Oikeusministeriö
Lainvalmisteluosasto
PL 25
00023

Asia: Lausunto tietoverkkorikosdirektiivin täytäntöönpanoa koskevasta mietinnöstä

Viite: OM 15/41/2013

Oikeusministeriö on pyytänyt allekirjoittaneelta lausuntoa asiakohdassa tarkoitetusta ministeriön työryhmän mietinnöstä.

Kiitän minua kohtaan esitetystä luottamuksesta.

Lausuntonani esitän kunnioittaen seuraavan.

Kokonaisuutena arvioiden mietintöä on pidettävä erittäin hyvänä, joten lainsäädäntöhanke voidaan toteuttaa mietinnön pohjalta.

Jatkovalmistelussa olisi suositeltavaa kiinnittää huomiota eräisiin yksityiskohtiin, joiden osalta olisi aiheellista harkita muutamien muutosten ja täydennysten tekemistä. Käsittelen jäljempänä näitä muutoskohtia, jotka olen jaotellut neljään pääryhmään:
1) Viestintäsalaisuuden loukkaus; tunnusmerkkien "suojauksen murtaen" poistaminen.
2) Identiteettivarkaus; tunnusmerkistön laajuus ja rangaistusarvo.
3) Monipolvinen viittaustekniikka.
4) Eräät yksityiskohdat.

1. Viestintäsalaisuuden loukkaus (RL 38:3)

Oikeusministeriön työryhmän mietinnössä on asianmukaisesti kiinnitetty huomiota viestintäsalaisuuden loukkausta koskevan RL 38 luvun 3 §:n 1 momentin 1) kohdan tunnusmerkistön puutteellisuuksiin, kuten rajoittuneisuuteen. Mietinnössä (s. 30-33) on selvitetty RL 38 luvun 3 §:n 1 momentin 1) ja 2) kohtien tunnusmerkistöjen välisiä eroja käyttäytymisen rangaistavuuden edellytysten suhteen. Sanotun momentin 1) kohdassa säädetyt rangaistavuuden edellytykset ovat paljon korkeammat kuin saman momentin 2) kohdan mukaiset edellytykset. Toisin sanoen sama sähköinen viesti saa laajempaa rikosoikeudellista suojaa mainitun 2) kohdan mukaisissa tilanteissa kuin 1) kohdassa tarkoitetussa tilanteessa.

Työryhmän mietinnössä tukeudutaan hallituksen esityksen HE 153/2006 perusteluissa lausuttuun. Tämän mukaisesti mietinnössä (s. 31) todetaan, että esimerkiksi sähköpostiviestin saama suoja perustuu RL 38:3:n säännöksen eri kohtiin viestin sijaintipaikasta riippuen. Mietinnössä lausutaan, että sähköpostiviesti saa a) televerkossa välitettävän viestin suojaa silloin, kun se on

televerkossa, ja b) ulkopuolisilta suojatun viestin suojaa silloin, kun se on osapuolen hallinnassa esimerkiksi tietokoneeseen tallennettuna.

Mietinnössä (s. 32) todetaan lisäksi hallituksen esityksiin HE 94/1993 ja HE 153/20062.9.2014 tukeutuen, että RL 38 luvun 3 §:n 1 momentin 1) kohdan säännös suojaa myös sellaista viestiä, joka sitä mihinkään siirtämättä tallennetaan tietokoneen muistiin tietyn henkilön tai henkilöpiirin luettavaksi. Mietinnössä lausutun mukaan rangaistavuuden edellytyksenä on tällöin kuitenkin se, a) että viesti on teknisin keinoin suojattu ulkopuolisilta ja b) että tiedon hankkiminen viestistä tapahtuu tämä suojaus murtaen. Vastaavia rangaistavuuden edellytyksiä ei ole asetettu saman momentin 2) kohdassa.

