteiden täytäntöönpanon varmistamiseksi säädettävä avoin määritelmä, esityksessä ehdotetaan, että se kattaa vain ne kriminalisoinnit, joiden on tarkoitettu kattavan direktiivin vähimmäisvelvoitteet.

Ehdotetun 2 momentin mukaan sovellettaessa 3, 7 a ja 8 §:ää datalla tarkoitetaan myös tietoverkkorikosdirektiivin 2013/40/EU 2 artiklan b kohdassa tarkoitettua:

1) sellaisessa muodossa olevien tosiseikkojen, tietojen, tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä; sekä

2) ohjelmaa, jonka avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon.

2.2 Pakkokeinolaki

3 §. *Telekuuntelu ja sen edellytykset.* Koska törkeä datavahingonteko erotettaisiin törkeästä vahingonteosta erilliseksi rikosnimikkeeksi, tulisi telekuuntelua ja sen edellytyksiä koskevaan pakkokeinolain 10 luvun 3 §:n 12 kohtaan tehdä tätä koskeva tarkistus. Kohdassa on aikaisemmin mainittu törkeä vahingonteko. Säännöstä tarkistettaisiin siten, että telekuunteluun voitaisiin antaa lupa myös silloin, jos epäiltyä on syytä epäillä törkeästä datavahingonteosta.

6 §. *Televalvonta ja sen edellytykset.* Pykälään tehtäisiin ehdotetuista rikoslain muutoksista johtuvat teknisluonteiset tarkistukset. Nykyisen pykälän 2 momentin 3 kohdan mukaan televalvonta on mahdollista teleosoitetta tai telepäätelaitetta käyttäen tehdystä, automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta luvattomasta käytöstä, vahingonteosta, viestintäsalaisuuden loukkauksesta tai tietomurrosta. Mainitut rikokset on ollut tarpeen listata 3 kohdassa, sillä niiden osalta televalvontaa ei nykyisin voi käyttää momentin 2 kohdan mukaisesti, sillä 2 kohdassa edellytetään kahden vuoden enimmäisrangaistusta.

Momentin 2 kohdan mukaan televalvonta on mahdollista teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Nyt ehdotetuilla rikoslain muutoksilla tietomurron ja viestintäsalaisuuden loukkauksen enimmäisrangaistus nousisi kahteen vuoteen vankeutta, jolloin 2 kohtaa voidaan soveltaa. Tämän vuoksi tietomurto ja viestintäsalaisuuden loukkaus voidaan poistaa 3 kohdan listasta. Kohdassa kolme tarkoitetulla tekotavalla tehty vahingonteko voidaan myös poistaa 3 kohdan listasta, sillä esityksessä tarkoitetuilla rikoslain muutoksilla niin sanottu ”tietovahingonteko” erotetaan rikoslain 35 luvun 1 §:n vahingontekoa koskevasta kriminalisoinnista itsenäiseksi datavahingontekoa koskevaksi kriminalisoinniksi rikoslain 35 luvun 3 a §:ään. Vastaavasti vahingontekoa koskevan 1 §:n 2 ja 3 momentti ehdotetaan kumottaviksi. Uuden datavahingontekoa koskevan teon enimmäisrangaistus on kaksi vuotta vankeutta, joten pakkokeinolain 10 luvun 6 §:n 2 momentin 2 kohta voi tulla sovellettavaksi.

2.3 Poliisilaki

8 §. *Televalvonta ja sen edellytykset.* Pykälään tehtäisiin vastaavat teknisluonteiset tarkistukset kuin pakkokeinolakiin johtuen ehdotetuista rikoslain muutoksista. Nykyisen pykälän 2 momentin 3 kohdan mukaan televalvonta on mahdollista teleosoitetta tai telepäätelaitetta käyttäen tehdystä, automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta luvattomasta käytöstä, vahingonteosta, viestintäsalaisuuden loukkauksesta tai tietomurrosta. Mainitut rikokset on ollut tarpeen listata 3 kohdassa, sillä niiden osalta televalvontaa ei nykyisin voi käyttää momentin 2 kohdan mukaisesti, sillä 2 kohdassa edellytetään kahden vuoden enimmäisrangaistusta.

Momentin 2 kohdan mukaan televalvonta on mahdollista teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Nyt ehdotetuilla rikoslain muutoksilla tietomurron ja viestintäsalaisuuden loukkauksen enimmäisrangaistus nousisi kahteen vuoteen vankeutta, jolloin 2 kohtaa voidaan soveltaa. Tämän vuoksi tietomurto ja viestintäsalaisuuden loukkaus voidaan poistaa 3 kohdan listasta. Kohdassa kolme tarkoitetulla tekotavalla tehty vahingonteko voi-

daan myös poistaa 3 kohdan listasta, sillä esityksessä tarkoitetuilla rikoslain muutoksilla niin sanottu ”tietovahingonteko” erotetaan rikoslain 35 luvun 1 §:n vahingontekoa koskevasta kriminalisoinnista itsenäiseksi datavahingontekoa koskevaksi kriminalisoinniksi rikoslain 35 luvun 3 a §:ään. Vastaavasti vahingontekoa koskevan 1 §:n 2 ja 3 momentti ehdotetaan kumottaviksi. Uuden datavahingontekoa koskevan teon enimmäisrangaistus on kaksi vuotta vankeutta, joten poliisilain 5 luvun 8 §:n 2 momentin 2 kohta voi tulla sovellettavaksi.

