Mietintöjä ja lausuntoja
Betänkanden och utlåtanden

35/2014

Tietoverkkorikosdirektiivin täytäntöönpano

Lausuntotiivistelmä

oikeusministeriö
justitieministeriet

Mietintöjä ja lausuntoja
Betänkanden och utlåtanden

35/2014

Tietoverkkorikosdirektiivin täytäntöönpano

Lausuntotiivistelmä

Oikeusministeriö, Helsinki 2014

KUVAILULEHTI

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

26.8.2014

Julkaisun nimi	Tietoverkkorikosdirektiivin täytäntöönpano Lausuntotiivistelmä
Tekijä	Inka-Liina Jääskeläinen
Oikeusministeriön julkaisu	35/2014 Mietintöjä ja lausuntoja
OSKARI numero	OM 15/41/2013 HARE numero OM017:00/2013
ISSN-L ISSN (PDF) ISBN (PDF)	1798-7105 1798-7105 978-952-259-391-7
URN Pysyvä osoite	URN:ISBN:978-952-259-391-7 http://urn.fi/URN:ISBN:978-952-259-391-7
Asia- ja avainsanat	rikosoikeus, tietoverkko, rikoslaki, identiteettivarkaus

Tiivistelmä

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.

Työryhmän mietintö valmistui 17 päivänä huhtikuuta 2014 (Tietoverkkorikosdirektiivin täytäntöönpano, OMML 27/2014). Mietinnössä ehdotetaan tehtäväksi tietoverkkorikosdirektiivin edellyttämät muutokset rikoslakiin. Muutokset koskisivat erityisesti vaaran aiheuttamista tietojenkäsittelylle, vahingontekoa, viestintäsalaisuuden loukkausta, tietojärjestelmän häirintää ja tietomurtoa. Niin sanottu datavahingonteko ja törkeä datavahingonteko erotettaisiin perusmuotoisesta vahingonteosta itsenäisiksi kriminalisoinneiksi. Datavahingonteon, viestintäsalaisuuden loukkauksen ja tietomurron enimmäisrangaistus puolestaan nostettaisiin kahteen vuoteen vankeutta. Törkeän tietomurron enimmäisrangaistus nostettaisiin kolmeen vuoteen vankeutta. Törkeään datavahingontekoon, törkeään tietoliikenteen häirintään ja törkeään tietojärjestelmän häirintään sisällytettäisiin direktiivin edellyttämät kvalifiointiperusteet. Törkeiden tekomuotojen enimmäisrangaistus olisi direktiivin edellyttämällä tavalla viisi vuotta vankeutta.

Direktiivin vaatimusten täyttämiseksi mietinnössä ehdotetaan myös uutta identiteettivarkautta koskevaa kriminalisointia. Sen enimmäisrangaistus olisi sakkoa. Mietintöön sisältyy eriävä mielipide koskien identiteettivarkauteen liittyviä tutkintavaltuuksia.

Oikeusministeriö pyysi ehdotuksesta lausunnon yhteensä 39 eri viranomaiselta, järjestöltä ja asiantuntijalta. Pyydetyistä lausunnoista saapui annettuun määräaikaan mennessä yhteensä 18. Tässä lausuntotiivistelmässä selostetaan työryhmän mietinnöstä annettuja lausuntoja.

PRESENTATIONS-
BLAD

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

26.8.2014

Publikationens titel	Genomförande av direktivet om it-relaterad brottslighet Remissammandrag
Författare	Inka-Liina Jääskeläinen
Justitieministeriets publikation	35/2014 Betänkanden och utlåtanden
OSKARI nummer	OM 15/41/2013 HARE nummer OM017:00/2013
ISSN-L ISSN (PDF) ISBN (PDF)	1798-7105 1798-7105 978-952-259-391-7
URN Permanent adress	URN:ISBN:978-952-259-391-7 http://urn.fi/URN:ISBN:978-952-259-391-7
Sak- och nyckelord	straffrätt, informationsnät, strafflagen, identitetsstöld

Referat

Den 27 september 2013 tillsatte justitieministeriet en arbetsgrupp som fick i uppdrag att bereda ett förslag till nationell lagstiftning om genomförande av direktivet 2013/40/EU om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF. Förslaget skulle ha formen av en regeringsproposition. Arbetsgruppen skulle i sitt arbete även beakta bedömningspromemorian om identitetsstöld (OM 4/41/2013) och remissyttrandena om den, till den del den gäller strafflagstiftningen i fråga som hör till justitieministeriets verksamhetsområde.

Arbetsgruppens betänkande blev klart den 17 april 2014 (Genomförande av direktivet om it-relaterad brottslighet, OMML 27/2014). I betänkandet föreslås sådana ändringar av strafflagen som direktivet om it-relaterad brottslighet förutsätter. Ändringarna gäller i synnerhet orsakande av fara för informationsbehandling, skadegörelse, kränkning av kommunikationshemlighet, systemstörning och dataintrång. Så kallad dataskadegörelse och grov dataskadegörelse avskiljs som självständiga kriminaliseringar från skadegörelse i grundform. Maximistraffet för dataskadegörelse, kränkning av kommunikationshemlighet och dataintrång höjs för sin del till fängelse i två år. Maximistraffet för grovt dataintrång höjs till fängelse i tre år. Grov dataskadegörelse, grovt störande av post- och teletrafik och grov systemstörning förenas med de kvalificeringsgrunder som direktivet förutsätter. Som maximistraff för de grova gärningsformerna föreslås, på det sätt som direktivet förutsätter, fängelse i fem år.

För att kraven enligt direktivet ska uppfyllas föreslås i betänkandet också en ny kriminalisering som gäller identitetsstöld. Maximistraffet för det brottet är enligt förslaget böter. I betänkandet ingår en avvikande mening som gäller utredningsbefogenheterna vid identitetsstöld.

Justitieministeriet sände förslaget på remiss till sammanlagt 39 olika myndigheter, organisationer och sakkunniga. Sammanlagt kom det in 18 av de begärda utlåtandena inom den utsatta tiden. I detta remissammandrag behandlas de utlåtanden om arbetsgruppens betänkande som kom in.

SISÄLLYS

1 Johdanto

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. Työryhmän mietintö valmistui 17 päivänä huhtikuuta 2014 (Tietoverkkorikosdirektiivin täytäntöönpano, OMML 27/2014).

Mietinnössä ehdotetaan tehtäväksi tietoverkkorikosdirektiivin edellyttämät muutokset rikoslakiin. Vaaran aiheuttamiseen tietojenkäsittelylle ehdotetaan lisättäväksi tekotavaksi tietoverkkorikosvälineen käyttöön hankkiminen. Lakiin ehdotetaan lisättäväksi uusi datavahingontekoa koskeva kriminalisointi sekä datavahingonteon törkeä ja lievä tekomuoto. Syyteoikeutta, toimenpiteistä luopumista, oikeushenkilön rangaistusvastuuta ja pakkokeinolakia tarkistettaisiin vastaamaan edellä mainittua muutosta. Viestintäsalaisuuden loukkausta ehdotetaan muutettavaksi niin, että se kattaa direktiivin vaatimusten mukaisesti myös tietojärjestelmän sisäisen luottamuksellisen datan siirron. Tietojärjestelmän häirinnästä ehdotetaan poistettavaksi toissijaisuuslauseke. Tietomurtoa ehdotetaan muutettavaksi niin, että se kattaa direktiivin edellyttämin tavoin myös pääsyn tietojärjestelmässä olevaan dataan ja tiedon hankkimisen siitä. Mietinnössä ehdotetaan myös uutta säännöstä, joka sisältäisi direktiivin velvoitteisiin rajautuen avoimet tietojärjestelmän ja datan määritelmät.

Datavahingonteon, viestintäsalaisuuden loukkauksen ja tietomurron enimmäisrangaistus nostettaisiin kahteen vuoteen vankeutta. Törkeän tietomurron enimmäisrangaistus puolestaan nostettaisiin kolmeen vuoteen vankeutta. Törkeään datavahingontekoon, törkeään tietoliikenteen häirintään ja törkeään tietojärjestelmän häirintään sisällytettäisiin direktiivin edellyttämät kvalifiointiperusteet, jotka liittyvät ns. bottiverkkoihin, rikollisjärjestöön, vakavaan vahinkoon ja elintärkeään infrastruktuuriin. Törkeiden tekomuotojen enimmäisrangaistus olisi direktiivin edellyttämällä tavalla viisi vuotta vankeutta.

Direktiivin vaatimusten täyttämiseksi mietinnössä ehdotetaan myös uutta identiteettivarkautta koskevaa kriminalisointia. Identiteettivarkaus olisi asianomistajarikos ja sen enimmäisrangaistus olisi sakkoa. Mietintöön sisältyy Sisäministeriön edustajan, poliisitarkastaja Antti Simanaisen eriävä mielipide koskien identiteettivarkauteen liittyviä tutkintavaltuuksia. Eriävässä mielipiteessä esitetään, että ehdotettu identiteettivarkaus lisätään pakkokeinolain 10 luvun 6 §:n 2 momenttiin uudeksi televalvonnan perusterikokseksi, jotta rikoksen tutkinta voidaan mahdollistaa esitutkintaviranomaiselle.