Mielenkiintoinen on mietinnössä (s. 32) tämän jälkeen esitetty lausuma siitä, että työryhmä on tullut siihen tulokseen, että edellä mainitut rikoslain säännökset eivät täysin kata yleissopimuksen (Euroopan neuvoston tietoverkkorikossopimuksen) tai tietoverkkorikosdirektiivin tavoitteita ja soveltamisalaa.

Mietinnössä todetaan tässä yhteydessä ensinnäkin, että direktiivin 6 artiklassa edellytetään, että viestintäsalaisuuden loukkaus tehdään teknisin keinoin, ja että sallittua olisi luonnollisesti säätää teko rangaistavaksi ilman tätä edellytystä. Mietinnössä mainitun mukaisesti rikoslain 38 luvun 3 §:n 1 kohdassa edellytetään kuitenkin “suojauksen murtamista”, mikä on rajoittavampi kriteeri kuin ”teknisin keinoin”. Mietinnössä esitetty vertailu on monessa suhteessa havahduttava. RL 38:3:n 1 momentin 1) kohdassa tarkoitettu tallennettu viesti saa rikosoikeudellista suojaa vain, jos tieto on hankittu oikeudettomasti “suojaus murtaen”. Tällaista korotettua rangaistavuuden edellytystä ei vaadita yleissopimuksessa eikä direktiivissä. Niissä puhutaan “teknisistä keinoista”. Mitään estettä ei ole myöskään sille, että oikeudettoman tiedon hankkimisen rangaistavuus ei edellyttäisi “suojauksen murtamista” eikä “teknistä keinoa”. Tällöin rangaistavuuden edellytys olisi sama RL 38:3:n 1 momentin 1) ja 2) kohdassa tarkoitetuissa tilanteissa. Hallituksen esityksessä HE 94/1993 ei aikanaan perusteltu sitä, miksi RL 38 luvun 3 §:n 1 momentin 1) kohdan rangaistavuuden edellytys on korotettu eli siinä vaaditaan tiedon hankkimista “suojaus murtaen”. Lainkohtien väliseltä erolta puuttuu rationaalinen peruste.

Mietinnössä lausutaan toiseksi, että viestintäsalaisuuden loukkausta koskevan RL 38 luvun 3 §:n tunnusmerkistön osalta on jossain määrin epäselvää, kattaako se kaikki ”teknisin keinoin” tapahtuvat tilanteet, joita direktiivin artiklassa on tarkoitettu. Mietinnön mukaan käytännössä on esiintynyt epäselvyyttä siitä, kattaako nykyinen RL 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. Mietinnön mukaan tällöin tietojärjestelmään ei välttämättä ole tunkeuduttu myöskään tietomurtosäännöksen tarkoittamassa mielessä. Mietinnössä esitetyt epäillyt tunnusmerkistön kattavuudesta ovat asianmukaisia, kun kysymys on oikeudettomasta tiedon hankkimisesta tallennetusta viestistä haittaohjelman avulla. Haittaohjelmien käyttö rikollisiin tarkoituksiin on tavattoman yleistä ICT-rikollisuudessa. Haittaohjelman ujuttaminen käyttäjän omien toimien avulla (esim. joltakin kohdesivulta, jossa käyttäjä vierailee) hänen tietokoneelleen ei oikein täytä RL 38 luvun 3 §:n 1 momentin 1) kohdan tekotapatunnusmerkkejä “suojauksen murtaen”.

Yhteenvetona työryhmän mietinnössä mainittujen seikkojen perusteella voidaan todeta, että RL 38:3.1:n 1) kohdassa tarkoitettu "tallennettu viesti" ei saa viestintäsalaisuuden loukkaamista koskevan kriminalisoinnin perusteella rikosoikeudellista suojaa, jos oikeudeton tiedon hankkiminen ei tapahdu "suojaus murtaen". Tämä on paha epäkohta lainsäädännössä. Sen sijaan RL 38:3.1:n 2 kohdan rikossäännös ei sisällä mitään lisäkriteereitä sen lisäksi, että a) tieto datasiirron sisällöstä tai b) viestin lähettämisestä tai vastaanottamisesta on hankittu oikeudettomasti, kuten on todettu työryhmän mietinnössä (sivu 33).