2.4 Sotilasoikeudenkäyntilaki

Sotilasoikeudenkäyntilain (326/1983) 2 §:n 2 momentin mukaan sotilasoikeudenkäyntiasiana käsitellään syyte sotilasta vastaan teosta, josta säädetään rangaistus rikoslain (39/1889) 21 luvun 1—3 tai 5—14 §:ssä, 25 luvun 7 tai 8 §:ssä, 28, 31—33 tai 35 luvussa, 36 luvun 1—3 §:ssä, 37 luvun 8—10 §:ssä, 38 luvun 1—7, 7 a, 7 b, 8 tai 8 a §:ssä taikka 40 luvun 1—3 tai 5 §:ssä. Edellytyksenä on, että teko on kohdistunut puolustusvoimiin tai toiseen sotilaaseen. Sotilasoikeudenkäyntiasiana käsitellään niin ikään syyte teosta, josta säädetään rangaistus asevelvollisuuslain (1438/2007) 118 §:ssä. Esityksessä rikoslain 38 luvun 9 b §:ään ehdotettu identiteettivarkaus voisi tulla tutkittavaksi rikosnimikkeeksi esimerkiksi palvelusrikosten tai omaisuus- tai väärennysrikosten yhteydessä. Esityksessä todetuin tavoin, identiteettivarkaus saattanee usein tapahtua osana muuta rangaistavaa käyttäytymistä. Tällöin ei voida resurssien käytön osalta pitää perusteltuna sitä, että puolustusvoimat joutuisi siirtämään identiteettivarkautta koskevan rikosnimikkeen osalta esitutkinnan poliisille. Edellä mainitusta syystä ehdotettu identiteettivarkautta koskeva kriminasiointi lisättäisiin sotilasoikeudenkäyntilain 2 §:n 2 momentin luetteloon.

3 Voimaantulo

Lait ehdotetaan tuleviksi voimaan 4 päivänä syyskuuta 2015, jolloin direktiivi on pantava täytäntöön.

4 Suhde perustuslakiin ja säätämisjärjestys

Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Useat esityksessä tarkoitetut tietoverkkorikoksia koskevat kriminalisoinnit ovat säännöksen kannalta merkityksellisiä ja laajentavat välillisesti mainitussa 1 momentissa tarkoitetun yksityiselämän suojaa.

Perustuslain 10 §:n 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Säännös on muotoiltu väline- ja tekniikkaneutraaliksi, ja säännöksellä turvataan yleisesti kaikenlaisen luottamuksellisen viestinnän salaisuutta (HE 309/1993 vp, s. 53). Esityksessä ehdotetut muutokset rikoslain 38 luvun 3 §:ssä tarkoitetun viestintäsalaisuuden loukkauksen osalta laajentavat luottamuksellisen viestinnän suojaa.

Perustuslain 10 §:n 3 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa. Ehdotettu telekuuntelua koskeva pakkokeinolain 10 luvun 3 §:n 2 momentin 12 kohdan tarkistus ei ole asiallinen muutos. Muutos on tarpeen sen vuoksi, että törkeästä datavahingonteosta säädettäisiin itsenäinen rikos ja se eriytettäisiin nykyisestä törkeästä vahingonteosta, jonka osalta telekuuntelu on mahdollista jo voimassaolevan lain mukaan. Tietoverkossa tehtyjen vakavien rikosten tutkinnassa telepakkokeinojen merkitys on korostunut, ja törkeän datavahingonteon voidaan katsoa olevan vastaavalla tavalla yksilön tai yhteiskunnan turvallisuutta vaarantava rikos kuin törkeä vahingonteko. Perustuslakivaliokunnan (PeVL 36/2002 vp, s. 4) mukaan perustuslain 10 §:n 3 momentissa tarkoitetun rajoituksen välttämättömyyden kannalta on keskeistä, että telekuuntelumahdollisuus kytkeytyy ainoastaan vakaviin rikoksiin. Törkeää datavahingontekoa voidaan pitää tällaisena vakavana rikoksena. Törkeän datavahingonteon enimmäisrangaistus on viisi vuotta vankeutta, joten se vakavuustasoltaan vastaa tai on ankarammin rangaistava kuin monet muut rikokset, joiden selvittämisessä nykyisin voi-

daan käyttää telekuuntelua pakkokeinolain 10 luvun 3 §:n 2 momentin mukaisesti.

Televalvontaan liittyvät pakkokeinolain 10 luvun 6 §:n ja poliisilain 5 luvun 8 §:n ehdotetut muutokset eivät ole asiallisia muutoksia. Esityksessä ehdotettujen rikoslain muutosten ja rangaistustasojen korottamisen johdosta teleosoitetta tai telepäätelaitetta käyttäen tehtyä automaattiseen tietojenkäsittelyjärjestelmään kohdistunutta vahingontekoa, viestintäsalaisuuden loukkausta ja tietomurtoa ei ole enää tarpeen nimenomaisesti listata televalvonnan perusterikoksena mainituissa pykälissä.

