Tietomurto ja Suomen rikosoikeudellinen lainsäädäntö

Lapin yliopisto
Oikeustieteiden tiedekunta
Maisteritutkielma
Matti Mämmi
Rikosoikeus
Syksy 2022

Lapin yliopisto
Tiedekunta: Oikeustieteiden tiedekunta
Työn nimi: Tietomurto ja Suomen rikosoikeudellinen lainsäädäntö
Tekijä: Matti Mämmi
Koulutusohjelma/oppiaine: Oikeustiede, rikosoikeus
Työn laji: Maisteritutkielma _X_ Lisensiaatin työ _
Sivumäärä: XII + 75
Vuosi: 2022

Tiivistelmä:
Maisteritutkielmani on rikosoikeudellinen tutkielma, jossa tutkin Suomen rikoslainsäädännön tieto- ja viestintärikoksiin kuuluvaa tietomurtoa. Vastaan tutkielmassani kysymykseen siitä, mitä erityisominaisuuksia tietomurtorikoksilla on, miten rikosoikeuden yleiset opit tulee ottaa huomioon käsiteltäessä tietomurtorikoksia sekä mitä tulee ottaa huomioon, jos rikos täyttää tietomurron tunnusmerkistön lisäksi toisenkin rikoksen tunnusmerkistön. Lisäksi tarkastelen tietomurtorikoksen tutkintaan ja oikeuskäsittelyyn liittyviä erityishaasteita.

Tutkimuksen keskeisenä aiheena on rikoslain (39/1889) 38 luvun tieto- ja viestintärikosten 8 ja 8a §:ien mukainen tietomurto ja törkeä tietomurto. Perehdyn tutkielmassani tietomurtoihin rikosoikeuden vastuuopin, lainkonkurrenssin ja rikosprosessuaalisen seuraamusjärjestelmän kannalta. Käsittelen tietomurtoa lisäksi poikkitieteellisesti tietoteknisestä näkökulmasta keskeisten käsitteiden määrittelemisen kannalta.

Tietomurtorikosten digitaalinen tekoympäristö asettaa korostuneita vaatimuksia tietomurtojen tutkinnalle ja tuomitsemiselle. Rikosoikeuden yleiset opit ja lainkonkurrenssisäännöt on laadittu fyysisen ympäristön kontekstiin, mikä asettaa haasteita sovellettaessa niitä digitaalisessa ympäristössä tapahtuviin tietomurtorikoksiin. Lainkonkurrenssitilanteissa kohteena oleva tietomurtotapaus tulee ratkaista abstraktien sääntöjen lisäksi tapauskohtaiset erityisolosuhteet huomioiden.

Avainsanat: rikosoikeus, tietomurto, kyberrikollisuus, lainkonkurrenssi, esitutkinta

Sisällys

LÄHTEET

Kirjallisuus

Aarnio, Aulis: Luentoja lainopillisen tutkimuksen teoriasta. Helsinki 2011.

Clough, Jonathan: ”A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation”. Monash University law review. Monash University. Faculty of Law 40(3):698.

Forss, Marko – Keinänen, Anssi: Rikoslakia koskeva lainvalmistelu – miten internet ja erityisesti sosiaalinen media huomioitiin vuosina 2009–2016 annetuissa hallituksen esityksissä. Edilex 2017.

Fredman, Markku – Kanerva, Janne – Tolvanen, Matti – Viitanen, Marko: Esitutkinta ja pakkokeinot. Alma Talent 2020. 6. uudistettu painos.

Frände, Dan: Yleinen rikosoikeus. Edita 2012.

Frände, Dan – Matikkala, Jussi – Tapani, Jussi – Tolvanen, Matti – Viljanen, Pekka – Wahlberg, Markus: Keskeiset rikokset. Edita 2018.

Hahto, Vilja: Uhrin myötävaikutus ja rikoksentekijän vastuu: rikos- ja vahingonkorvausoikeudellinen tutkimus tekoa edeltävästä uhrikäyttäytymisestä fyysistä koskemattomuutta loukkaavissa rikoksissa. Edita 2004.

Helenius, Dan – Linna, Tuula: Siviili- ja rikosprosessioikeus. Alma Talent 2021.

Helminen, Klaus – Fredman, Markku – Kanerva, Janne – Tolvanen, Matti – Viitanen, Marko: Esitutkinta ja pakkokeinot. Helsinki 2014.

Husa, Jaakko: Tuomioistuinratkaisut oikeuslähteenä – oikeuslähdeoppi ja oikeusyhteisön kulttuurinen identiteetti. Lakimies 7–8/2020. s. 972–992.

Hyttinen, Tatu: Olosuhdetahallisuuden vakioitu alaraja – oikeusturvaa vai korkeimman oikeuden retoriikkaa? Defensor Legis N:o 6/2016. s. 916–933. Referee-artikkeli.

Häyhä, Juha. Johdanto, s. 15–34, teoksessa *Häyhä, Juha* (toim.): Minun metodini. Werner Söderström Lakitieto OY 1997.