Olen aikanaan toisessa yhteydessä kiinnittänyt huomiota ns. takaporttien aiheuttamaan tulkintaongelmaan.[1)] Ohjelmoitsijat ovat aikaisemmin usein jättäneet ohjelmaan ns. takaportin, jota on voitu käyttää hätätapauksissa varmistusjärjestelmien ohittamiseen. Kysymyksenalaisena voidaan pitää sitä, kattaako tekotapatunnusmerkki "suojauksen murtaen" tällaisen takaportin oikeudettoman käytön. Sama ongelma koskee nykyisin eräiden ohjelma- ja laitevalmistajien tuotteisiinsa tietoisesti sijoittamia takaportteja tai -ovia (aukkoja) esim. yhdysvaltalaisen vakoiluorganisaatio NSA:n vaatimuksesta.[2)] Tarkoituksellisesti tehdyn takaportin käyttö mahtuu huonosti "suojauksen murtaen" tekotapatunnusmerkkien puitteisiin, vaikka sanaa "murtaa" on käytetty eräänlaisena kielikuvana.[3)] Oikeuskirjallisuudessa on katsottu, että RL 38:3.1:n 1) kohdan tarkoittamasta "suojauksen murtamisesta" ei ole kysymys silloin, kun tieto hankitaan sähköpostiviestistä tietojärjestelmän pääkäyttäjän (ns. järjestelmän ylläpitäjän) oikeuksilla eli käyttäjätunnuksella ja salasanalla.[4)] Tallennetun viestin osalta on käytännössä monia tilanteita, joissa viestin sisällön pitäisi saada rikosoikeudellista suojaa samoilla edellytyksillä kuin viestin tunnistamistiedot saavat RL 38:3.1:n 2) kohdan nojalla.

RL 38 luvun 3 §:n 1 momentin 1) kohdan tekotapatunnusmerkit jakautuvat kahteen osaan. Lakiesityksen perusteluissa on kutsuttu tekotapatunnusmerkkien alkuosaa perinteiseksi kirjesalaisuuden loukkaamiseksi ja loppuosaa sähköisesti tallennettua viestiä koskevaksi lisäykseksi.[5)] Tämän 1) kohdan loppuosa koskee sähköisesti tai muulla vastaavalla teknisellä keinolla tallennettua, ulkopuoliselta suojattua viestiä. Perustelujen mukaan tällä on tarkoitettu lähinnä elektronista postia

---

1) Ks. Lehtonen, Asko (1999). Tietokoneviruksella aiheutettu vahinko ja oikeudellinen vastuu. Teoksessa: Pohjois-Suomen tuomarikoulu. Julkaisuja 3/1999, sivu 172. Lapin yliopisto ja Rovaniemen hovioikeus. Rovaniemi 1999.

2) Ks. tarkemmin Greenwald, Glenn (2014). No Place to Hide. Edward Snowden and the USA. Surveillance State. New York: Metropolitan Books. ja Järvinen, Petteri (2014). Näin meitä seurataan. Jyväskylä: Docendo Oy.

3) Ks. HE 94/1993 s. 155.

4) Ks. Nyblin, Klaus (2004). Työelämän sähköposti. 2. painos. Helsinki: Talentum Media Oy s. 277 ja Lehtonen, Asko (2005). Sähköpostin rikosoikeudellisen suojan kehitys muutosten paineissa. Teoksessa: Rikos, rangaistus ja prosessi. Juhlajulkaisu Eero Backman 1945-14/5-2005, sivu 164. Toim. Ari-Matti Nuutila ja Elina Pirjatanniemi. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. A. Juhlajulkaisut n:o 15. Turku: Turun yliopisto.

5) Ks. HE 94/1993 s. 148.

(eli sähköpostia).[6] Rangaistavuuden edellytyksenä on kuitenkin, että oikeudeton tiedon hankinta viestistä tapahtuu "suojaus murtaen".