Tietojärjestelmiä ja tietoverkkoja koskevat ehdotetut rangaistussäännökset, erityisesti rikoslain 38 luvun 6 §:ssä tarkoitettu törkeä tietoliikenteen häirintä ja 7 b §:ssä tarkoitettu törkeä tietojärjestelmän häirintä turvaavat välillisesti myös perustuslain 12 §:ssä turvatun sananvapauden toteutumista. Säännöksen mukaan sananvapauteen sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Verkkoviestinnän teknisten erityispiirteiden vuoksi viestintäjärjestelmien häiriötöntä toimintaa on tarpeen edistää myös lainsäädännöllä (PeVL 9/2004 vp).

Myös ehdotettu uusi rikoslain 38 luvun 9 b §:ssä tarkoitettu identiteettivarkautta koskeva kriminalisointi on merkityksellinen perustuslain 12 §:ssä turvatun sananvapauden kannalta. Rangaistussäännös kaventaa vähäisessä määrin sananvapautta, mutta kriminalisoinnilla suojataan samalla perustuslain 10 §:ssä turvattua oikeutta yksityiselämään. Oikeus henkilökohtaiseen identiteettiin liittyy perustuslaissa turvatun yksityiselämän suojan piiriin (ks. PeVL 25/2006 vp, s. 2, PeVL 16/2006 vp, s. 3, PeVL 59/2002 vp, s. 3). Ehdotettu kriminalisointi on oikeasuhtainen, se ei kohdistu sananvapauden ydinalueeseen eikä se merkitse ennakollista puuttumista sanavapauden käyttöön.

Lakiehdotukset voidaan hallituksen käsityksen mukaan hyväksyä tavallisen lain säätämisjärjestyksessä.

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

Lakiehdotukset

1.

Laki

rikoslain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan rikoslain (39/1889) 35 luvun 1 §:n 2 ja 3 momentti, sellaisina kuin ne ovat, 1 §:n 2 momentti laissa 769/1990 ja 3 momentti laissa 540/2007,

muutetaan 34 luvun 9 a §, 35 luvun 2, 6—8 §, 38 luvun 3 §, 6 §:n 1 momentin loppukappale, 7 a, 7 b, 8, 8 a ja 11 §,

sellaisina kuin ne ovat, 34 luvun 9 a §, 35 luvun 8 § sekä 38 luvun 7 a, 7 b ja 8 a § laissa 540/2007, 35 luvun 2 § laeissa 769/1990, 17/2003 ja 540/2007, 35 luvun 6 § laissa 441/2011, 35 luvun 7 § laissa 769/1990, 38 luvun 3 § laissa 531/2000, 38 luvun 6 §:n 1 momentin loppukappale ja 8 § laissa 578/1995 ja 38 luvun 11 § laissa 1118/2001, sekä

lisätään 34 lukuun uusi 14 §, 35 lukuun uusi 3 a—3 c ja 9 §, 38 luvun 6 §:n 1 momenttiin, sellaisena kuin se on laissa 578/1995, uusi 3—6 kohta, 38 lukuun uusi 9 b §, 38 luvun 10 §:ään, sellaisena kuin se on laissa 441/2011, uusi 4 momentti, sekä 38 lukuun uusi 13 § seuraavasti:

34 luku

Yleisvaarallisista rikoksista

9 a §

Vaaran aiheuttaminen tietojenkäsittelylle

Joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle

1) tuo maahan, hankkii käyttöön, valmistaa, myy tai muuten levittää taikka asettaa saataville

a) sellaisen laitteen tai tietokoneohjelman taikka ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa taikka murtamaan tai purkamaan sähköisen viestinnän teknisen suojauksen tai tietojärjestelmän suojauksen taikka

b) tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon taikka

2) levittää tai asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseksi,

on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

14 §

Määritelmät

Mitä 38 luvun 13 §:n 1 momentissa säädetään tietojärjestelmän määritelmästä, sovelletaan myös 9 a ja 9 b §:ään.

35 luku

Vahingonteosta

2 §

Törkeä vahingonteko

Jos vahingonteolla aiheutetaan

1) erittäin suurta taloudellista vahinkoa,

2) rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa vahinkoa tai

3) historiallisesti tai sivistyksellisesti erityisen arvokkaalle omaisuudelle huomattavaa vahinkoa

ja vahingonteko on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä vahingonteosta* vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

Yritys on rangaistava.

3 a §

Datavahingonteko

Joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee, vahingoittaa, muuttaa, saattaa käyttökelvottomaksi tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen taikka tietojärjestelmässä olevan datan, on tuomittava *datavahingonteosta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yritys on rangaistava.

3 b §

Törkeä datavahingonteko

Jos datavahingonteossa

1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa,

2) rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa,

3) rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa, tai

4) rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon

ja datavahingonteko on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä datavahingonteosta* vankeuteen vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi.

Yritys on rangaistava.

3 c §

Lievä datavahingonteko

Jos datavahingonteko, huomioon ottaen vahingon vähäisyys tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on tuomittava *lievästä datavahingonteosta* sakkoon.

6 §

Syyteoikeus

Jos 1, 3, 3 a tai 3 c §:ssä tarkoitetun rikoksen kohteena on ollut ainoastaan yksityinen omaisuus, syyttäjä saa nostaa syytteen vain, jos asianomistaja ilmoittaa rikoksen syytteeseen pantavaksi.