Oikeusministeriö pyysi ehdotuksesta lausunnon yhteensä 39 eri viranomaiselta, järjestöltä ja asiantuntijalta. Tiivistelmän liitteenä on luettelo lausunnonantajista. Pyydetyistä lausunnoista saapui annettuun määräaikaan mennessä yhteensä 18. Helsingin käräjäoikeus totesi, ettei se anna lausuntoa mietinnöstä.

Tiivistelmän jaksossa 2 esitetään lausunnonantajien arviot mietinnöstä yleisellä tasolla. Jaksossa 3 eritellään lausunnonantajien pykäläkohtaisia arvioita ehdotetuista lakiuudistuksista. Jaksossa ei ole mainittu pykäliä, joihin mietinnössä on ehdotettu muutoksia, mikäli lausunnonantajat eivät ole lausuneet niistä. Jaksossa 4 tuodaan esille lausunnonantajien yksittäisiä huomioita ja heidän ehdotuksiaan jatkovalmistelua varten. Jos lausunnonantaja ei ole lausunut yksityiskohtaisesti ehdotuksista, ei lausunnonantajaa välttämättä enää mainita jaksojen 3 tai 4 yhteydessä.

2 Yleiset arviot työryhmän ehdotuksista

2.1 Aluksi

Lausunnonantajat yleisesti kannattavat työryhmän ehdotuksia rikoslakiin ja pakkokeinolakiin tehtävistä muutoksista tietoverkkorikosdirektiivin täytäntöön panemiseksi. Erityisesti identiteettivarkauden kriminalisointia itsenäisenä rikoksena pidetään perusteltuna ja tarpeellisena. Työryhmän mietintöön sisältyvän eriävän mielipiteen tavoin eräät lausunnonantajat painottavat televalvonnan mahdollistamista identiteettivarkauden selvittämisessä. Lausuntopalautteessa esitetään myös tarkennuksia ja muutosehdotuksia ehdotettujen säännösten sanamuotoihin ja esityksessä käytettyyn terminologiaan.

2.2 Ylimmät laillisuusvalvojat ja ministeriöt

Eduskunnan apulaisoikeusasiamies (EAOA) kiinnittää huomiota siihen, että nykyisessä tilanteessa tietorikosten suojeluobjektien määrittely saattaa olla haasteellista. EAOA toteaa, että ehdotettu rikosoikeudellinen sääntely on vain osa tietoyhteiskunnan ylläpitämiseksi tarkoitettua perusrakennetta; se voi ratkaista vain osan tietoturvallisen toimintaympäristön ongelmista. EAOA katsoo, että esityksestä syntyy teknisen täytäntöönpanouudistuksen kuva ja lakiehdotuksista tulisi hankkia aikanaan eduskunnan perustuslakivaliokunnan lausunto. EAOA:n mukaan säännösehdotukset vaaran aiheuttamisesta tietojenkäsittelylle ja identiteettivarkaudesta sisältävät joitakin tulkinnanvaraisuuksia. EAOA katsoo, että mietinnössä olisi tullut arvioida enemmän identiteettivarkautta koskevaa oikeuskäytäntöä. Vahingontekoa tietojenkäsittelyssä koskevien säännösten osalta valmistelussa olisi tullut perehtyä enemmän oikeuskirjallisuuteen, mikä olisi syventänyt vaikutusten arviointia. Lisäksi esityksen viittaus pakkokeinolakiin olisi kaivannut ohelleen viittauksen ns. esitutkintapakettiin ja arvioinnin sen vaikutuksista tietoverkkoympäristössä. Viestintäsalaisuuden loukkauksen osalta ehdotettuja muutoksia tulisi EAOA:n mukaan arvioida vielä Euroopan ihmisoikeussopimuksen määräysten ja ihmisoikeustuomioistuimen oikeuskäytännön valossa. Lisäksi EAOA toteaa, että lainvalmistelussa määritelmäsäännökset voidaan koota lain alkuun omaksi pykäläkseen, ja tässä yhteydessä se olisi tarpeellista.

Valtioneuvoston oikeuskansleri (OKA) on ilmoittanut, että hänellä ei ole huomautettavaa esitysluonnoksen yksittäisistä säännösehdotuksista.

Liikenne- ja viestintäministeriö on ilmoittanut, että sillä ei ole lausuttavaa mietinnöstä.

Puolustusministeriö (PM) pitää työryhmän ehdotuksia tärkeinä ja perusteltuina. PM kiinnittää huomiota puolustushallinnon osalta ehdotukseen niiltä osin kuin se koskee rikoslain 35 ja 38 lukujen muuttamista. PM katsoo, että viittaus identiteettivarkautta koskevaan pykälään tulisi lisätä sotilasoikeudenkäyntilain 2 §:n 2 momentin luetteloon. Lisäksi PM tuo sotilasrikosoikeudenkäyntilain kannalta esiin näkökohtia ehdotetuista syyteoikeutta ja toimenpiteistä luopumista koskevista säännöksistä. PM toteaa, että pakkokeinolain 10 luvun 3 §:n muutoksella ei tulisi olemaan vaikutuksia puolustusvoimien suorittamaan esitutkintaan, koska telekuuntelu ei sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain (255/2014) mukaan ole esitutkintaa suorittavien pääesikunnan virkamiesten käytettävissä. Terminologian osalta PM ehdottaa käsitteen ”elintärkeä infrastruktuuri” korvaamista termillä ”elintärkeä toiminto”. Tähän liittyen ehdotetuissa ja voimassa olevissa säännöksissä ”tärkeitä toimintoja” kuvaava esimerkinomainen luettelo voitaisiin PM:n näkemyksen mukaan korvata muotoilulla ”yhteiskunnan elintärkeä toiminto”.

Sisäministeriö (SM) toteaa, että sen edustaja on ollut mukana asiaa valmistelleessa työryhmässä, joten SM:n näkemykset ovat tulleet pääsääntöisesti huomioiduksi valmistelun aikana. SM:n edustaja jätti mietintöön eriävän mielipiteen, joka koski identiteettivarkauteen liittyvää televalvontatietojen käyttömahdollisuutta. SM toteaa, että poliisilaissa ja pakkokeinolaissa säädettyjen telepakkokeinojen käyttö on tietoverkkorikollisuuden selvittämisessä säännönmukaista, ei poikkeuksellista. SM pitää poliisin operatiivisen toiminnan kannalta kannatettavana, että nostettaessa eräiden kriminalisointien rangaistustasoja eräät pakkokeinot tulevat sovellettaviksi ilman pakkokeinolain muuttamista. Identiteettivarkauden osalta SM kuitenkin toteaa, että säännös ei esitetyssä muodossaan turvaa niitä keinoja, joita tarvitaan kyseisten rikosten torjunnassa. SM esittää, että pakkokeinolaissa säädettyjä televalvonnan perusteita täydennetään siten, että televalvonta olisi mahdollista identiteettivarkauden selvittämisessä. Muilta osin SM toteaa, että tietoverkkorikosdirektiivin täytäntöönpano vahvistaa osaltaan kyberturvallisuusstrategian linjausta 8, jossa todetaan, että kansallisella lainsäädännöllä varmistetaan tehokaan kyberturvallisuuden toteuttamisen edellytykset. SM toteaa direktiivin pitävän sisällään pitkälti samoja säännöksiä kuin Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (CETS 185). SM pitää tavoiteltavana, että yhä useampi EU:n ulkopuolinen maa liittyisi yleissopimukseen.

2.3 Tuomioistuimet

Helsingin käräjäoikeus on ilmoittanut, että se ei anna lausuntoa työryhmän mietinnöstä.

Pirkanmaan käräjäoikeus puoltaa luonnoksen mukaista ehdotusta hallituksen esitykseksi. Käräjäoikeus pitää uutta identiteettivarkautta koskevaa säännöstä tarpeellisena jo kunkin henkilön oman yksilöllisyyden suojaamiseksi. On myös hyvä, että säännös suojaa henkilön identiteettiä muutoinkin kuin tietojärjestelmien käytössä. Vaaran aiheuttamista tietojenkäsittelylle koskevaan säännökseen ehdotetun lisäyksen osalta esityksen

perusteluja tulisi käräjäoikeuden näkemyksen mukaan täsmentää niin, että teon täyttymishetki olisi selkeämmin ilmaistu. Käräjäoikeus katsoo myös, että jää jonkin verran epäselväksi, mitä käsitteillä data ja tieto tarkoitetaan ehdotetuissa säännöksissä.

Varsinais-Suomen käräjäoikeuden mukaan identiteettivarkauden kriminalisointi on toteutettu mietinnössä tavalla, joka vastaa käräjäoikeuden aikaisempaa käsitystä kriminalisointitarpeesta ja sen perusteista. Käräjäoikeus pitää ehdotettua säännöstä laillisuusperiaatteen näkökulmasta riittävän tarkkana ja arvioi sen kattavan suurimman osan kriminalisoinnin tarpeen aiheuttavista tilanteista. Käräjäoikeus pitää hyväksyttävinä myös työryhmän perusteluita 38 luvun 10 §:n mukaisesta syyteoikeudesta. Muista ehdotuksista käräjäoikeudella ei ole huomautettavaa.