RL 38 luvun 3 §:n 1 momentin 1) ja 2) kohdan tekotapatunnusmerkkien väliset erot ovat merkittäviä. Edellisessä kohdassa edellytetään tiedon hankintaa ulkopuoliselta suojatusta viestistä läpäisemällä turvajärjestely "suojaus murtaen", kun taas jälkimäisessä kohdassa on riittävää rangaistavuuden edellytyksenä mikä tahansa "oikeudeton" tiedonhankintatapa. Tämän 2) kohdan mukaan tiedon hankinta sähköpostiviestin tunnistamistiedoista on aina rangaistavaa viestintäsalaisuuden loukkauksena, jos se tapahtuu "oikeudettomasti". Sen sijaan oikeudeton tiedon hankkiminen sähköisesti tallennetusta "viestistä" on rangaistavaa viestintäsalaisuuden loukkauksena vain, jos se suoritetaan "suojaus murtaen". Viestin tunnistamistietojen rikosoikeussuoja on selvästi vahvempi kuin itse "viestin" sisällön vastaava suoja,[7] vaikka perusoikeussäännöstä on vakiintuneesti tulkittu siten, että tunnistamistiedot eivät kuuluu perusoikeussuojan ydinalueeseen. Sama ero koskee televerkossa välitettävänä olevaa sähköpostiviestiä ja vastaanottajalle saapunutta sähköpostia, joka on tallennettu sähköisesti ulkopuolisilta suojatulla tavalla. Tiedon hankinnan rangaistavuus edellyttää edellisessä tapauksessa vain "oikeudettomuutta", kun taas jälkimmäisessä tilanteessa vaaditaan lisäksi "suojauksen murtamista".

Sähköpostiviestin sisältö saa RL 38 luvun 3 §:ssä tarkoitettua rikosoikeussuojaa kaikkea oikeudetonta tiedon hankintaa vastaan sinä lyhyenä aikana, kun viesti on välitettävänä televerkossa. Sähköpostiviestin tunnistamistietoja suojataan kaikissa tilanteissa mitä tahansa oikeudetonta tiedon hankintaa vastaan. Perille tulleen sähköpostiviestin sisältö saa tätä rikosoikeussuojaa vain, jos tiedon hankkiminen tapahtuu suojaus murtaen. Sama rajoitus koskee sähköpostiviestin sisältöä, kun viesti on tallennettu tulevaa lähettämistä varten. Saapuneita sähköpostiviestejä säilytetään yleisen käytännön mukaan tallennettuina varsinkin silloin, kun sähköpostiviesti on merkityksellinen vastaanottajalle tai hänen edustamalleen taholle. Toisinaan perille tulleet sähköpostiviestit joutuvat odottamaan sopivaa ajankohtaa lukemista, tulostamista tai vastaamista varten, joten sähköpostiviestien säilyttäminen ei ole poikkeuksellista. Edellä selostettu oikeustila ja eri tilanteiden väliset erot eivät vaikuta johdonmukaisilta ja asianmukaisilta.

PL 10 §:n 2 momentissa tarkoitettu perusoikeussuoja eli luottamuksellisen viestin salaisuus koskee vakiintuneen käsityksen mukaan ensisijaisesti viestin sisällön suojaa. Viestin sisältö kuuluu perusoikeussuojan ydinalueeseen. Luottamuksellisen viestin suoja on nimenomaisesti suojaa muun muassa suljetun viestin avaamista vastaan. Tunnistamistiedot eivät kuulu perusoikeuden ydinalueeseen. Tunnistamistietojen suojaan voidaan lailla puuttua vähäisemmillä edellytyksillä kuin viestin sisältöön.[8] RL 38 luvun 3 §:ään perustuva luottamuksellisen viestin salaisuuden rikosoikeussuoja näyttää poikkeavan perusoikeussuojan painotuksista. Viestin sisällön rikosoikeussuoja on kapeampaa ja epäselvempää kuin tunnistamistietojen suoja.

---

6) Ks. HE 94/1993 s. 149.