7 §

Toimenpiteistä luopuminen

Vahingonteosta, datavahingonteosta, lievästä vahingonteosta ja lievästä datavahingonteosta voidaan jättää ilmoitus tekemättä, syyte ajamatta tai rangaistus tuomitsematta, jos rikoksen tekijä on korvannut vahingon ja vahingonkorvaus harkitaan riittäväksi seuraamukseksi.

8 §

Oikeushenkilön rangaistusvastuu

Datavahingontekoon ja törkeään datavahingontekoon sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.

9 §

Määritelmät

Mitä 38 luvun 13 §:n 1 momentissa säädetään tietojärjestelmän määritelmästä, sovelletaan myös 3 a ja 3 b §:ään.

Mitä 38 luvun 13 §:n 2 momentissa säädetään datan määritelmästä, sovelletaan myös 3 a §:ään.

38 luku

Tieto- ja viestintärikoksista

3 §

Viestintäsalaisuuden loukkaus

Joka oikeudettomasti

1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka

2) hankkii tiedon televerkossa tai tietojärjestelmässä välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta,

on tuomittava *viestintäsalaisuuden loukkauksesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yritys on rangaistava.

6 §

Törkeä tietoliikenteen häirintä

Jos tietoliikenteen häirinnässä

— — — — — — — — — — — — — — —

3) rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa,

4) rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa,

5) rikoksella aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai

6) rikos kohdistuu laitteeseen, tietojärjestelmään tai viestintään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon

ja tietoliikenteen häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä tietoliikenteen häirinnästä* vankeuteen vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi.

— — — — — — — — — — — — — — —

7 a §

Tietojärjestelmän häirintä

Joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, on tuomittava *tietojärjestelmän häirinnästä* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yritys on rangaistava.

7 b §

Törkeä tietojärjestelmän häirintä

Jos tietojärjestelmän häirinnässä

1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa,

2) rikos tehdään erityisen suunnitelmallisesti,

3) rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa,

4) rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai

5) rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon

ja tietojärjestelmän häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä

on tuomittava *törkeästä tietojärjestelmän häirinnästä* vankeuteen vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi.

Yritys on rangaistava.

8 §

Tietomurto

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta

1) teknisen erikoislaitteen avulla tai

2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin

oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta.

Yritys on rangaistava.

Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.

8 a §

Törkeä tietomurto

Jos tietomurto tehdään

1) osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai

2) erityisen suunnitelmallisesti

ja tietomurto on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä tietomurrosta* sakkoon tai vankeuteen enintään kolmeksi vuodeksi.

Yritys on rangaistava.

9 b §

Identiteettivarkaus

Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.

10 §

Syyteoikeus

— — — — — — — — — — — — — — —

Syyttäjä saa nostaa syytteen identiteettivarkaudesta vain, jos asianomistaja ilmoittaa rikoksen syytteeseen pantavaksi.

11 §

Menettämisseuraamus

Edellä 8 b §:ssä tarkoitettu suojauksen purkujärjestelmä on tuomittava valtiolle menetetyksi.

13 §

Määritelmät

Sovellettaessa 3, 6, 7 a, 7 b ja 8 §:ää tietojärjestelmällä tarkoitetaan myös tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta annetun Euroopan parlamentin ja neuvoston direktiivin 2013/40/EU, jäljempänä *tietoverkkorikosdirektiivi*, 2 artiklan a kohdassa tarkoitettua:

1) laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten; sekä

2) dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään

sen tai niiden toimintaa, käyttöä, suojausta tai huoltoa varten.

Sovellettaessa 3, 7 a ja 8 §:ää datalla tarkoitetaan myös tietoverkkorikosdirektiivin 2 artiklan b kohdassa tarkoitettua:

1) sellaisessa muodossa olevien tosiseikkojen, tietojen, tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä; sekä

2) ohjelmaa, jonka avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon.

Tämä laki tulee voimaan päivänä kuuta 20 .

2.

Laki

pakkokeinolain 10 luvun 3 ja 6 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan pakkokeinolain (806/2011) 10 luvun 3 §:n 2 momentin 12 kohta ja 6 §:n 2 momentti, sellaisina kuin ne ovat laissa 1146/2013, seuraavasti:

10 luku

Salaiset pakkokeinot

3 §

Telekuuntelu ja sen edellytykset

Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa telekuuntelua rikoksesta epäillyn hallussa olevan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:

— — — — — — — — — — — — — — —

12) törkeästä vahingonteosta tai törkeästä datavahingonteosta;

— — — — — — — — — — — — — — —

6 §

Televalvonta ja sen edellytykset

— — — — — — — — — — — — — — —

Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa televalvontaa rikoksesta epäillyn hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:

1) rikoksesta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;

2) teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;

3) teleosoitetta tai telepäätelaitetta käyttäen tehdystä, automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta luvattomasta käytöstä;

4) seksikaupan kohteena olevan henkilön hyväksikäytöstä, lapsen houkuttelemisesta seksuaalisiin tarkoituksiin tai parituksesta;

5) huumausainerikoksesta;

6) terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta;

7) törkeästä tulliselvitysrikoksesta;

8) törkeästä laittoman saaliin kätkemisestä;

9) panttivangin ottamisen valmistelusta; taikka

10) törkeän ryöstön valmistelusta.

— — — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20 .

3.