2.4 Syyttäjänvirastot

Valtakunnansyyttäjänvirasto (VKSV) toteaa, että sen edustaja on osallistunut jäsenenä työryhmän toimintaan, joten syyttäjälaitoksen näkemykset ovat pääosin tulleet mietinnössä huomioiduksi. VKSV pitää perusteltuna ja tarpeellisena uutta identiteettivarkauden kriminalisointia itsenäisenä rikoksena. VKSV esittää identiteettivarkauden lisäämistä pakkokeinolakiin televalvonnan perusterikokseksi, jotta viranomaisilla olisi käytettävissä riittävät telepakkokeinot tunnistamistietojen saamiseksi ja rikoksen selvittämiseksi. VKSV:lla ei ole huomautettavaa syyteoikeutta koskeviin säännöksiin tai mietintöön muilta osin kuin kvalifioitujen tekomuotojen osalta eräitä, lähinnä teknisiä seikkoja. Ehdotetut törkeä datavahingonteko, törkeä tietoliikenteen häirintä, törkeä tietojärjestelmän häirintä ja törkeä tietomurto sisältävät hyvin samankaltaiset luettelot rikoksen kvalifiointiperusteista. VKSV ehdottaa, että nämä kohdat voisivat olla johdonmukaisesti samassa ja todennäköisessä esiintymisjärjestyksessä.

Helsingin syyttäjänvirasto kiinnittää huomiota eräisiin syyttäjän työn kannalta merkityksellisiin muutosehdotuksiin. Syyttäjänvirasto pitää erittäin kannatettavana tietomurtoa koskevan säännöksen osalta sitä, että ”murtautumisen” määritelmää ehdotetaan laajennettavaksi. Syyttäjänviraston mukaan kyseessä on usein juuri tietojärjestelmän haavoittuvuuden hyväksi käyttäminen eikä suora murtautuminen tietojärjestelmään, ja harkittavaksi voisi tulla, pitäisikö tietomurtoa vastaava lavennus lisätä myös viestintäsalaisuuden loukkaamisen tunnusmerkistöön. Järjestäytyneen rikollisryhmän määritelmän osalta syyttäjänvirasto tuo esiin potentiaalisen soveltamisongelman tietoverkkorikoksissa. Identiteettivarkauden osalta syyttäjänvirasto katsoo, että yleisestävyyden ja tehokkaan tutkinnan kannalta televalvonnan käyttö tulisi mahdollistaa pakkokeinolaissa. ”Elintärkeää infrastruktuuria” koskevan kvalifiointiperusteen osalta syyttäjänvirasto esittää harkittavaksi, tulisiko listauksessa vielä mainita erikseen esimerkiksi elintarvikehuolto ja finanssipalvelut, vaikka muotoilu ”näihin rinnastettava yhteiskunnan tärkeä toiminto” voitaneen tulkita laajasti.

Sisä-Suomen syyttäjänviraston näkemyksen mukaan identiteettivarkaus ei ole saanut mietinnössä ansaitsemaansa huomiota ja asemaa. Syyttäjänvirasto haluaa esityksen perusteluista poistettavaksi maininnan siitä, että ”erehtymisen vaaraa ei esimerkiksi olisi, jos toiminta on selkeästi tunnistettavissa satiiriksi”. Lisäksi syyttäjänvirasto katsoo, että rangaistusasteikon olisi vastattava paremmin teon rangaistusarvoa ja riittävien pakkokeinojen käyttö tulisi mahdollistaa esimerkiksi pakkokeinolakia muuttamalla.

2.5 Muut lausunnonantajat

Viestintävirasto pitää hallituksen esityksen muotoon laadittua työryhmän mietintöä hyvin valmisteltuna ja perusteltuna. Viestintävirastolla ei ole mietinnöstä erityistä lausuttavaa.

Dosentti Seppo Virtanen Turun yliopistosta pitää esitystä kokonaisuutena kattavana ja hyvänä. Virtanen toteaa, että esitys ajanmukaistaa asiallisesti aiheeseen liittyvän lainsäädännön. Virtasen mukaan identiteettivarkauden tuominen osaksi rikoslainsäädäntöä on tärkeä parannus nykytilanteeseen. Tutkintamenetelmien osalta Virtanen viittaa mietinnössä esitettyyn eriävään mielipiteeseen ja esittää jatkovalmistelussa pohdittavaksi, mahdollistaako esitys riittävät työkalut identiteettivarkauden tutkinnalle itsenäisenä rikoksena. Virtanen katsoo, että identiteettivarkauksia tulisi voida tutkia myös itsenäisinä rikoksina ja käytettävissä olevien tutkintamenetelmien tulee tällöin olla riittävän kattavat. Lisäksi Virtanen katsoo, että esityksen perusteluissa olisi tärkeää tuoda esille myös identiteettivarkauden uhrin statuksen merkitys sekä sähköisen äänestämisen tilanne tietoverkkorikollisuuteen liittyen.

Elinkeinoelämän keskusliitto EK ry:lla (EK) ei ole huomautettavaa ehdotettuihin muutoksiin. EK pitää tärkeänä, että tietoverkkorikoksiin reagoidaan saattamalla rikoslaki lähemmäs ilmiön vakavuuden vaatimaa tasoa. Identiteettivarkauden kriminalisoimista EK pitää erittäin tärkeänä. EK kuitenkin ehdottaa eriävässä mielipiteessä esitetyin tavoin, että identiteettivarkaus lisätään pakkokeinolakiin uudeksi televalvonnan perusterikokseksi, jotta identiteettivarkauksien tutkinta ylipäätään tulee mahdolliseksi.

Finanssialan Keskusliitto ry (FK) pitää hyvänä mietinnön linjauksia, joilla pyritään varmistamaan verkkohyökkäysten kattava kriminalisointi. FK:n mukaan ehdotetut muutokset vaikuttavat keskeisellä tavalla siihen, millaiseksi kansallinen kybertoimintaympäristö muovautuu. FK toteaa, että direktiivin jättäessä kansalliseen sääntelyyn liikkumavaraa on huolehdittava siitä, etteivät kansalliset erot muodostu esteeksi rikosten torjunta- ja tutkintayhteistyölle EU:n alueella eikä Suomesta puutteellisen sääntelyn vuoksi muodostu identiteettivarkaiden tai muiden verkkorikollisten turvasatamaa. FK yhtyy pääosin mietinnön ehdotuksiin ja pitää erittäin hyvänä ehdotusta identiteettivarkauden kriminalisoimisesta. Identiteettivarkauden osalta FK kuitenkin esittää useita pidemmälle meneviä ehdotuksia, kuten identiteettitietojen oikeudettoman keräämisen ja hallussapidon tekotavaksi, vankeusrangaistuksen mahdollisuuden rangaistustyypiksi sekä törkeän tekomuodon säätämistä. FK pitää tärkeänä, että riittävät telepakkokeinot sallitaan sekä

identiteettivarkauden että muiden tietoverkkorikosten esitutkinnassa. Lisäksi FK pitää välttämättömänä, että törkeään datavahingontekoon, törkeään tietoliikenteen häirintään ja törkeään tietojärjestelmän häirintään ehdotettu elintärkeään infrastruktuuriin liittyvä kvalifiointiperuste määritellään yhdenmukaiseksi eräissä muissa asiakirjoissa sovellettujen määritelmien kanssa. Tietoverkkorikosdirektiivin kansallisessa täytäntöönpanossa tulisi myös huomioida EU:ssa vireillä oleva tietosuoja-asetusta koskeva sääntelyhanke.

Suomen Ammattiliittojen Keskusjärjestö SAK ry:n (SAK) mukaan uusien rikosnimikkeistöjen säätäminen ja rangaistusmaksimien nostaminen ovat kannatettavia lainsäädäntömuutoksia tietoverkkorikosten ennalta ehkäisemiseksi ja niiden selvittämiseksi. Myös uusi identiteettivarkautta koskeva kriminalisointi on perusteltu lisäys lainsäädäntöön. SAK viittaa mietinnössä esitettyyn eriävään mielipiteeseen, jossa ehdotetaan identiteettivarkauden lisäämistä pakkokeinolakiin uudeksi televalvonnan perusterikokseksi. Tältä osin olisi SAK:n mukaan hyvä vielä tarkemmin selvittää, onko varsinainen työryhmän esitys riittävä.

Suomen Yrittäjät ry (Suomen Yrittäjät) kannattaa ehdotettuja muutoksia ja pitää niitä tarpeellisina, koska tietoverkkorikokset ja niiden uhka aiheuttavat yritystoiminnalle kasvavaa haittaa ja vahinkoa. Suomen Yrittäjät pitää aiheellisena identiteettivarkauden kriminalisoimista itsenäiseksi rikokseksi. Identiteettivarkauden osalta Suomen Yrittäjät esittää lausunnossaan useita tarkennuksia lakiehdotuksen perusteluihin koskien yritysten asemaa identiteettivarkauden kohteena. Suomen Yrittäjät ehdottaa myös kyseisen säännöksen sanamuotoa tarkennettavaksi siten, että siitä ilmenisi, että kyse on nimenomaan toisena henkilönä oikeudettomasti esiintymisestä, ei pelkästään tietojen oikeudettomasta käytöstä.

Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry (FiCom) kiinnittää huomiota ehdotettuihin 38 luvun 13 §:n tietojärjestelmän ja datan määritelmiin. FiCom ei pidä tarkoituksenmukaisena, että lisättäväksi ehdotetut määritelmät kattaisivat mietinnön mukaan ainoastaan ne kriminalisoinnit, joiden on tarkoitettu kattavan direktiivin velvoitteet. FiCom tuo esiin, että kyseiset käsitteet löytyvät rikoslain muistakin kohdista, ja ehdottaa, että käsitteiden sisältö ja merkitys yhtenäistettäisiin koko lakia koskien. Lisäksi FiCom tuo esiin, että vaaran aiheuttamista tietojenkäsittelylle koskevaan säännökseen ehdotettu lisäys sanoilla ”hankkii käyttöön” osaltaan laajentaa pakkokeinolain mukaisen televalvonnan käyttömahdollisuuksia, minkä mahdollisia vaikutuksia ei ole otettu huomioon mietinnössä. Muilta osin FiComilla ei ole varsinaista lausuttavaa huolellisesti valmistellusta mietinnöstä.

Tietoturva ry on todennut, että sillä ei ole mietintöön tutustuttuaan kommentoitavaa.

3 Pykäläkohtaiset arviot

3.1 Laki rikoslain muuttamisesta

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.

Pirkanmaan käräjäoikeuden mukaan ehdotetun ”hankkii käyttöön” lisäyksen osalta perusteluista voi olla ymmärrettävissä, että säännös edellyttää täyttyäkseen sitä, että säännöksessä tarkoitettu väline on tullut tekijän hallintaan. Käräjäoikeuden mukaan säännöstä voisi sanamuodon perusteella tulkita kuitenkin niin, että rangaistavaa olisi jo hankkiminen eli menettely, joka edeltää välineen saamista hallintaan. Perusteluja tulisi täsmentää niin, että teon täyttymishetki olisi selkeästi ilmaistu.

FiCom tuo esiin, että tunnusmerkistön täydennys sanoilla ”hankkii käyttöön” osaltaan laajentaa pakkokeinolain mukaisen televalvonnan käyttömahdollisuuksia. Tämän laajennuksen mahdollisia vaikutuksia ei ole tarkastelussa otettu huomioon.

EAOA toteaa, että vaikka säännöksen muutos koskien tietoverkkorikosvälineen käyttöön hankkimista on osin tekninen, ehdotettuun sääntelyyn sisältyy tulkinnanvaraisuuksia. EAOA:n mukaan rikoksentekoon soveltuvan välineen yksilöinti voi olla käytännössä pulmallista.

35 luku

Vahingonteosta

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 on kohdistunut 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.

VKSV tuo esiin, että ehdotetun rikoslain 35 luvun 3 b §:n törkeä datavahingonteko sekä 38 luvun 6 §:n törkeä tietoliikenteen häirintä, 7 b §:n törkeä tietojärjestelmän häirintä ja 8 a §:n törkeä tietomurto sisältävät hyvin samankaltaiset luettelot rikoksen kvalifiointiperusteista. VKSV ehdottaa, että kohdat voisivat olla johdonmukaisesti samassa ja

todennäköisessä esiintymisjärjestyksessä; tällöin perusjärjestys olisi törkeän tietojärjestelmän häirinnässä esitetty. VKSV ehdottaa, että törkeässä datavahingonteossa esitetty 2 kohta siirrettäisiin 3 kohdan jälkeen.

PM esittää, että pykälään ehdotettu ”tärkeitä toimintoja” kuvaava tekstiosuus jätetään pois ja muotoilu ”rikos on kohdistunut tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon” muutetaan muotoon ”rikos on kohdistunut tietojärjestelmään, jonka vahingoittaminen vaarantaisi yhteiskunnan elintärkeän toiminnon”. PM:n mukaan luettelomainen ”energiahuolto, yleinen terveydenhuolto, maanpuolustus, oikeudenhoito tai muu näihin rinnastettava yhteiskunnan tärkeä toiminto” toistuu useissa pykälissä ja edustaa vakiintuneesta käytöstä jo poistunutta muotoilua. Myöskään ”muu näihin rinnastettava” ei PM:n näkemyksen mukaan ole riittävän informatiivinen. PM kuitenkin toteaa, että mikäli terminologiassa halutaan säilyttää esimerkinomainen luettelo tärkeistä toiminnoista, voisi muotoilu kuulua ”…vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan *elin*tärkeän toiminnon”.

PM katsoo, että työryhmä on ehdotuksen perusteluissa käyttänyt käsitettä ”elintärkeä infrastruktuuri” samassa mielessä kuin vakiintunut käsite ”elintärkeä toiminto”, joka on määritelty Yhteiskunnan turvallisuusstrategiassa (valtioneuvoston periaatepäätös 16.12.2010). Periaatepäätöksessä kuvataan, että elintärkeät toiminnot ovat poikkihallinnollisia, yhteiskunnalle välttämättömiä toimintokokonaisuuksia, jotka on oltava turvattuna kaikissa tilanteissa. Tällaisia toimintoja ovat: valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky sekä henkinen kriisinkestävyys. PM:n mukaan Euroopan unionissa ei ole aivan vastaavaa termiä käytössä. PM toteaa, että käsitteen ”elintärkeä infrastruktuuri” englanninkielinen versio on ”critical infrastructure”, joka yleisesti käännetään suomenkielisissä teksteissä sanaparilla ”kriittinen infrastruktuuri”. ”Critical infrastructure” on kuitenkin käsitteellisesti kotimaassa käytettyä ”elintärkeää toimintoa” suppea-alaisempi. Työryhmän käyttämä ”elintärkeä infrastruktuuri” ei myöskään ole Suomessa yhtä laajasti käytössä kuin ”elintärkeät toiminnot” tai ”kriittinen infrastruktuuri”. Asiakirjojen yhtenäistämiseksi ”elintärkeä infrastruktuuri” tulisi korvata termillä ”elintärkeä toiminto”.

Myös *FK* esittää lausunnossaan huomion ”elintärkeää infrastruktuuria” koskevasta kvalifiointiperusteesta. FK toteaa, että kvalifiointiperustetta ei ole määritelty direktiivissä. Mietinnössä peruste on muotoiltu seuraavasti: ”… jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon”. FK:n mukaan mietinnössä ehdotettu muotoilu poikkeaa selvästi elintärkeän (tai kriittisen) infrastruktuurin käsitteestä, jota käytetään ainakin Yhteiskunnan turvallisuusstrategiassa (valtioneuvoston periaatepäätös 16.12.2010), Suomen kyberturvallisuusstrategiassa (valtioneuvoston periaatepäätös 24.1.2013) ja valtioneuvoston päätöksessä huoltovarmuuden tavoitteista (5.12.2013). Viimeksi mainitussa on sisällytetty kriittiseen infrastruktuuriin seuraavat

osa-alueet: energian tuotanto-, siirto- ja jakelujärjestelmät; tieto- ja viestintäjärjestelmät, -verkot ja -palvelut; finanssialan palvelut; liikenne ja logistiikka; vesihuolto; infrastruktuurin rakentaminen ja kunnossapito sekä jätehuolto. FK pitää välttämättömänä, että elintärkeään infrastruktuuriin liittyvä kvalifiointiperuste määritellään niin, että se on yhdenmukainen edellä mainituissa asiakirjoissa sovellettujen määritelmien kanssa.

Helsingin syyttäjänvirasto toteaa, että vaikka kvalifiointiperusteissa mainittu muu ”näihin rinnastettava yhteiskunnan tärkeä toiminto” voitaneen tulkita laajasti, voisi harkittavaksi tulla, tulisiko listauksessa vielä erikseen mainita esimerkiksi elintarvikehuolto ja finanssipalvelut. Syyttäjänvirasto tarkoittaa esimerkiksi verkossa olevia pankkipalveluita, joihin kohdistuvat teot voivat vakavasti vaarantaa järjestelmää ilman, että olisi jo aiheutunut erityisen tuntuvaa haittaa tai taloudellista vahinkoa.

Lisäksi Helsingin syyttäjänvirasto toteaa, että ehdotuksessa esitetään lisättäväksi kvalifiointiperusteeksi se, että rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa. Voimassa olevaan törkeään vahingontekoon ja törkeään tietomurtoon vastaava kvalifiointiperuste on jo lisätty. Syyttäjänvirasto toteaa, että tietoverkkojen rikollisryhmät ovat usein varsin löyhiä yhteenliittymiä, joissa järjestäytyminen on erilaista verrattuna ns. perinteiseen rikollisuuteen. Syyttäjänvirasto huomauttaa, että oikeuskäytännön perusteella on käynyt selväksi, että kynnys tuomita henkilöitä järjestäytyneen rikollisryhmän osana on varsin korkea – etenkin tietoverkkorikoksissa näyttötaakka voi osoittautua erittäin vaikeaksi täyttää. Tietoverkkorikoksista epäillyt henkilöt ovat usein verkostoituneita, mutta jälkien ja näytön peittäminen on rikostyypeille ominaista. Esimerkiksi haittaohjelmarikoksissa tekijät toimivat usein alihankinta- ja värväysperusteella. Tämän vuoksi perinteiset rikollisryhmän määritelmät eivät toimi oikein hyvin. Syyttäjänvirasto ei esitä suoranaista ratkaisuehdotusta, mutta pitää potentiaalisena soveltamisongelmaa, joka olisi syytä huomioida jatkossa.