7) Ks. Nyblin 2004 mt s. 275 ja 279.

8) Ks. PeVL 3/1992, PeVL 47/1996, PeVL 7/1997, PeVL 26/2001 ja PeVL 9/2004.

Työryhmän mietinnössä on katsottu kaikesta huolimatta, että mietinnössä mainitut seikat rikoslain 38 luvun 3 pykälän 1 kohdan ja tallennetun tiedon osalta eivät ole erityisen merkityksellisiä direktiivin edellyttämien velvoitteiden kannalta, sillä artiklan velvoitteet koskevat tiedon hankkimista tietojärjestelmien välisestä tai sisäisestä datan siirrosta. Asianmukaiselta ei vaikuta yksilöidysti todetun puutteen korjaamatta jättäminen pelkästään sen vuoksi, että sitä ei ole nimenomaisesti edellytetty direktiivissä. Direktiiviä laadittaessa ei ole otettu huomioon kaikkien jäsenvaltioiden lainsäädännön yksittäisiä puutteita, joiden korjaaminen jää kunkin jäsenvaltion omien toimien varaan.

Tallennetun viestin suojaa koskeva puute voitaisiin yksinkertaisimmillaan korjata poistamalla RL 38 luvun 3 §:n 1 momentin 1) kohdasta ilmaisu "suojauksen murtaen". Tämä korjaus olisi suositeltavaa tehdä samassa yhteydessä, kun pannaan täytäntöön direktiivin edellyttämät muutokset.

2. Identiteettivarkaus

Työryhmän mietinnössä on esitetty viisi eri vaihtoehtoa direktiivin vaatimusten täyttämiseksi. Mietinnössä ehdotetaan valittavaksi viides toteuttamisvaihtoehto, mikä tarkoittaa identiteettivarkauden erilliskriminalisointia. Tämän vaihtoehdon tueksi esitetyt perustelut ovat asianmukaisia ja vahvoja argumentteja.

Työryhmän ehdotuksen eräistä yksityiskohdista olisi aiheellista käydä kriminaalipoliittista keskustelua.

Lakiehdotuksissa on kysymys tietoverkkorikoksista. Tällöin olisi suositeltavaa pitää lähtökohtana Internetissä tapahtuvia rikoksia, kun arvioidaan kriminalisoitavaan käyttäytymiseen tyypillisesti liittyviä vahinkoja ja haittoja. Internetin osalta olisi syytä muistaa, että Internetissä toimii kymmenittäin hakupalveluita, joiden hakukoneet keräävät tietoja kaikkialta verkosta ja jotka tallentavat kerättyjä tietoja tietovarastoihinsa mahdollisesti vuosikausiksi. Google on vain yksi hakupalveluista - mahdollisesti eniten käytetty. Identiteettivarkauteen kuuluvan henkilötiedon (esim. kuvan) julkistaminen pitkähkön ajan verkossa tiedon käyttämisen yhteydessä merkitsee käytännössä sitä, että tiedon poistoa on pyydettävä ainakin kymmenistä hakupalveluista. Tällaisten poisto-operaatioiden toteuttaminen on tavalliselle Internetin käyttäjälle lähtökohtaisesti ylivoimainen tehtävä. Eri puolilla maailmaa olevien hakupalveluiden yhteystietojen löytyminen voi olla todella työlästä ammattilaisellekin. Kielelliset seikat voivat myös muodostaa pahan esteen poistopyynnöille. Näistä lähtökohdista käsin olisi suositeltavaa harkita, tulisiko identiteettivarkauden tunnusmerkistöstä poistaa tunnusmerkit "vähäistä suurempaa". Vahingon ja haitan suhteen rangaistavuuden edellytykset voisivat olla samat, koska vahingon ja haitan käsitteiden alat ovat kuitenkin osittain päällekkäisiä ja koska taloudellisilla ja immateriaalisilla arvoilla pitäisi olla yhtäläinen rikosoikeudellinen suoja varsinkin, kun kysymys on ihmis- ja perusoikeuksien, kuten yksityisyyden, suojaamisesta. Haitta ja taloudellinen vahinko ovat rinnasteisessa asemassa esim. RL 38:7a:n tunnusmerkistössä, mikä koskee tietojärjestelmän häirintää. Hyväksyttävänä ei voida pitää edes sosiaalisessa mediassa oikeudetonta "valeprofiilin" muodostamista toisen, todellisen henkilön henkilötiedoilla, koska sellaiseen menettelyyn ei ole mitään aitoa ja todellista tarvetta.