Laki

poliisilain 5 luvun 8 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan poliisilain (872/2011) 5 luvun 8 §:n 2 momentti, sellaisena kuin se on laissa 1168/2013, seuraavasti:

5 luku

Salaiset tiedonhankintakeinot

8 §

Televalvonta ja sen edellytykset

— — — — — — — — — — — — — — —

Poliisille voidaan rikoksen estämiseksi antaa lupa kohdistaa televalvontaa henkilön hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos henkilön lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän:

1) rikokseen, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;

2) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn rikokseen, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;

3) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn, automaattiseen tietojenkäsittelyjärjestelmään kohdistuvaan luvattomaan käyttöön;

4) seksikaupan kohteena olevan henkilön hyväksikäyttöön, lapsen houkuttelemiseen seksuaalisiin tarkoituksiin tai paritukseen;

5) huumausainerikokseen;

6) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun; taikka

7) törkeään tulliselvitysrikokseen.

— — — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20 .

4.

Laki

sotilasoikeudenkäyntilain 2 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sotilasoikeudenkäyntilain (326/1983) 2 §:n 2 momentti, sellaisena kuin se on laissa 1442/2007, seuraavasti:

2 §

— — — — — — — — — — — — — — —

Sotilasoikeudenkäyntiasiana käsitellään myös syyte sotilasta vastaan teosta, josta säädetään rangaistus rikoslain (39/1889) 21 luvun 1—3 tai 5—14 §:ssä, 25 luvun 7 tai 8 §:ssä, 28, 31—33 tai 35 luvussa, 36 luvun 1—3 §:ssä, 37 luvun 8—10 §:ssä, 38 luvun 1—7, 7 a, 7 b, 8, 8 a tai 9 b §:ssä taikka 40 luvun 1—3 tai 5 §:ssä. Edellytyksenä on, että teko on kohdistunut puolustusvoimiin tai toiseen sotilaaseen. Sotilasoikeudenkäyntiasiana käsitellään niin ikään syyte teosta, josta säädetään rangaistus asevelvollisuuslain (1438/2007) 118 §:ssä.

— — — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä 13 päivänä marraskuuta 2014

Pääministeri

ALEXANDER STUBB

Oikeusministeri *Anna-Maja Henriksson*

Liite
Rinnakkaistekstit

1.

Laki

rikoslain muuttamisesta

Eduskunnan päätöksen mukaisesti
kumotaan rikoslain (39/1889) 35 luvun 1 §:n 2 ja 3 momentti, sellaisina kuin ne ovat, 1 §:n 2 momentti laissa 769/1990 ja 3 momentti laissa 540/2007,
muutetaan 34 luvun 9 a §, 35 luvun 2, 6—8 §, 38 luvun 3 §, 6 §:n 1 momentin loppukappale, 7 a, 7 b, 8, 8 a ja 11 §,
sellaisina kuin ne ovat, 34 luvun 9 a §, 35 luvun 8 § sekä 38 luvun 7 a, 7 b ja 8 a § laissa 540/2007, 35 luvun 2 § laeissa 769/1990, 17/2003 ja 540/2007, 35 luvun 6 § laissa 441/2011, 35 luvun 7 § laissa 769/1990, 38 luvun 3 § laissa 531/2000, 38 luvun 6 §:n 1 momentin loppukappale ja 8 § laissa 578/1995 ja 38 luvun 11 § laissa 1118/2001, sekä
lisätään 34 lukuun uusi 14 §, 35 lukuun uusi 3 a—3 c ja 9 §, 38 luvun 6 §:n 1 momenttiin, sellaisena kuin se on laissa 578/1995, uusi 3—6 kohta, 38 lukuun uusi 9 b §, 38 luvun 10 §:ään, sellaisena kuin se on laissa 441/2011, uusi 4 momentti, sekä 38 lukuun uusi 13 § seuraavasti:

Voimassa oleva laki	*Ehdotus*
34 luku	
Yleisvaarallisista rikoksista	
9 a §	9 a §
Vaaran aiheuttaminen tietojenkäsittelylle	*Vaaran aiheuttaminen tietojenkäsittelylle*
Joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle	Joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle
1) tuo maahan, valmistaa, myy tai muuten levittää taikka asettaa saataville	1) tuo maahan, *hankkii käyttöön*, valmistaa, myy tai muuten levittää taikka asettaa saataville
a) sellaisen laitteen tai tietokoneohjelman taikka ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa taikka murtamaan tai purkamaan sähköisen viestinnän teknisen suojauksen tai tietojärjestelmän suojauksen taikka	a) sellaisen laitteen tai tietokoneohjelman taikka ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa taikka murtamaan tai purkamaan sähköisen viestinnän teknisen suojauksen tai tietojärjestelmän suojauksen taikka
b) tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon taikka	b) tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon taikka
2) levittää tai asettaa saataville ohjeen	

Voimassa oleva laki	*Ehdotus*
1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseksi, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, *vaaran aiheuttamisesta tietojenkäsittelylle* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.	2) levittää tai asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseksi, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, *vaaran aiheuttamisesta tietojenkäsittelylle* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
(uusi)	14 §
	Määritelmät
	Mitä 38 luvun 13 §:n 1 momentissa säädetään tietojärjestelmän määritelmästä, sovelletaan myös 9 a ja 9 b §:ään.