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.

PM huomauttaa, että syyteoikeutta koskeva säännös ei voi koskea sotilasoikeudenkäyntiasioita, koska nämä eivät sotilasoikeudenkäyntilain 4 §:n 3 momentti huomioon ottaen ole ns. asianomistajarikoksia; ks. ”Muita huomioita” käsittelevässä jaksossa esitetty.

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.

PM huomauttaa, että sotilasoikeudenkäyntiasioissa toimenpiteistä luopuminen virallisen syyttäjän toimenpitein ei ole mahdollista vähäisyysperusteella, jos toimivaltainen kurinpitoesimies on lähettänyt asian syyttäjän harkittavaksi; ks. ”Muita huomioita” käsittelevässä jaksossa esitetty. Lausunnossa todetaan, että voimassa olevassa laissa on vastaava toimenpiteistä luopumista koskeva säännös.

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.

Helsingin syyttäjäviraston mukaan harkittavaksi voisi tulla, pitäisikö tietomurtoa vastaava lavennus, joka on kirjattu RL 38 luvun 8 §:n 2 momenttiin, lisätä myös viestintäsalaisuuden loukkaamisen tunnusmerkistöön, jossa ei ole samanlaista haavoittuvuuden hyväksi käyttämistä. Syyttäjänvirasto huomauttaa, että esimerkiksi tietojärjestelmän haavoittuvuutta hyväksi käyttäen saatu tieto sähköisesti tallennetusta viestistä täyttäisi

todennäköisesti vain tietomurron tunnusmerkistön. Kun viestintäsalaisuuden loukkauksen rangaistavuuden edellytyksenä on, että viesti on sähköisesti tai muulla vastaavalla teknisellä keinolla suojattu ulkopuolisilta, olisi loogista, että tunnusmerkistöä ei olisi rajattu pelkästään suojauksen murtamisen kriteeriin.

EAOA toteaa lausunnossaan viestintäsalaisuuden loukkauksen osalta, että perusoikeuksien välisen oikeudenmukaisen tasapainon löytäminen on viime kädessä riippuvainen arvostuksista. Ehdotettuja rikoslain muutoksia tulisi viestintäsalaisuuden loukkauksen osalta arvioida vielä Euroopan ihmisoikeussopimuksen määräysten ja ihmisoikeustuomioistuimen oikeuskäytännön valossa. EAOA viittaa lausunnossaan erityisesti tapauksiin K.U. v. Finland (nro 2872/02, EIT 2.12.2008) ja I. v. Finland (nro 40412/98, EIT 17.7.2008).

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. *teko 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.

VKSV ehdottaa, että törkeässä tietoliikenteen häirinnässä 5 kohta siirrettäisiin ehdotetun 3 kohdan paikalle ja muut kohdat seuraisivat sitä esitetyssä järjestyksessä; ks. törkeää datavahingontekoa koskevan pykälän yhteydessä esitetty.

PM esittää, että muotoilu ”teko kohdistuu laitteeseen, tietojärjestelmään tai viestintään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon” muutettaisiin muotoon ”teko kohdistuu laitteeseen, tietojärjestelmään tai viestintään, jonka vahingoittaminen vaarantaisi yhteiskunnan elintärkeän toiminnon”. PM:n perustelut ehdotukselle on avattu törkeää datavahingontekoa koskevan pykälän yhteydessä.

Helsingin syyttäjänvirasto ehdottaa harkittavaksi, tulisiko listauksessa vielä erikseen mainita esimerkiksi elintarvikehuolto ja finanssipalvelut. Järjestäytyneen rikollisryhmän kvalifiointiperusteeseen liittyen syyttäjänvirasto nostaa esiin mahdollisen soveltamisongelman. Ks. törkeää datavahingontekoa koskevan pykälän yhteydessä esitetty.

FK esittää lausunnossaan huomion ”elintärkeää infrastruktuuria” koskevasta kvalifiointiperusteesta; ks. törkeää datavahingontekoa koskevan pykälän yhteydessä esitetty.

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. *teko 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.

VKSV ehdottaa, että mietinnössä ehdotettujen törkeiden tekomuotojen samankaltaisetrikoksen kvalifiointiperusteet voisivat olla johdonmukaisesti samassa ja todennäköisessä esiintymisjärjestyksessä – tällöin perusjärjestys olisi törkeän tietojärjestelmän häirinnässä esitetty.

PM esittää, että muotoilu ”teko kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon” muutettaisiin muotoon ”teko kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi yhteiskunnan elintärkeän toiminnon”. PM:n perustelut ehdotukselle on avattu törkeää datavahingontekoa koskevan pykälän yhteydessä.

Helsingin syyttäjänvirasto ehdottaa harkittavaksi, tulisiko listauksessa vielä erikseen mainita esimerkiksi elintarvikehuolto ja finanssipalvelut. Järjestäytyneen rikollisryhmän kvalifiointiperusteeseen liittyen syyttäjänvirasto nostaa esiin mahdollisen soveltamisongelman. Ks. törkeää datavahingontekoa koskevan pykälän yhteydessä esitetty.

FK esittää lausunnossaan huomion ”elintärkeää infrastruktuuria” koskevasta kvalifiointiperusteesta; ks. törkeää datavahingontekoa koskevan pykälän yhteydessä esitetty.

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.

Helsingin syyttäjänvirasto pitää erittäin kannatettavana sitä, että säännöksen 2 momentin 2 kohdassa ehdotetaan laajennettavaksi ”murtautumisen” määritelmää. Syyttäjänviraston mukaan kyseessä on usein juuri tietojärjestelmän haavoittuvuuden hyväksi käyttäminen eikä suora murtautuminen tietojärjestelmään, esimerkkinä esityksessäkin mainittu SQL-injektiotekniikka.

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.

VKSV ehdottaa, että törkeässä tietomurrossa 1 ja 2 kohta vaihtaisivat paikkaa; ks. törkeää datavahingontekoa koskevan pykälän yhteydessä esitetty.

Helsingin syyttäjänvirasto nostaa esiin mahdollisen soveltamisongelman liittyen järjestäytyneen rikollisryhmän kvalifiointiperusteeseen; ks. törkeää datavahingontekoa koskevan pykälän yhteydessä esitetty.

9 b §

Identiteettivarkaus

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

Pirkanmaan käräjäoikeus pitää ehdotettua identiteettivarkautta koskevaa säännöstä tarpeellisena jo kunkin henkilön oman yksilöllisyyden suojaamiseksi. On myös hyvä, että säännös suojaa henkilön identiteettiä muutoinkin kuin tietojärjestelmien käytössä.

Varsinais-Suomen käräjäoikeus pitää ehdotettua säännöstä identiteettivarkaudesta riittävän tarkkana laillisuusperiaatteen näkökulmasta ja arvioi pykälän kattavan suurimmanosan kriminalisoinnin tarpeen aiheuttavista tilanteista. Kriminalisointi on toteutettu mietinnössä tavalla, joka vastaa käräjäoikeuden aikaisempaa käsitystä kriminalisointitarpeesta ja sen perusteista.

SM, VKSV, Helsingin ja *Sisä-Suomen syyttäjänvirastot, EK, FK, SAK* ja *dosentti Seppo Virtanen* katsovat mietintöön sisältyvässä eriävässä mielipiteessä esitetyin tavoin, että viranomaisilla tulee olla käytettävissä riittävät tutkintamenetelmät identiteettivarkauksien selvittämisessä. Lausunnonantajat epäilevät nykyisen esityksen riittävyyttä tutkintavaltuuksien osalta.

SM toteaa teon rangaistusmaksimin olevan vain sakkoa, mikä ei mahdollistaisi tapausten selvittämisessä pakkokeinolain 10 luvun 6 §:ssä säädetyn televalvonnan käyttämistä. Tilannetta, jossa esitutkintaviranomaisella ei olisi mitään mahdollisuuksia selvittää asianomistajan nimissä tehtyjen verkkoviestien oikean kirjoittajan henkilöllisyyttä, ei voida SM:n mukaan pitää oikeudenmukaisena asianomistajan oikeusturvan kannalta. SM viittaa myös Jyrki Kataisen 22.6.2011 vahvistettuun hallitusohjelmaan, jossa todetaan, että ”Turvataan keinot torjua identiteettivarkauden kaikissa tapauksissa. Huolehditaan kansalaisten oikeusturvan yhdenmukaisesta toteutumisesta digitaalisessa ympäristössä”. SM:n mukaan säännös ei esitetyssä muodossaan turvaa niitä keinoja, joita tarvitaan identiteettivarkauden torjunnassa. Myöskään yleisestävää vaikutusta ei muodostu eikä kansalaisten yhdenvertainen oikeusturva toteudu. SM esittää, että pakkokeinolain 10 luvun 6 §:ssä säädettyjä televalvonnan perusteita täydennetään siten, että televalvonta olisi mahdollista identiteettivarkauden selvittämisessä.