Tietoverkkorikollisuuteen liittyy se merkittävä ongelma, että teko voidaan valitettavasti (esim. automatisoinnilla eli tietokoneohjelman avulla) monissa tapauksissa toteuttaa lukuisissa eri paikoissa ympäri verkkoa tai kohdistaa suureen joukkoon henkilöitä, kuten kymmeniin, satoihin tai tuhansiin ihmisiin. Tällaisten tekojen osalta ei voitane oikein pitää riittävänä rangaistuksena pelkästään sakkoa. Internetissä aiheutuvien vahinkojen ja haittojen laajuus ja suuruus huomioon ottaen suositeltavaa olisi sisällyttää rangaistussäännökseen myös vankeusuhka (esim. vankeutta enintään 2 vuotta). Tämä rangaistustaso olisi luontevaa pelkästään ihmisten suojelemiseksi, mutta siihen on erityistä tarvetta, koska lakiehdotuksen mukaan "toinen" voisi olla myös oikeushenkilö, kuten useassa maassa toimiva yritys tai lukuisista yhtiöistä muodostuva kansainvälinen konserni.

Mietinnössä on lausuttu (sivu 61), ettei henkilötietojen käyttäminen koskisi valmisteluluonteista "henkilötietojen käsittelyä". Lausumaa ei ole perusteltu mietinnössä, joten sen hyväksyttävyys jää epäselväksi. Asiassa on kysymys henkilötietolain mukaisista henkilötiedoista. Tämän perusteella olisi johdonmukaista ja perusteltua, että "henkilötietojen käsittely" ymmärrettäisiin henkilötietolain 3 §:ssä säädetyllä tavalla, jotta vältyttäisiin tarpeettomilta tulkintaongelmilta ja liian suppealta tunnusmerkistöltä tietoverkkomaailmassa. Sanotun lausuman poistamista olisi suositeltavaa harkita.

3. Monipolvinen viittaustekniikka

Lain esitöillä on vanhastaan ollut merkittävä asema Pohjoismaisessa oikeuslähdeopissa. Lain esitöitä, erityisesti hallituksen lakiesitystä ja Eduskunnan valiokunnan mietintöä, hyödynnetään lain soveltamisessa niin tuomioistuimien, asianajajien, syyttäjien, poliisin ja muiden valvontaviranomaisten kuin opiskelijoiden ja muiden kansalaisten toimesta. Lain esitöiden loogisuudella ja helppolukuisuudella on merkittävä informaatioarvo lainsäätämistyön aikana kansanedustajille ja sen jälkeen lain soveltajille.

Työryhmän mietinnön 7 luvussa "Lakiehdotuksen perustelut" lausutaan monissa kohdissa, että yksityiskohtien osalta viitataan direktiivin "yksityiskohtaisissa perusteluissa" lausuttuun tai esitettyyn (ks. esim. sivut 52-58 ja 60). Ilmeisesti toiston välttämiseksi viitataan muualla aikaisemmin esitettyyn. Tämä viittaustekniikka aiheuttaa huomattavaa vaivaa lakiesityksen lukijalta, koska hänen täytyy lukea samanaikaisesti lakiehdotuksen perusteluita ja direktiiviä koskevia yksityiskohtaisia perusteluita sekä suorittaa vertailuja niiden välillä. Asianomaisten direktiivin yksityiskohtaisen perustelun löytyminen voi toisinaan olla työlästä, joten esim. maallikolle voi tapahtua erehdyksiäkin. Lakiehdotuksen perustelujen informaatioarvon ja hyödynnettävyyden parantamiseksi olisi suositeltavaa toistaa direktiiviä koskevissa yksityiskohtaisissa perusteluissa esitettyjä seikkoja lakiehdotuksen asianomaisissa kohdissa.