35 luku

Vahingonteosta

1 §	1 §
Vahingonteko	*Vahingonteko*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Vahingonteosta tuomitaan myös se, joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen.	(2 mom. kumotaan)
Edellä 2 momentissa tarkoitetun vahingonteon yritys on rangaistava.	(3 mom. kumotaan)
2 §	2 §
Törkeä vahingonteko	*Törkeä vahingonteko*
Jos *1)* vahingonteolla aiheutetaan a) erittäin suurta taloudellista vahinkoa, b) rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa vahinkoa, c) historiallisesti tai sivistyksellisesti erityisen arvokkaalle omaisuudelle huomattavaa vahinkoa *taikka* *2) edellä 1 §:n 2 momentissa tarkoitettu vahingonteko tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa*	Jos vahingonteolla aiheutetaan *1)* erittäin suurta taloudellista vahinkoa, *2)* rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa vahinkoa *tai* *3)* historiallisesti tai sivistyksellisesti erityisen arvokkaalle omaisuudelle huomattavaa vahinkoa

Voimassa oleva laki	*Ehdotus*
ja vahingonteko on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä vahingonteosta* vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi. Yritys on rangaistava.	ja vahingonteko on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä vahingonteosta* vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi. Yritys on rangaistava.
(uusi)	3 a § *Datavahingonteko* *Joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee, vahingoittaa, muuttaa, saattaa käyttökelvottomaksi tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen taikka tietojärjestelmässä olevan datan, on tuomittava **datavahingonteosta** sakkoon tai vankeuteen enintään kahdeksi vuodeksi.* *Yritys on rangaistava.*
(uusi)	3 b § *Törkeä datavahingonteko* *Jos datavahingonteossa* *1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa,* *2) rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa,* *3) rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa, tai* *4) rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon* *ja datavahingonteko on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava **törkeästä datavahingonteosta** vankeuteen vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi.* *Yritys on rangaistava.*

Voimassa oleva laki	*Ehdotus*
(uusi)	3 c §
	Lievä datavahingonteko
	Jos datavahingonteko, huomioon ottaen vahingon vähäisyys tai muut rikokseen liittyvät seikat, on kokonaisuutena arvostellen vähäinen, rikoksentekijä on ***tuomittava lievästä datavahingonteosta*** *sakkoon.*
6 §	6 §
Syyteoikeus	*Syyteoikeus*
Jos 1 tai 3 §:ssä tarkoitetun rikoksen kohteena on ollut ainoastaan yksityinen omaisuus, syyttäjä ei saa nostaa syytettä, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi.	Jos 1, 3, *3 a tai 3 c* §:ssä tarkoitetun rikoksen kohteena on ollut ainoastaan yksityinen omaisuus, syyttäjä saa nostaa syytteen vain, jos asianomistaja ilmoittaa rikoksen syytteeseen pantavaksi.
7 §	7 §
Toimenpiteistä luopuminen	*Toimenpiteistä luopuminen*
Vahingonteosta ja lievästä vahingonteosta voidaan jättää ilmoitus tekemättä, syyte ajamatta tai rangaistus tuomitsematta, jos rikoksen tekijä on korvannut vahingon ja vahingonkorvaus harkitaan riittäväksi seuraamukseksi.	Vahingonteosta, *datavahingonteosta*, lievästä vahingonteosta ja *lievästä datavahingonteosta* voidaan jättää ilmoitus tekemättä, syyte ajamatta tai rangaistus tuomitsematta, jos rikoksen tekijä on korvannut vahingon ja vahingonkorvaus harkitaan riittäväksi seuraamukseksi.
8 §	8 §
Oikeushenkilön rangaistusvastuu	*Oikeushenkilön rangaistusvastuu*
Edellä 1 §:n 2 momentissa tarkoitettuun vahingontekoon sekä 2 §:ssä tarkoitettuun törkeään vahingontekoon, silloin kuin se on tehty 1 §:n 2 momentissa säädetyllä tavalla, sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.	*Datavahingontekoon ja törkeään datavahingontekoon* sovelletaan, mitä oikeushenkilön rangaistusvastuusta säädetään.

Voimassa oleva laki	*Ehdotus*
(uusi)	9 §
	Määritelmät
	Mitä 38 luvun 13 §:n 1 momentissa säädetään tietojärjestelmän määritelmästä, sovelletaan myös 3 a ja 3 b §:ään. *Mitä 38 luvun 13 §:n 2 momentissa säädetään datan määritelmästä, sovelletaan myös 3 a §:ään.*
38 luku	
Tieto- ja viestintärikoksista	
3 §	3 §
Viestintäsalaisuuden loukkaus	*Viestintäsalaisuuden loukkaus*
Joka oikeudettomasti 1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka 2) hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta, on tuomittava *viestintäsalaisuuden loukkauksesta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Yritys on rangaistava.	Joka oikeudettomasti 1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka 2) hankkii tiedon televerkossa *tai tietojärjestelmässä* välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta, on tuomittava *viestintäsalaisuuden loukkauksesta* sakkoon tai vankeuteen enintään *kahdeksi* vuodeksi. Yritys on rangaistava.
6 §	6 §
Törkeä tietoliikenteen häirintä	*Törkeä tietoliikenteen häirintä*
Jos tietoliikenteen häirinnässä	Jos tietoliikenteen häirinnässä
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(3—6 kohdat uusi)	*3) rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa,* *4) rikos tehdään osana 17 luvun 1 a §:n*