Innanen, Antti – Saarimäki, Jarkko: Internetoikeus. Edita 2012. 2. uudistettu painos.

Kalkela, Eeva-Maija – Kotiranta, Kai: Todennäköisesti ja väliinpitämättömästi – seurausta-hallisuuden määrittelyä suomalaisen ja ruotsalaisen oikeuskäytännön valossa, s. 229–302, teoksessa *Kaisto, Janne* (toim.): Oikeustiede = Jurisprudentia: Suomalaisen Lakimiesyhdistyksen vuosikirja LIV 2021. Helsinki 2021.

Kallio, Heikki: Toissijaisuuslausekkeet rikoslaissa. Defensor Legis N:o 1/2018. s. 19–36, Referee-artikkeli.

Kemppinen, Heikki – Tapani, Jussi: Rangaistuksen määrääminen ja ennakkopäätöksiä koskeva tulkintaoppi. Lakimies 7–8/2020. s. 1035–1059.

Kemppinen, Heikki: Rangaistuksen määräämisen perusteleminen. Helsinki 2021.

Kimpimäki, Minna: Kansainvälinen rikosoikeus. Kauppakamari 2015.

Kimpimäki, Minna: Vastavuoroinen tunnustaminen rikosoikeudellisen yhteistyön muotona – tehokasta yhteistyötä vai sokeaa luottamusta? s. 140–155, teoksessa *Riekkinen, Juhana* (toim.): Oikeutta oikeudenkäynnistä täytäntöönpanoon: Juhlajulkaisu Tuula Linna 1957 – 25/9 – 2017. Alma Talent 2017.

Lappi-Seppälä, Tapio: Rikosten seuraamukset. Werner Söderström Lakitieto OY 2000.

Lappi-Seppälä, Tapio: Rikollisuus ja kriminaalipolitiikka. Helsinki 2006.

Lappi-Seppälä, Tapio – Hakamies, Kaarlo – Helenius, Dan – Melander, Sakari – Nuotio, Kimmo – Ojala, Timo – Rautio, Ilkka – Koskinen, Pekka – Majanen, Martti – Nuutila, Ari-Matti: Rikosoikeus. Alma Talent 2022.

Lappi-Seppälä, Timo. Rikosoikeustutkimus, kriminaalipoliittinen orientaatio – ja metodi, s. 189–218, teoksessa *Häyhä, Juha* (toim.): Minun metodini. Werner Söderström Lakitieto OY 1997.

Li, Xingan: Cybercrime and deterrence: networking legal systems in the networked information society. Turun yliopisto 2008.

Limnéll, Jarno – Majewski, Klaus – Salminen, Mirva: Kyberturvallisuus. Docendo 2014.

Linna, Tuula: Oikeudenmukaisen rankaisemisen ideaali ja reaali: tunnustaminen rangaistuksen lieventämisperusteena, s. 275–297, teoksessa *Sakari Melander* (toim.), Juhlajulkaisu Kimmo Nuotio 1959 – 18/4 – 2019. Helsingin yliopisto 2019.

Luoto, Lauri: Avunannon rangaistavuuden edellytykset. Helsinki 2018.

Luoto, Lauri: Lainkonkurrenssin ratkaisukriteerit KKO:n tuoreen oikeuskäytännön ja oikeustieteen valossa. Defensor Legis N:o 2/2022. s. 403–418, Referee-artikkeli.

Matikkala, Jussi: Rikoslain kokonaisuudistuksesta, s. 89–99, teoksessa *Lahti, Raimo* (toim.): Rikosoikeuden muutos 1960-luvulta 2010-luvulle: Pekka Koskisen (1943–2011) muistojulkaisu. Helsinki 2013.

Melander, Sakari: Rikosoikeuden peruskysymyksiä. Helsinki 2015.

Melander, Sakari: EU-rikosoikeus. Talentum 2015.

Metsäranta, Tuomas: Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja. Turku 2015.

Nuotio, Kimmo: Todennäköisyystahallisuuden tilasta ja tarinasta. Lakimies 7–8/2017 s. 970–991.

Nuutila, Ari-Matti: Rikosoikeuden ABC-kirja. Turku 1995.

Nuutila, Ari-Matti: Rikoslain yleinen osa. Helsinki: Lakimiesliiton kustannus 1997.

Oerlemans, Jan-Jaap: Investigating Cybercrime. Leiden: Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University 2017.

Oksanen, Ville – Välimäki, Mikko: Tietokonelaitteiston ja sen sisältämän tiedon takavarikosta rikosasioissa. Defensor Legis N:o 2/2008, s. 219–227, Asiantuntija-artikkeli.

Piippo, Jenna: Rikossäännösten oikeushyväulottuvuus lainkonkurrenssiarvioinnissa korkeimman oikeuden ratkaisukäytännön valossa. Lakimies 3–4/2022 s. 645–668, Referee-artikkeli.