Työryhmän mietinnössä valittu viittaustekniikka muuttuu todella monipolviseksi, kun otetaan huomioon mietinnön 6 luvussa "Direktiivin sisältö ja sen suhde Suomen lainsäädäntöön" esitetyt uudet viittaukset. Monissa kohdissa (esim. sivulla 24, 28-30 ja 34) viitataan yksityiskohtien osalta yleissopimuksen määräysten täytäntöönpanoa koskevaan hallituksen lakiesitykseen HE 153/2006. Tilanne muodostuu lukijan kannalta erittäin haastavaksi, koska yksityiskohdat on lakiesityksessä HE 153/2006 hajautettu myös kahteen osaan eli direktiivien artikloiden ja lakiehdotuksen yhteyteen. Tässäkin lakiesityksessä on viittauksia lakiehdotuksen perusteluista direktiivin artikloja koskeviin yksityiskohtaisiin perusteluihin. Oikeiden yksityiskohtaisten perustelujen löy-

tyminen voi olla poikkeuksellisen työlästä, jolloin erehtymisen vaara lisääntyy viittausten monipolvisuudesta johtuen. Työryhmän laatiman lakiehdotuksen perustelujen informaatioarvon ja hyödynnettävyyden parantamiseksi olisi suositeltavaa toistaa lakiesityksessä HE 153/2006 esitetyt seikat tarpeellisilta osiltaan "Lakiehdotuksen perustelujen" (luvun 7) asianomaisissa kohdissa.

4. Eräitä yksityiskohtia

4.1. Viittaukset direktiiviin

Työryhmän mietinnössä ehdotetaan, että RL 38 luvun 13 §:n määritelmäsäännöksissä viitattaisiin direktiivin artikloihin. Viittaukset direktiivien artikloihin ovat erittäin epäinformatiivisia tavallisille kansalaisille ja jopa opiskelijoille, koska heillä voi olla ylivoimaisia vaikeuksia selvittää direktiivin sisältöä. Traditionaalisena tavoitteena voidaan pitää sitä, että rikossäännöksen keskeinen sisältö pitäisi vaikeuksitta ilmetä myös kansalaisille kotimaisen lain tunnusmerkistöstä. Informatiivisyyden lisäämiseksi olisi suositeltavaa poistaa viittaukset direktiivin artikloihin.

Rikossäännöksissä olevat viittaukset direktiiviin synnyttävät myös tarpeettomia tulkintaongelmia. Direktiivin mahdollisen muutoksen jälkeen voidaan kysyä, tuleeko direktiivin muutos voimaan rikossäännöksen osalta heti, kun direktiivin muutos on annettu, vai vasta, kun direktiivin muutos on saatettu voimaan Suomessa asianomaista rikossäännöstä koskevalla lainmuutoksella. Nämäkin seikat puoltavat direktiiviä koskevien viittausten poistamista rikossäännöksistä. Rikossäännös olisi suositeltavaa kirjoittaa siten, että säännöksen koko sisältö ilmenee tunnusmerkistöstä ja sitä täydentävistä määritelmäsäännöksistä.

4.2. Yleiset lainkonkurrenssiperiaatteet

Työryhmän mietinnössä mainitaan muutamissa kohdissa (esim. sivu 25, 27 ja 43) yleiset lainkonkurrenssia koskevat periaatteet. Mietinnössä ei ole kuitenkaan kattavasti selvitty, mitä ovat nämä yleiset periaatteet. Suositeltavaa olisi täydentää perusteluja siten, että yleiset lainkonkurrenssia koskevat periaatteet selostettaisiin kattavasti tarpeellisilta osin.

