EDUSKUNNAN APULAISOIKEUSASIAMIES

Helsinki 12.6.2014 Dnro 2035/5/14

OIKEUSMINISTERIÖ
lausunnot@om.fi

Viite: Lausuntopyyntönne 7.5.2014 hallituksen esitysluonnoksesta ja arviomuistiosta (OM 4/41/2013); "Tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan EU:n direktiivin (2013/40/EU) kansalliset täytäntöönpanotoimet"

LAUSUNTO

Oikeusministeriö on pyytänyt lausuntoani viitekohdassa tarkoitetusta työryhmän mietinnöstä.

Lausuntonani esitän kohteliaimmin seuraavaa.

Yleistä

Lainvalmistelussa tehtävänä on ollut ottaa huomioon identiteettivarkautta koskeva arviomuistio ja saatu lausuntopalaute siltä osin kuin se koskee oikeusministeriön toimialaan kuuluvaa rikoslainsäädäntöä. Hallituksen esitysluonnoksen sisältävä työryhmän mietintö valmistui 17.4.2014.

Olen antanut 28.4.2011 sisäasiainministeriön poliisiosastolle lausuntoni (Dnro 1339/5/11) ns. identiteettiohjelmasta (SM 092:00/2008). Oikeusministeriölle annoin 26.3.2013 oman lausuntoni (dnro 1241/5/13) oikeusministeriössä 15.3.2013 erityisesti ns. identiteettivarkauksista laaditusta muistiosta. Tässä lausunnossani arvioin oikeusministeriön tavoin, ettei ainakaan tuossa vaiheessa ollut edellytyksiä säätää erityistä identiteettivarkautta koskevaa yleissäännöstä. Identiteettivarkaussäännöksen mukanaan tuoma yleisestävyys ja "habeas data" voisivat puoltaa yleisen säännöksen säätämistä mutta tulkinnanvaraisuus ja sisällöllinen yleisluontoisuus olisivat tällaista sääntelyä vastaan. Omasta puolestani toivoin silti, että yhteisymmärrys linjauksista toisaalta sisäasiainministeriön ja toisaalta oikeusministeriön välillä olisi kohtuullisessa ajassa saavutettavissa.

Mietinnössään 27/2014 tietoverkkodirektiivin täytäntöönpanosta oikeusministeriön työryhmä ehdottaa nyt direktiivin vaatimusten täyt-

Osoite: 00102 Eduskunta
Puhelin: (09) 4321
Telefax: (09) 432 2268
Sähköposti: oikeusasiamies@eduskunta.fi
Internet: www.oikeusasiamies.fi

tämiseksi muun muassa, että säädettäisiin uusi identiteettivarkautta koskeva ja sakkoa seuraamukseksi sanktioiva kriminalisointi. Muutokset koskisivat erityisesti vaaran aiheuttamista tietojenkäsittelylle ("nykyajan politiarikos"), vahingontekoa, viestintäsalaisuuden loukkausta, tietojärjestelmän häirintää ja tietomurtoa.

Esitysluonnos sisältää osin uutta, meillä rikosoikeudessa ja yleisemminkin ICT-oikeudessa vielä vakiintumatonta terminologiaa. Uusi sääntely on kuitenkin ICT-alan arvopohjan kannalta tärkeää (vrt. Petteri Järvinen: NSA - Näin meitä seurataan 2014). Direktiivillä puututaan uusiin uhkakuviin kuten laajamittaisiin tietoverkkohyökkäyksiin ns. bottiverkkoja ja kaapattuja tietokoneita käyttämällä sekä tietoverkkorikoksen yhteydessä tapahtuvaan henkilöllisyyden väärinkäyttöön.

Rikosoikeudelliselta kannalta tullee kyberturvallisuuden näkökulma vaikuttamaan puheena olevan uudistustyön ohella rikosoikeuden sisältöön. Suomen puolustusvoimat ja poliisikin haluaisi laajat signaalitiedusteluoikeudet.

Tässä tilanteessa tietorikosten suojeluobjektien määrittely saattaa olla haasteellista.