Voimassa oleva laki	*Ehdotus*
	4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa,
	5) rikoksella aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai
	6) rikos kohdistuu laitteeseen, tietojärjestelmään tai viestintään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon
ja tietoliikenteen häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä tietoliikenteen häirinnästä* vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.	ja tietoliikenteen häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä tietoliikenteen häirinnästä* vankeuteen vähintään neljäksi kuukaudeksi ja enintään *viideksi* vuodeksi.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
7 a §	7 a §
Tietojärjestelmän häirintä	*Tietojärjestelmän häirintä*
Joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, on tuomittava, *jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, tietojärjestelmän häirinnästä* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.	Joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, on tuomittava *tietojärjestelmän häirinnästä* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
Yritys on rangaistava.	Yritys on rangaistava.
7 b §	7 b §
Törkeä tietojärjestelmän häirintä	*Törkeä tietojärjestelmän häirintä*
Jos tietojärjestelmän häirinnässä	Jos tietojärjestelmän häirinnässä
1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa tai	1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa,
2) rikos tehdään erityisen suunnitelmallisesti	2) rikos tehdään erityisen suunnitelmallisesti,
(3—5 kohdat uusi)	*3) rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa,*

Voimassa oleva laki

ja tietojärjestelmän häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä tietojärjestelmän häirinnästä* vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.

Yritys on rangaistava.

8 §

Tietomurto

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava *tietomurrosta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta.

Yritys on rangaistava.

Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.

8 a §

Törkeä tietomurto

Ehdotus

4) rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai

5) rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon

ja tietojärjestelmän häirintä on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä tietojärjestelmän häirinnästä* vankeuteen vähintään neljäksi kuukaudeksi ja enintään *viideksi* vuodeksi.

Yritys on rangaistava.

8 §

Tietomurto

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja *tai dataa*, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava *tietomurrosta* sakkoon tai vankeuteen enintään *kahdeksi* vuodeksi.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta

1) teknisen erikoislaitteen avulla *tai*

2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin

oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta *tai datasta*.

Yritys on rangaistava.

Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.

8 a §

Törkeä tietomurto

Voimassa oleva laki	*Ehdotus*
Jos tietomurto tehdään 1) osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai 2) erityisen suunnitelmallisesti ja tietomurto on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä tietomurrosta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Yritys on rangaistava.	Jos tietomurto tehdään 1) osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai 2) erityisen suunnitelmallisesti ja tietomurto on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava *törkeästä tietomurrosta* sakkoon tai vankeuteen enintään *kolmeksi* vuodeksi. Yritys on rangaistava.
(uusi)	9 b § *Identiteettivarkaus* *Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava **identiteettivarkaudesta** sakkoon.*
10 § *Syyteoikeus*	10 § *Syyteoikeus*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(4 mom. uusi)	*Syyttäjä saa nostaa syytteen identiteettivarkaudesta vain, jos asianomistaja ilmoittaa rikoksen syytteeseen pantavaksi.*
11 § *Menettämisseuraamus*	11 § *Menettämisseuraamus*
Edellä 8 a §:ssä tarkoitettu suojauksen purkujärjestelmä on tuomittava valtiolle menetetyksi.	Edellä 8 *b* §:ssä tarkoitettu suojauksen purkujärjestelmä on tuomittava valtiolle menetetyksi.
(uusi)	13 § *Määritelmät* *Sovellettaessa 3, 6, 7 a, 7 b ja 8 §:ää tietojärjestelmällä tarkoitetaan myös tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kor-*

Voimassa oleva laki

Ehdotus

*vaamisesta annetun Euroopan parlamentin ja neuvoston direktiivin 2013/40/EU, jäljempänä **tietoverkkorikosdirektiivi**, 2 artiklan a kohdassa tarkoitettua:*

1) laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten; sekä

2) dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään sen tai niiden toimintaa, käyttöä, suojausta tai huoltoa varten.

Sovellettaessa 3, 7 a ja 8 §:ää datalla tarkoitetaan myös tietoverkkorikosdirektiivin 2 artiklan b kohdassa tarkoitettua:

1) sellaisessa muodossa olevien tosiseikkojen, tietojen, tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä; sekä

2) ohjelmaa, jonka avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon.

Tämä laki tulee voimaan päivänä kuuta 201 .

2.

Laki

pakkokeinolain 10 luvun 3 ja 6 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan pakkokeinolain (806/2011) 10 luvun 3 §:n 2 momentin 12 kohta ja 6 §:n 2 momentti, sellaisina kuin ne ovat laissa 1146/2013, seuraavasti:

Voimassa oleva laki	*Ehdotus*
10 luku	
Salaiset pakkokeinot	
3 §	3 §
Telekuuntelu ja sen edellytykset	*Telekuuntelu ja sen edellytykset*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa telekuuntelua rikoksesta epäillyn hallussa olevan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:	Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa telekuuntelua rikoksesta epäillyn hallussa olevan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
12) törkeästä vahingonteosta;	12) törkeästä vahingonteosta *tai törkeästä datavahingonteosta*;
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
6 §	6 §
Televalvonta ja sen edellytykset	*Televalvonta ja sen edellytykset*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa televalvontaa rikoksesta epäillyn hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:	Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa televalvontaa rikoksesta epäillyn hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:
1) rikoksesta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;	1) rikoksesta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;
2) teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;	2) teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeut-