VKSV pitää perusteltuna ja tarpeellisena uutta identiteettivarkauden kriminalisointia itsenäisenä rikoksena. VKSV yhtyy mietinnössä esitetyn eriävän mielipiteen huoleen siitä, että pelkällä rangaistussäännöksellä ei saavuteta mitään, mikäli viranomaisilla ei ole aina käytettävissä riittäviä telepakkokeinoja tunnistamistietojen saamiseksi ja rikoksen selvittämiseksi. VKSV esittää eriävässä mielipiteessä esitetyin tavoin identiteettivarkauden lisäämistä pakkokeinolain 10 luvun 6 §:n 2 momentin luetteloon, esimerkiksi 3 kohtaan, jotta televalvonta olisi käytettävissä myös itsenäisissä identiteettivarkauksissa. Samalla voi olla syytä tarkentaa myös vahingonteko-nimike datavahingonteoksi.

Helsingin syyttäjänvirasto arvioi käytännössä ongelmalliseksi muodostuvan sen, että jutun tutkinta nykyisten pakkokeinosäännösten mukaisesti ei olisi riittävää. Syyttäjänvirasto toteaa, että todennäköisesti tyypillisin identiteettivarkaus tällä hetkellä on valeprofiili sosiaalisessa mediassa, ja juttujen tutkiminen vaatii usein aikaa vieviä ja niiden vakavuuteen nähden raskaita tutkintakeinoja. Jotta tutkinnassa voitaisiin edetä riittävän tehokkaasti, syyttäjänvirasto katsoo, että pakkokeinolaissa tulisi mahdollistaa televalvonnan käyttö myös identiteettivarkauksissa. Syyttäjänvirasto tuo esiin sen, että yleisestävyyden kannalta olisi välttämätöntä antaa mahdollisille tekijöille viesti siitä, että kiinnijäämisriski on todellinen ja käytettävissä olevat tutkintakeinot ovat riittävän tehokkaat. Syyttäjänvirasto toteaa olevan vaarana, että kynnys lopettaa juttujen tutkinta jo esitutkinnan aikana saattaa muodostua matalaksi, mikäli identiteettivarkauden tutkintaa ei tosiasiassa pystytä hoitamaan menestyksekkäästi.

EK pitää identiteettivarkauden kriminalisoimista erittäin tärkeänä. EK muistuttaa, että identiteettivarkaus olisi sakkouhkainen teko, johon telepakkokeinojen käyttöala ei ulottuisi. Tietoverkoissa tapahtuvien identiteettivarkausrikosten yhteydessä esitutkintaviranomaisella ei olisi käytännössä mahdollisuuksia selvittää tekijän henkilöä eikä siten tutkia asiaa – kriminalisointi jäisi tältä osin hyödyttömäksi. EK esittää eriävässä mielipiteessä esitetyin tavoin, että identiteettivarkaus lisätään pakkokeinolain 10 luvun 6 §:n 2 momenttiin uudeksi televalvonnan perusterikokseksi, jotta identiteettivarkauksien tutkinta ylipäätään tulee mahdolliseksi.

SAK:n mukaan uusi identiteettivarkautta koskeva kriminalisointi on perusteltu lisäys lainsäädäntöön. SAK:n mukaan mietinnössä esitetyn eriävän mielipiteen osalta olisi hyvä vielä tarkemmin selvittää, onko varsinainen työryhmän esitys riittävä. SAK toteaa, että identiteettivarkauksien tehokas selvittäminen ja rikoksentekijöiden etsiminen edellyttää viranomaisilta riittäviä toimivaltuuksia – muuten voi käydä niin, että ehdotetulla kriminalisoinnilla ei käytännössä ole merkitystä.

Dosentti Seppo Virtasen mukaan identiteettivarkauden tuominen osaksi rikoslainsäädäntöä on tärkeä parannus nykytilanteeseen. Tutkintamenetelmien osalta Virtanen viittaa mietinnössä esitettyyn eriävään mielipiteeseen ja esittää jatkovalmistelussa pohdittavaksi, mahdollistaako esitys riittävät työkalut identiteettivarkauden tutkinnalle itsenäisenä rikoksena vai vaatiiko kunnollinen tutkinta aina rinnalleen epäilyn vakavammasta rikoksesta. Virtanen katsoo, että identiteettivarkauksia tulisi voida tutkia myös itsenäisinä rikoksina ja käytettävissä olevien tutkintamenetelmien tulee tällöin olla riittävän kattavat.

Sisä-Suomen syyttäjänvirasto katsoo tarpeelliseksi mahdollistaa riittävien pakkokeinojen käyttö esimerkiksi pakkokeinolakia muuttamalla; mietinnössä mainitut keinot eivät takaa tätä tyydyttävästi. Lisäksi syyttäjänvirasto katsoo, että identiteettivarkaus ei ole saanut mietinnössä ansaitsemaansa huomiota ja asemaa. Syyttäjänvirasto toteaa, että verkkoympäristössä on yleistynyt toisen henkilöllisyyden käyttö taloudellisen hyödyn tavoittelun lisäksi myös puhtaassa haittaamistarkoituksessa. Mahdollisuuksia on rajattomasti, vaikutukset ovat paljon vahingollisemmat ja teon moitittavuus on huomattavasti suurempi kuin esimerkiksi perinteisessä kunnianloukkausrikoksessa, jossa tekijä toimii omalla henkilöllisyydellään tai henkilöllisyytensä vain salaten. Esityksen perusteluista syyttäjänvirasto haluaa poistettavaksi maininnan siitä, että ”erehtymisen vaaraa ei esimerkiksi olisi, jos toiminta on selkeästi tunnistettavissa satiiriksi”, koska käytännön soveltamisohjeeksi nouseva lausuma on liian tulkinnan- ja arvostuksenvarainen. Syyttäjänvirasto huomauttaa, että satiiri pitää olla mahdollista esittää varastamatta toisen identiteettiä, eikä sananvapauden käyttämiseen yleensäkään saa kuulua oikeus toimia toisen henkilöllisyyttä hyväksi käyttäen. Syyttäjänvirasto katsoo myös, että rangaistusasteikon olisi vastattava paremmin teon rangaistusarvoa.

FK pitää erittäin hyvänä, että rikoslakiin ehdotetaan otettavaksi identiteettivarkautta koskeva säännös. Mietintöön sisältyvän eriävän mielipiteen mukaisesti FK pitää kuitenkin välttämättömänä, että esitutkintaviranomaiselle turvataan riittävät mahdollisuudet telepakkokeinojen käyttämiseen myös niissä tilanteissa, joissa identiteettivarkaus esiintyy muista rikoksista erillisenä itsenäisenä rikoksena. FK toteaa, että pelkkä epäily

sähköisen identiteetin joutumisesta vääriin käsiin riittää usein siihen, ettei identiteettiin voi enää luottaa vaan sen laillisen omistajan on ryhdyttävä ylimääräisiin toimenpiteisiin sen vaihtamiseksi tai turvaamiseksi. FK:n mukaan mahdollista on myös, että aika identiteetin anastamisen ja hyödyntämisen välillä on pitkä, mikä tosiasiallisesti voi estää esitutkintatoimenpiteiden käynnistämisen. Näistä syistä teon rangaistavuutta ei FK:n näkemyksen mukaan tulisi kytkeä identiteettitiedon oikeudettomaan käyttöön taikka taloudellisen vahingon tai haitan aiheuttamiseen vaan jo identiteettitietojen oikeudettoman keräämisen ja hallussapidon tulisi olla rangaistavaa. FK pitää sakkorangaistusta riittämättömänä sekä rangaistuksen ennaltaehkäisevän vaikutuksen että epäiltyjen rikosten tutkinnan kannalta. FK katsoo, että rangaistusasteikko tulisi määritellä niin, että vankeusrangaistuksenkin määrääminen olisi tarvittaessa mahdollista – tätä FK perustelee sillä, että verkkotalouden laajetessa identiteetin merkitys ja arvo haltijalleen kasvaa ja tähän aineettomaan henkilökohtaiseen oikeuteen liittyy myös varallisuusoikeudellisia piirteitä. FK toteaa olevan mahdollista, että käytännön tilanteissa laajamittainen tai ammattimainen identiteettien varastaminen voisi tulla rangaistavaksi muidenkin kuin identiteettivarkauden tunnusmerkistön pohjalta. FK kuitenkin katsoo, että olisi perusteltua säätää erikseen törkeästä tekomuodosta niitä tilanteita varten, joissa törkeän rikoksen tunnusmerkistön täyttävä identiteettivarkaus esiintyy erillisenä itsenäisenä rikoksena. Tulisi myös pohtia, onko identiteettivarkauden tutkinnan aloittaminen kaikissa tilanteissa perusteltua jättää asianomistajan ilmoituksen varaan.