Vaaran aiheuttaminen tietojenkäsittelylle

Direktiivin 2013/40/EU edellyttämät keskeisimmät muutokset liittyvät tunnusmerkistöjen enimmäisrangaistustasojen korottamiseen ja eräiden kvalifiointiperusteiden sisällyttämiseen kansalliseen lainsäädäntöön. Vaikka Suomen lainsäädäntö vastanneekin jo nykyisin pitkälti direktiivin vaatimuksia, on esitysluonnoksessa edellytetty joitakin uusia rikoksen tekotapojenkin lisäyksiä.

Eräs näistä uusista tekotavoista olisi rikoslain 34 luvun 9 a §:n säännös vaaran aiheuttamisesta tietojenkäsittelylle siten, että tekijä hankkii tietoverkkorikosvälineen käyttöönsä. Vaikka muutos tältä osin on osin tekninen, sisältyy ehdotettuun sääntelyyn nähdäkseni tulkinnanvaraisuuksia. Rikoksentekoon soveltuvan välineen yksilöinti voi olla käytännössä pulmallista. Tietoverkkoympäristössä (kuten Tor-verkko) on tunnetusti helpostikin saatavissa "hakkerointivälineitä" ja ohjelmia (mm. SQL-injektio ja Key logger), joten tekijän subjektiivinen puoli ja osaamistasokin vaikuttavat asiaan. Voidaan myös kysyä, mikä kussakin tilanteessa on tavanomaisesta poikkeavaa, "rikollista" tai "ilmeisen vilpillistä" (esitys s. 58). Tietoverkkoasioinnin kaupallinen seuranta evästein, kanta-asiakaskortein ja sähköisin tunnistein on joka tapauksessa arkipäiväistä.

Vahingonteko tietojenkäsittelyssä

Ns. datavahinkojen tekotapoja on määrä täsmentää "normaaliin vahingontekoon" verrattuna. Datavahingonteko ja törkeä datavahingon-

teko muuttuisivat omiksi rikosnimikkeikseen aiemman perusmuotoisen vahingonteon sijaan. Törkeä datavahingonteko sisältäisi kvalifiointiperusteet, joiden osalta direktiivi edellyttää datavahingonteon enimmäisrangaistuksen vähimmäistasoksi vähintään kolmen ja viiden vuoden vankeutta.

Tässäkin kohtaa korostuvat nähdäkseni yhteiskunnan yleinen turvallisuus sekä näyttö- että tutkintamahdollisuuksien merkitys. Työryhmän ehdotuksen mukaan "kriminalisointi on rajattu tilanteisiin joissa on aiheutunut taloudellista vahinkoa taikka muuta vähäistä suurempaa haittaa". Muotoilu jättää sijaa tulkinnalle. Esimerkiksi nettikiusaaminen valeprofiileja käyttäen ei yleensä aiheuta suoranaista taloudellista vahinkoa. Mikäli kiusaaminen ei ylitä "vähäistä suuremman haitan" rajaa – mikä se sitten onkaan – valeprofiilien tekeminen jäisi sallituksi. Esityksen vaikutusten arviointia olisi syventänyt, mikäli valmistelussa olisi perehdytty esityksestä ilmenevää enemmän myös oikeuskirjallisuuteen (ks. mm. Anu Jounio: Tieto- ja viestintärikokset rikoslain 38 luvussa. Maisteritutkielma Rovaniemi syksy 2011).

Tieto- ja viestintäsalaisuuden loukkauksista

Esityksen mukaan viestintäsalaisuuden loukkausta koskevan säännöksen soveltamisala on jo ennestään laaja (vrt. HE 94/1993 vp ja HE 153/2006 vp). Datan muodossa olevan viestin pitää kuitenkin olla ulkopuolisilta suljettu tai televerkossa välitettävänä. Jo aikanaan vuonna 1995, kun tietomurto (vrt. Ruotsin dataintrång) ns. tietorikostyöryhmän työn pohjalta säädettiin rangaistavaksi, oli edellytyksenä, että rikoksentekijän tulee läpäistä oikeudettomasti jonkinlainen tietojärjestelmän tekninen/ohjelmallinen pääsykontrolli (vrt. KKO:2003:36 ja 2003:58 sekä Defensor Legis 4/2003).