4.3. Avoin tekotapatunnusmerkistö

Työryhmän mietinnössä (sivu 28) on todettu, että RL 38 luvun 7a §:n tunnusmerkistöstä puuttuvat tietoverkkorikosdirektiivin 4 artiklassa mainitut tekotavat "tuhoamalla" ja "turmelemalla". Mietinnössä katsotaan, että RL 38:7a:n avoin tekotapaluettelo "taikka muulla niihin rinnastettavalla tavalla" kattaa direktiivin mukaiset tekotavat. Suositeltavaa olisi harkita avoimen tekotavan poistamista ja sen korvaamista direktiivin mukaisilla tekotavoilla. Rikosoikeudellisen legaliteettiperiaatteen vuoksi olisi toivottaa välttää tarpeettomia avoimia tunnusmerkistöjä.

4.4. Elintärkeä infrastruktuuri

Mietinnössä on käsitelty (sivu 42-43) direktiivin ilmaisua "elintärkeä infrastruktuuri", mitä ei ole määritelty direktiivissä. Mietinnössä haetaan johtoa tuhotyötä koskevasta RL 34 luvun 1 §:n 2 momentin säännöksestä.

RL 34:1.2:n mukaan tuhotyöstä tuomitaan myös se, joka 1) omaisuutta vahingoittamalla tai tuhoamalla taikka 2) a) tuotantojärjestelmän, b) jakelujärjestelmän tai c) tietojärjestelmän toimintaan oikeudettomasti puuttumalla aiheuttaa vakavan vaaran 1) energiahuollolle, 2) yleiselle terveydenhuollolle, 3) maanpuolustukselle, 4) oikeudenhoidolle tai 5) muulle näihin rinnastettavalle yhteiskunnan tärkeälle toiminnolle.

RL 34:1.2:n tunnusmerkistö edustaa 1990-luvun alkuvuosien tietoverkkokäsitystä, joka on nykyisin kovin vanhahtava. Työryhmän mietinnössä mainitaan eräänlaisena täydennyksenä julkisen hallinnon turvallisuusverkko viittaamalla hallituksen lakiesitykseen HE 54/2013. Sanottuun vanhanaikaiseen näkökulmaan perustuvat seikat ehdotetaan lisättäväksi uudeksi kvalifiointiperusteeksi tietojärjestelmän häirintää, tietoliikenteen häirintää ja datavahinkoa koskeviin tunnusmerkistöihin.

Mietinnössä jää tavallaan huomiotta yksityissektorin tärkeät järjestelmät, kuten tietoliikenneverkot (esm. Internet ja matkapuhelinverkot) ja valtakunnalliset pankkijärjestelmät. Esimerkiksi pankkijärjestelmien rikkoutuminen romahduttaisi rahatalouden.

Julkishallintoa koskevaa näkökulmaa voisi laajentaa tietoturvallisuuden näkökulmasta esim. seuraavilla valtakunnallisilla tietojärjestelmillä: Kelan tietojärjestelmät, verohallinnon valtakunnalliset tietojärjestelmät, ulosoton valtakunnalliset atk-järjestelmät ja poliisin valtakunnalliset tietojärjestelmät. Esimerkkinä voidaan mainita verohallinnon järjestelmät, joiden tuhoaminen lopettaisi verotuksen toimittamisen ja verojen maksuunpanemisen eli verotulojen kertymisen.

Ilmaisu “muu näihin rinnastettava yhteiskunnan tärkeä toiminto” siinä määrin avoin, että se jättää lainsoveltajalle kovin paljon harkintavaltaa.

Suositeltavaa olisi täydentää ja modernisoida uutta kvalifiointiperustetta koskevaa luetteloa ja välttää rikosoikeudellisen laillisuusperusteen nimissä liian avoimia tunnusmerkkejä.

Toivon, että edellä esitetyistä näkökohdista olisi apua lakiehdotuksen jatkovalmistelussa.

Vaasassa 31.8.2014

Asko Lehtonen
oikeustieteen professori (emeritus)
rikosoikeuden dosentti
oikeustieteen tohtori, varatuomari