EAOA:n mukaan kriminalisoinnin rajaus tilanteisiin, joissa on aiheutunut taloudellista vahinkoa tai muuta vähäistä suurempaa haittaa, jättää sijaa tulkinnalle. EAOA pitää esityksen puutteena sitä, että identiteettivarkautta koskevaa oikeuskäytäntöä on siteerattu ja arvioitu varsin rajoitetusti.

Suomen Yrittäjät katsoo, että tunnusmerkistön sanamuotoa tulisi harkita osin uudelleen siten, että säännöksestä tulisi täsmällisempi. Säännöksestä voisi ilmetä suoraan se, että kyse on nimenomaan toisena henkilönä oikeudettomasti esiintymisestä, ei pelkästään tietojen oikeudettomasta käytöstä. Suomen Yrittäjät ehdottaa seuraavaa sanamuotoa: ”Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti *esiintyy toisena henkilönä käyttämällä tämän* henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa *ja näin aiheuttaa* taloudellista tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.” Tämä sanamuoto rajaisi pois ne tilanteet, joissa käytetään toisen yksilöivää tietoa sinänsä oikeudettomasti, mutta siten, ettei sitä hyväksi käyttäen yritetä esiintyä toisena henkilönä. Sanamuoto merkitsisi myös identiteettivarkauden selvempää erottamista immateriaalioikeudellisista rikossäännöksistä, joissa voi olla kyse yrityksen yksilöivien tietojen oikeudettomasta käytöstä mutta ei välttämättä kuitenkaan tilanteesta, jossa esiinnytään yrityksenä.

Suomen Yrittäjät esittää useita tarkennuksia myös lakiehdotuksen perusteluihin. Säännöksen perusteluissa tulisi huomioida yritysten asema identiteettivarkauden kohteena, sillä ”toinen” voi olla myös oikeushenkilö. Yritysten osalta olisi syytä avata myös käsitettä ”yksilöivä tieto”; Suomen Yrittäjät viittaa lausunnossaan esimerkiksi yrityksen nimeen, aputoiminimeen, y-tunnukseen tai tavaramerkkiin. Lisäksi huomiota tulisi perusteluissa kiinnittää yritysten osalta siihen, mikä on yrityksen yksilöivän tiedon ”oikeudetonta” käyttöä. Sanamuodon osalta jää epäselväksi se, soveltuisiko säännös tilanteeseen,

jossa yrityksestä levitetään valheellista tietoa siten, että yritykseen viitataan sen nimellä tai muulla yksilöivällä tiedolla. Esimerkkitilanteena Suomen Yrittäjät mainitsee julkisuudessa esitetyn valheellisen väitteen siitä, että yritys harjoittaa laitonta toimintaa. Luonnollisten henkilöiden osalta kyseeseen voi tulla kunnianloukkaus, mutta yritysten osalta vastaavaa säännöstä ei ole. Suomen Yrittäjät toteaa olevan oma kysymyksensä, pitäisikö rikoslakiin lisätä yritystä koskevan valheellisen tiedon levittämistä koskeva kriminalisointi erityisesti kaikkein räikeimpien tilanteiden varalta.

Suomen Yrittäjät katsoo, että lakiehdotuksessa olisi myös syytä selostaa tarkemmin sitä, miten oikeushenkilöön kohdistuva identiteettivarkaus voi toteutua. Esityksessä olisi myös hyvä pohtia identiteettivarkauden suhdetta muihin säännöksiin, jotka koskevat yrityksen yksilöivien tietojen loukkaamista. Suomen Yrittäjät nostaa esiin immateriaalioikeusloukkaukset, kuten rikoslain 49 luvun 2 §:n teollisoikeusrikoksen, tavaramerkkilain 39 §:n tavaramerkkirikkomuksen tai toiminimilain 22 §:n toiminimen loukkauksen. Suomen Yrittäjät toteaa, että mietinnön mukaan identiteettivarkauden tekijä voidaan tuomita myös muusta kuin identiteettivarkaudesta – tätä koskeva esimerkki olisi selvyyden vuoksi hyvä ottaa esille niitä tilanteita varten, jossa identiteettivarkauden kohteena on yritys. Lisäksi perusteluissa olisi hyvä pohtia yhtiön edustajan asemaa sellaisissa tilanteissa, joissa säännöksen mukaiseen erehdyttämiseen käytetään sekä yrityksen että sen edustajana olevan luonnollisen henkilön tietoja – olisiko asianomistaja-asema tällöin sekä yrityksen edustajalla että yrityksellä?

10 §

Syyteoikeus

— — — — — — — — — — — — — —

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

PM ehdottaa lausunnossaan identiteettivarkautta koskevan pykäläviittauksen lisäämistä sotilasoikeudenkäyntilakiin; ks. ”Muita huomioita” käsittelevässä jaksossa esitetty. Tästä seuraa, että syyteoikeutta koskeva säännös ei voisi koskea sotilasoikeudenkäyntiasioita, koska nämä eivät sotilasoikeudenkäyntilain 4 §:n 3 momentti huomioon ottaen ole ns. asianomistajarikoksia.

Varsinais-Suomen käräjäoikeus pitää hyväksyttävinä työryhmän perusteluita 10 §:n mukaisesta syyteoikeudesta.

13 §

Määritelmät

Tämän luvun 3, 6, 7 a, 7 b ja 8 §:ssä tietojärjestelmällä tarkoitetaan myös direktiivin 2013/40/EU 2 artiklan a kohdassa tarkoitettua 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.

Tämän luvun 3, 7 a ja 8 §:ssä datalla tarkoitetaan myös direktiivin 2013/40/EU 2 artiklan b kohdassa tarkoitettua sellaisessa muodossa olevien tosiseikkojen, tietojen, tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä, mukaan lukien ohjelmat, joiden avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon.

Pirkanmaan käräjäoikeus toteaa tietojärjestelmien ja datan määritelmien osalta, että lakiehdotuksen esityksillä on haluttu varmistaa, että direktiivin vähimmäisvelvoitteet tulevat katetuksi. Lakiehdotuksessa on kuitenkin käytetty muitakin termejä datan yhteydessä tai rinnalla. Käräjäoikeus viittaa 35 luvun 3 a §:ssä tarkoitettuun datavahingontekoon sekä 38 luvun 8 §:ssä tarkoitettuun tietomurtoon. Lisäksi käräjäoikeus viittaa hallituksen esitykseen (153/2006, s. 68), jossa todetaan datan tarkoittavan tietoa, joka on tietokoneessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla. Käräjäoikeus edelleen toteaa hallituksen esityksessä (153/2006 s. 16) viitattavan toiseen hallituksen esitykseen (HE 66/1988). Tältä osin käräjäoikeuden mukaan todetaan, että rikoslain vahingontekoa koskevan säännöksen esitöiden mukaan tietovälineelle tallennetulla tiedolla tarkoitetaan tiedon asiasisältöä eli informaatiota ja asiasisältöä viestittäviä merkkejä eli dataa. Käräjäoikeuden näkemyksen mukaan jää jonkin verran epäselvä kuva siitä, mitä nyt ehdotetuissa säännöksissä tarkoitetaan tiedolla ja datalla. Käsitteiden sisältöjen yhdenmukaisuudella on suuri merkitys rikosoikeudessa, ja määritelmillä tullee olemaan vielä suurempi merkitys tietotekniikan kehittyessä.

FiCom toteaa, että työryhmä ehdottaa määritelmiä, joiden kirjallisen ilmaisun mukaan ne tarkoittavat myös ko. direktiivin mukaisia tietojärjestelmiä ja dataa. FiCom tuo esiin, että voimassa olevassa rikoslaissa tietojärjestelmä-käsite löytyy muun muassa seuraavista kohdista, jotka eivät kuulu nyt tarkastelussa olevaan asiakokonaisuuteen: yritysvakoilu (30 luvun 4 §), tuhotyö (34 luvun 1 §), petos (36 luvun 1 §) ja tekijänoikeusrikos (49 luvun 1 §). FiCom toteaa, että näissä rikoslain kohdissa tietojärjestelmä tarkoittaa käänteispäätelmän mukaan jotain muuta kuin 38 luvun 13 §:n 1 momentissa määriteltyä. Data-käsitteen osalta vastaava tarkastelu liittyy rikoslain 36 luvun 1 §:ään, jossa käytetään sanaa data. FiCom huomauttaa, että mietinnön mukaan lisättäväksi ehdotetut määritelmät kattaisivat ainoastaan ne kriminalisoinnit, joiden on tarkoitettu kattavan direktiivin velvoitteet. FiCom ei pidä tarkoituksenmukaisena sitä, että käsitteet määritellään tapauskohtaisesti alkuperäisen sovellettavan sopimuksen, direktiivin tai muun

lähteen mukaan. Kyseisellä perusteella valitut, toisistaan poikkeavat määritelmät merkitsevät käytännössä sitä, että jopa saman säädöksen sisällä tietyllä termillä saattaa olla useita eri merkityksiä – tämä tekee lainsäädännöstä monimutkaista ja lisää varsinaisen säännöksen tulkinnanvaraisuutta. FiCom ehdottaa, että käsitteiden ”tietojärjestelmä” ja ”data” sisältö ja merkitys yhtenäistettäisiin koko lakia koskien.