Voimassa oleva laki

3) teleosoitetta tai telepäätelaitetta käyttäen tehdystä, automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta luvattomasta käytöstä, *vahingonteosta, viestintäsalaisuuden loukkauksesta tai tietomurrosta*;
4) seksikaupan kohteena olevan henkilön hyväksikäytöstä, lapsen houkuttelemisesta seksuaalisiin tarkoituksiin tai parituksesta;
5) huumausainerikoksesta;
6) terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta;
7) törkeästä tulliselvitysrikoksesta;
8) törkeästä laittoman saaliin kätkemisestä;
9) panttivangin ottamisen valmistelusta; taikka
10) törkeän ryöstön valmistelusta.

— — — — — — — — — — — — — —

Ehdotus

3) teleosoitetta tai telepäätelaitetta käyttäen tehdystä, automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta luvattomasta käytöstä;
4) seksikaupan kohteena olevan henkilön hyväksikäytöstä, lapsen houkuttelemisesta seksuaalisiin tarkoituksiin tai parituksesta;
5) huumausainerikoksesta;
6) terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta;
7) törkeästä tulliselvitysrikoksesta;
8) törkeästä laittoman saaliin kätkemisestä;
9) panttivangin ottamisen valmistelusta; taikka
10) törkeän ryöstön valmistelusta.

— — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 201 .

3.

Laki

poliisilain 5 luvun 8 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan poliisilain (872/2011) 5 luvun 8 §:n 2 momentti, sellaisena kuin se on laissa 1168/2013, seuraavasti:

Voimassa oleva laki	*Ehdotus*
5 luku	
Salaiset tiedonhankintakeinot	
8 §	8 §
Televalvonta ja sen edellytykset	*Televalvonta ja sen edellytykset*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Poliisille voidaan rikoksen estämiseksi antaa lupa kohdistaa televalvontaa henkilön hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos henkilön lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän:	Poliisille voidaan rikoksen estämiseksi antaa lupa kohdistaa televalvontaa henkilön hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos henkilön lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän:
1) rikokseen, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;	1) rikokseen, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;
2) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn rikokseen, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;	2) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn rikokseen, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;
3) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn, automaattiseen tietojenkäsittelyjärjestelmään kohdistuvaan luvattomaan käyttöön, *vahingontekoon, viestintäsalaisuuden loukkaukseen tai tietomurtoon*;	3) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn, automaattiseen tietojenkäsittelyjärjestelmään kohdistuvaan luvattomaan käyttöön;
4) seksikaupan kohteena olevan henkilön hyväksikäyttöön, lapsen houkuttelemiseen seksuaalisiin tarkoituksiin tai paritukseen;	4) seksikaupan kohteena olevan henkilön hyväksikäyttöön, lapsen houkuttelemiseen seksuaalisiin tarkoituksiin tai paritukseen;
5) huumausainerikokseen;	5) huumausainerikokseen;
6) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun; taikka	6) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun; taikka

Voimassa oleva laki	*Ehdotus*
7) törkeään tulliselvitysrikokseen.	7) törkeään tulliselvitysrikokseen.
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
	Tämä laki tulee voimaan päivänä kuuta 201 .

4.

Laki

sotilasoikeudenkäyntilain 2 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan sotilasoikeudenkäyntilain (326/1983) 2 §:n 2 momentti, sellaisena kuin se on laissa 1442/2007, seuraavasti:

Voimassa oleva laki	*Ehdotus*
2 §	2 §
Sotilasoikeudenkäyntiasiana käsitellään myös syyte sotilasta vastaan teosta, josta säädetään rangaistus rikoslain (39/1889) 21 luvun 1—3 tai 5—14 §:ssä, 25 luvun 7 tai 8 §:ssä, 28, 31—33 tai 35 luvussa, 36 luvun 1—3 §:ssä, 37 luvun 8—10 §:ssä, 38 luvun 1—7, 7 a, 7 b, 8 tai 8 a §:ssä taikka 40 luvun 1—3 tai 5 §:ssä. Edellytyksenä on, että teko on kohdistunut puolustusvoimiin tai toiseen sotilaaseen. Sotilasoikeudenkäyntiasiana käsitellään niin ikään syyte teosta, josta säädetään rangaistus asevelvollisuuslain (1438/2007) 118 §:ssä.	Sotilasoikeudenkäyntiasiana käsitellään myös syyte sotilasta vastaan teosta, josta säädetään rangaistus rikoslain (39/1889) 21 luvun 1—3 tai 5—14 §:ssä, 25 luvun 7 tai 8 §:ssä, 28, 31—33 tai 35 luvussa, 36 luvun 1—3 §:ssä, 37 luvun 8—10 §:ssä, 38 luvun 1—7, 7 a, 7 b, 8, 8 a *tai 9 b* §:ssä taikka 40 luvun 1—3 tai 5 §:ssä. Edellytyksenä on, että teko on kohdistunut puolustusvoimiin tai toiseen sotilaaseen. Sotilasoikeudenkäyntiasiana käsitellään niin ikään syyte teosta, josta säädetään rangaistus asevelvollisuuslain (1438/2007) 118 §:ssä.
	Tämä laki tulee voimaan päivänä kuuta 201 .