Ehdotettujen muutosten taustalla on Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö, jonka perusteella voimassa olevan lainsäädäntömme mukaan toimittaessa ei ole aina löydetty oikeudenmukaista tasapainoa vaikkapa sananvapauden ja erityisesti yksityiselämän suojan välillä. Perusoikeuksien valvonnassa ja siis oikeusasiamiehen laillisuusvalvonnassa muun ohella sananvapauden ja yksityiselämän suojan välinen punninta on tullut usein esille tutkittaessa viranomaisten menettelyä kiellettäessä kuvaamista erilaisissa tilanteissa.

Perusoikeuksien välisen oikeudenmukaisen tasapainon löytäminen on viime kädessä riippuvainen arvostuksista. Ehdotettuja rikoslain muutoksia tulisi nähdäkseni viestintäsalaisuudenkin osalta arvioida vielä Euroopan ihmisoikeussopimuksen määräyksiä ja ihmisoikeustuomioistuimen oikeuskäytäntöä kunnioittaen. Viittaan erityisesti tapauksiin K.U. v. Finland, nro 2872/02, EIT 2.12.2008 (Kysymys yksityiselämän suojan loukkauksesta, kun internetiin alaikäisen nimellä hänen tietämättään seksuaalisluonteisen seuranhakuilmoituksen laittanutta henkilöä ei voitu lainsäädännön puutteista johtuen

selvittää eikä saattaa syytteeseen) ja I. v. Finland, nro 40412/98, EIT 17.7.2008 (Kysymys potilaan yksityisyyden suojan loukkauksesta, kun ei ollut järjestetty riittäviä takeita sen varmistamiseksi, että potilasrekisteriin pääsi vain potilasta hoitanut henkilöstö).

Euroopan unionin tuomioistuimen käytännöstä tähdennän, että jäsenvaltioiden viranomaisten ja tuomioistuinten on lisäksi pannessaan täytäntöön mainittujen direktiivien noudattamisen edellyttämiä toimenpiteitä tulkittava kansallista oikeuttaan näiden samojen direktiivien mukaisesti. Tämän lisäksi ne eivät myöskään saa nojautua sellaiseen kyseisten direktiivien tulkintaan, joka johtaisi ristiriitaan perusoikeuksien kanssa tai muiden yhteisön oikeuden yleisten periaatteiden, kuten suhteellisuusperiaatteen, kanssa (tästä LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH, C 557/07, EYT 19.2.2009). Euroopan Unionin tuomioistuin on 8.4.2014 julistanut pätemättömäksi Euroopan yhteisöjen vuoden 2006 direktiivin, joka määrittelee oikeuden kerätä ja säilyttää kansalaisten viestintätietoja rikollisuuden, muun muassa terrorismin torjuntaa varten (Tuomiot C-293/12 ja C-594/12). Tuomioistuimen mielestä lain tulisi rajoittaa enemmän sitä, millaisia tietoja voidaan kerätä ja samoin viranomaisten pääsyä tietoihin (vrt. Hallintovaliokunnan lausunto 9/2014 vp).

IdentiteettivarkaussäänteIystä

Rikoslain 38 lukuun ehdotetaan direktiivin velvoitteiden täyttämiseksi uutta identiteettivarkautta koskevaa 9 b pykälää, josta lienee nyt siis saavutettu yhteisymmärrys toisaalta oikeusministeriön ja toisaalta sisäasiainministeriön välillä. Ehdotuksen mukaan identiteettivarkaudesta tuomittaisiin se, joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa. Lisäksi teon on tullut aiheuttaa taloudellista vahinkoa tai "muuta vähäistä suurempaa haittaa" sille, jota tieto koskee (vrt. Mika Viljanen: Ihmisen identiteetti ja tuottamusarviointi, LM 3/2005 s. 426–451). Haittaa saattaisi joissakin tapauksissa syntyä myös silloin, kun internetin sosiaaliseen mediaan on luotu valeprofiili toisen henkilötiedoilla (vrt. virtuaalipersoonan kaappaaminen pelipalvelussa). Joissakin tapauksissa tällaisen väärän profiilin poistaminen saattaa olla kansainvälisessä tietoverkossa ja palvelimilta vaikeaa. Lisäksi tilanne saattaa edellyttää yhteydenottoja lukuisiin henkilöihin, jotka ovat kuvitelleet kommunikoivansa sen henkilön kanssa, jota väärä identiteettitieto koskee.