3.2 Laki pakkokeinolain 10 luvun 3 §:n muuttamisesta

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*;
— — — — — — — — — — — — — — —

PM toteaa, että ehdotetulla muutoksella ei tulisi olemaan vaikutuksia puolustusvoimien suorittamaan esitutkintaan, koska salaisista pakkokeinoista telekuuntelu ei sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain (255/2014) mukaan ole esitutkintaa suorittavien pääesikunnan virkamiesten käytettävissä.

4 Muita huomioita

EAOA muistuttaa lausunnossaan, että direktiivien noudattamisen edellyttämiä toimenpiteitä täytäntöön pantaessa viranomaisten ja tuomioistuinten on tulkittava kansallista oikeutta direktiivien mukaisesti. Ne eivät myöskään saa nojautua sellaiseen direktiivien tulkintaan, joka johtaisi ristiriitaan perusoikeuksien tai EU-oikeuden yleisten periaatteiden kanssa. Lisäksi EAOA tuo esiin, että Euroopan Unionin tuomioistuin on 8.4.2014 julistanut pätemättömäksi direktiivin, joka määrittelee oikeuden kerätä ja säilyttää kansalaisten viestintätietoja rikollisuuden torjuntaa varten. Tuomioistuimen mielestä lain tulisi rajoittaa enemmän sitä, millaisia tietoja voidaan kerätä ja samoin viranomaisten pääsyä tietoihin.

OKA toteaa teknisenä huomiona, että mietinnön sivulla 24 on kahteen kertaan viitattu hallituksen esitykseen HE 156/2014 vp ilmeisesti tarkoitetun hallituksen esityksen HE 153/2014 vp sijasta.

PM tuo lausunnossaan esiin huomion koskien sotilasoikeudenkäyntiasioita. PM toteaa, että sotilasoikeudenkäyntilain 2 §:n 2 momentin mukaan sotilasoikeudenkäyntiasiana käsitellään syyte sotilasta vastaan teosta, josta on säädetty rangaistus muun muassa rikoslain 35 luvussa ja eräissä 38 luvun pykälissä, jos teko on kohdistunut puolustusvoimiin tai toiseen sotilaaseen. PM katsoo, että viittaus ehdotettuun identiteettivarkautta koskevaan rikoslain 38 luvun 9 b §:ään tulisi lisätä sotilasoikeudenkäyntilain 2 §:n 2 momentin luetteloon – identiteettivarkaus edes toiseen sotilaaseen tai puolustusvoimiin kohdistettuna ei olisi ns. epävarsinainen sotilasrikos ilman mainitun momentin muuttamista. Identiteettivarkaus voisi tulla tutkittavaksi rikosnimikkeeksi esimerkiksi palvelusrikosten tai omaisuus- tai väärennysrikosten yhteydessä. PM:n mukaan identiteettivarkaus tapahtuu usein osana muuta rangaistavaa käyttäytymistä, jolloin järkevänä ei voida pitää sitä, että puolustusvoimat joutuisi siirtämään tämän rikosnimikkeen osalta esitutkinnan poliisille.

Törkeää datavahingontekoa koskevan pykälän yhteydessä esitettyä vastaavasti PM ehdottaa, että myös rikoslain 34 luvun 1 §:n tuhotyötä koskevassa tekstissä ”tärkeitä toimintoja” kuvaava esimerkinomainen luettelo voitaisiin korvata muotoilulla ”yhteiskunnan elintärkeä toiminto”. Tuhotyötä koskevaa pykälää ei ole mietinnössä ehdotettu muutettavaksi. PM esittää, että nykyinen voimassaoleva muotoilu ”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” muutettaisiin kuulumaan seuraavasti: ”Tuhotyöstä tuomitaan myös se, joka omaisuutta vahingoittamalla tai tuhoamalla taikka tuotanto-, jakelu- tai tietojärjestelmän toimintaan oikeudettomasti puuttumalla aiheuttaa vakavan vaaran yhteiskunnan elintärkeälle toiminnolle”.

SM viittaa lausunnossaan tietoverkkorikosdirektiivin artiklaan 13 koskien jäsenvaltioiden välistä tiedonvaihtoa ja ympärivuorokautista kansallista yhteyspistettä. Tähän liittyen SM toteaa, että Suomen kyberturvallisuusstrategian toimeenpano-ohjelmassa on esitetty poliisin operatiivisen tietoverkkorikososaamisen liittämistä jo olemassa olevaan poliisin kansalliseen 24/7 yhteyspisteeseen. SM:n lausunnossa todetaan, että poliisihallituksen mukaan toiminnan suunnittelu on jo aloitettu. Toiminnan aloittaminen vaatii lisäresursseja.

Dosentti Seppo Virtanen tuo esiin, että tulevaisuudessa sähköinen yhteiskunnallinen vaikuttaminen tulee voimakkaasti lisääntymään, joten on erityisen tärkeää huolehtia siitä, että todennäköisesti käyttöön tuleva sähköinen äänestäminen ja sen mahdollistavat järjestelmät tulevat huomioiduksi tietoverkkorikoslainsäädännössä. Virtasen näkemyksen mukaan esitys kattaa myös sähköisen äänestämisen suojaamisen ja sen häirinnän rangaistavuuden, mutta tekstissä olisi kuitenkin hyvä tuoda esille myös tähän liittyvät perustelut esityksen kokonaiskattavuuden kannalta.

Lisäksi Virtanen huomauttaa, että esitys ei juuri ota kantaa identiteettivarkauden uhrin mahdollisuuksiin normalisoida elämänsä mahdollisen mittavan identiteettivarkauden jälkeen. Virtanen toteaa kuitenkin, että tämä ei sinänsä olekaan suoraan osa rikoslainsäädäntöä ja rikoksen selvittämistä vaan jälkihoitoa. Virtanen tuo esiin, että henkilön olisi todennäköisesti huomattavasti helpompaa edistää identiteettivarkaudesta johtuvien ongelmiensa ratkomista, jos hän saisi identiteettivarkauden uhrin statuksen viranomaiselta. Virtanen toteaa, että viranomaisellekin voitaisiin saada, niin haluttaessa, virallinen velvoite avustaa identiteettivarkauden uhria. Status voitaisiin antaa henkilölle, jonka todetaan joutuneen identiteettivarkauden uhriksi mietinnön määritelmien mukaan. Virtanen korostaa, että uhrin kannalta on erityisen tärkeää, että rekisterimerkinnät saadaan mahdollisimman nopeasti palautettua ennalleen ja erilaiset virheelliset rekisterimerkinnät poistettua. Virtasen mukaan virheellisen merkinnän syntytilannetta voi olla haasteellista jäljittää ja todentaa sen olevan virheellinen usean vuoden jälkeen ja etenkin kansainvälisellä tasolla.

LIITE: LAUSUNTOPYYNNÖT

Liikenne- ja viestintäministeriö*
Puolustusministeriö*
Sisäministeriö*
Valtiovarainministeriö

Eduskunnan oikeusasiamies*
Valtioneuvoston oikeuskansleri*

Helsingin käräjäoikeus
Pirkanmaan käräjäoikeus*
Varsinais-Suomen käräjäoikeus*

Valtakunnansyyttäjänvirasto*
Helsingin syyttäjänvirasto*
Länsi-Suomen syyttäjänvirasto
Sisä-Suomen syyttäjänvirasto*

Kilpailu- ja kuluttajavirasto
Tietosuojavaltuutetun toimisto
Viestintävirasto*

Oikeuspoliittinen tutkimuslaitos

Electronic Frontier Finland (EFFI) ry
Elinkeinoelämän keskusliitto EK ry*
Finanssialan Keskusliitto ry*
Finnet-liitto ry
Finnish Information Security Cluster (FISC) ry
Oikeuspoliittinen yhdistys Demla ry
Piraattipuolue ry
Suomen Ammattiliittojen Keskusjärjestö SAK ry*
Suomen Asianajajaliitto
Suomen Internet-yhdistys ry
Suomen Lakimiesliitto ry
Suomen seutuverkot ry
Suomen Syyttäjäyhdistys ry
Suomen Tuomariliitto ry
Suomen Yrittäjät ry*
Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry*
Tietoturva ry*

Professori Asko Lehtonen, Vaasan yliopisto
Professori Kimmo Nuotio, Helsingin yliopisto
Professori Raimo Lahti, Helsingin yliopisto
Apulaisprofessori Sakari Melander, Helsingin yliopisto
Dosentti Seppo Virtanen, Turun yliopisto*

* tähdellä on merkitty ne tahot, jotka ovat toimittaneet lausuntonsa

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

ISSN-L 1798-7105
ISBN 978-952-259-391-7 (PDF)

Oikeusministeriö
PL 25
00023 VALTIONEUVOSTO
www.oikeusministerio.fi

Justitieministeriet
PB 25
00023 STATSRÅDET
www.oikeusministerio.fi