Asiattoman häirinnän muodot tietoverkossa voivat olla henkilöön menevää loanheittoa, seksuaalissävytteistä ehdottelua etenkin nuorille, keskustelua häiritseviä tarkoituksellisen provosoivia kommentteja eli trollaamista tai roskapostia. Kokemukset Suomesta osoittavat, että ns. lapsipornon vastainen toiminta ja poliisin listausten tekeminen verkkopalveluista voi olla käytännössä vaikeata.

RL 38:9 b §:n säännös merkitsisi uutta kriminalisointia, josta saattaa aiheutua esityksessäkin (s. 19) mainittuja lisäkuluja ja tietenkin poliisin ja syyttäjien lisäkoulutustarvetta. Identiteetti varkaus olisi asianomistajarikos eli virallinen syyttäjä nostaisi syytteen identiteettivarkaudesta vain, jos asianomistaja ilmoittaa rikoksen syytteeseen pantavaksi.

Syyteoikeuden sääntelystä

Ehdotetun sääntelyn myötä rikoslain muutoksilla olisi vaikutuksia joihinkin pakkokeinolaissa (806/2011) tarkoitettuihin toimivaltuuksiin. Mikäli eräitä enimmäisrangaistuksia, varsinkin tietomurto ja viestintäsalaisuuden loukkaus, nostettaisiin, tulisivat jotkin pakkokeinoista käyttöön ilman pakkokeinolain muutoksia. Pakkokeinolain 10 luvun 56 §:ssä tarkoitetun ylimääräisen tiedon käytön osalta olisi jatkossakin mahdollista käyttää ylimääräistä tietoa myös törkeän tietomurron tutkintaan, sillä esityksen mukaan enimmäisrangaistus olisi jatkossa kolme vuotta vankeutta (vrt. esitys s.40). Esityksen viittaus pakkokeinolakiin (HE 226/2010 ja 806/2011) olisi kaivannut ohelleen myös ajankohtaisen viittauksen ns. esitutkintapakettiin ja arvioinnin sen vaikutuksista tietoverkkoympäristössä.

Silti on tässä yhteydessä aiheellista kiinnittää perusoikeusnäkökulmasta lainvalmistelijoiden huomiota siihen, että identiteettivarkaudesta on syntynyt jo nykyisenkin sääntelyn puitteissa oikeuskäytäntöä. Yleisemminkin pidän kyseisen esityksen puutteena sitä, että muun ohella identiteettivarkautta koskevaa oikeuskäytäntöä on siteerattu ja arvioitu varsin rajoitetusti (vrt. http://www.secmeter.com/esitutkinta.html). Lainvalmistelussa määritelmäsäännökset voidaan koota lain alkuun omaksi pykäläkseen ja tässä yhteydessä siihen on tarvetta.

Muuta

Ehdotettu sääntely on vain osa järjestäytyneen tietoyhteiskunnan yllä pitämiseksi tarkoitettua perusrakennetta, joka edellyttää perustakseen toimivaa tietoteknistä infrastruktuuria. Viime aikoina on säädetty ja ollaan säätämässä muutakin tähän aihekokonaisuuteen kuuluvaa lainsäädäntöä, kuten tietoyhteiskuntakaari velvoitteineen (HE 221/2013 vp) sekä ns. TUVE-laki. Viestintäpalvelujen häiriöttömyyttä edistetään luomalla häiriön hallinnassa tarvittavalle yritysten ja viranomaisten yhteistyölle entistä parempia edellytyksiä. Keskeisimmät verkonvalvomot ja muut kriittiset järjestelmät olisi jatkossa ylläpidettävä siten, että ne voidaan poikkeusoloissa viipymättä palauttaa Suomeen. Tietoyhteiskuntakaaren vaatimusten mukaisuuden ohjausta ja valvontaa koskevat säännökset ulottunevat vuodesta 2015 lukien sekä yleisiin viestintäverkkoihin että viranomaisverkkoihin.

Rikoslainkin säännökset voivat ratkaista tahollaan vain osan tietoturvallisen toiminta- ja asiointiympäristön ongelmista. Nyt esityksestä syntyy jotenkin teknisen täytäntöönpanouudistuksen kuva.

Pidän perusteltuna, että lakiehdotuksista hankittaisiin aikanaan eduskunnan perustuslakivaliokunnan lausunto.

Apulaisoikeusasiamies Jussi Pajuoja

Esittelijäneuvos Jorma Kuopus