Rautio, Jaakko: Uudet menettämisseuraamuksiin liittyvät menettelysäännökset, s. 269–279, teoksessa *Riekkinen, Juhana* (toim.): Oikeutta oikeudenkäynnistä täytäntöönpanoon: Juhlajulkaisu Tuula Linna 1957 – 25/9 – 2017. Alma Talent 2017.

Riekkinen, Juhana: Verkkopetoksista ja todisteluista. Lakimies 1/2018 s. 75–102, Referee-artikkeli.

Riekkinen, Juhana: Sähköiset todisteet rikosprosessissa: tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaariin. Alma Talent 2019.

Riekkinen, Juhana: Postihuumetapaukset ja selitystaakka erityisesti Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa. Defensor Legis N:o 6/2020 s. 997–1012, Referee-artikkeli.

Tapani, Jussi – Tolvanen, Matti – Hyttinen, Tatu: Rikosoikeuden yleinen osa: vastuuoppi. Alma Talent 2019.

Saarenpää, Ahti: Kadonneet systeemit, s. 261–279, teoksessa *Häyhä, Juha* (toim.): Minun metodini. Werner Söderström Lakitieto OY 1997.

Sieber, Ulrich: The international handbook on computer crime: computer related economic crime and the infringements of privacy. Chichester 1986.

Shipley, Todd: Investigating internet crimes: an introduction to solving crimes in cyberspace. Syngress 2014.

Sutela, Mika: Rangaistusten jakautuminen rangaistusasteikkojen rajoissa oikeuskäytännössä. Defensor Legis N:o 2/2020 s. 215–229.

Viljanen, Pekka: Konfiskaatio rikosoikeudellisena seuraamuksena. Edita 2007.

Wylie, Phillip L. – Crawley, Kim: The Pentester BluePrint: Starting a Career as an Ethical Hacker. Wiley 2021.

Internet-lähteet

Euroopan neuvosto: ”Vahvempi kyberturvallisuus ja häiriönsietokyky koko EU:hun – neuvoston ja Euroopan parlamentin alustava yhteisymmärrys” https://www.consilium.europa.eu/fi/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/ (käyty 16.9.2022)

Fortinet: ”What is a Brute Force Attack?” https://www.fortinet.com/resources/cyberglossary/brute-force-attack (käyty 20.3.2022)

Fortinet: ”Types of Cyber Attacks” https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks (käyty 21.3.2022)

Helsingin Sanomat: ”Muistot: Antti Pihlajamäki” https://www.hs.fi/muistot/art-2000002627016.html (käyty 11.9.2022)

Kyberturvallisuuskeskus: ”Bug Bounty -ohjelmien avulla tietoturvaongelmat voi kääntää PR-voitoiksi” https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/bug-bounty-ohjelmien-avulla-tietoturvaongelmat-voi-kaantaa-pr-voitoiksi (käyty 9.10.2022)

OWASP Foundation: ”SQL Injection” https://owasp.org/www-community/attacks/SQL_Injection (käyty 11.9.2022)

OWASP Foundation: ”Top 10 2017” https://wiki.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf (käyty 11.9.2022)

StatFin: ”Tilastokeskuksen maksuttomat tilastotietokannat” https://statfin.stat.fi/PxWeb/pxweb/fi/StatFin/ (käyty 17.9.2022)

Yleisradio: ”Vastaamon tietomurtotapaus” https://yle.fi/uutiset/3-11610267 (käyty 16.9.2022)

Virallisaineisto

Hallituksen esitykset ja valiokunta-aineisto

HE 94/1993 vp Hallituksen esitys eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi.

HE 309/1993 vp Hallituksen esitys eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

HE 80/2000 vp Hallituksen esitys eduskunnalle menettämisseuraamuksia koskevan lainsäädännön uudistamiseksi.

HE 44/2002 vp Hallituksen esitys eduskunnalle rikosoikeuden yleisiä oppeja koskevan lainsäädännön uudistamiseksi.

HE 153/2006 vp Hallituksen esitys eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain, pakkokeinolain 4 luvun, esitutkintalain

27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 ja 23 §:n muuttamisesta.

HE 222/2010 vp Hallituksen esitys eduskunnalle esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi.

HE 232/2014 vp Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

LaVM 22/1994 vp Lakivaliokunnan mietintö rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien uudistukseksi.

PeVL 66/2010 vp Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi.

PeVL 32/2013 vp Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle laeiksi esitutkintalain ja pakkokeinolain muuttamisesta sekä eräiksi niihin liittyviksi laeiksi.

Muu virallisaineisto

Organization for Economic Co-operation and Development: Computer-related crime: analysis of legal policy. Paris: OECD, 1986.

European Committee on Crime Problems. Computer-related crime: Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems. Strasbourg: Council of Europe, Legal Affairs 1990.

VAHTI 8/2008. Valtionhallinnon tietoturvasanasto. Valtionhallinnon tietoturvallisuuden johtoryhmän ohje. Valtiovarainministeriön julkaisuja. Helsinki 2008. https://www.suomi-digi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-82008-valtionhallinnon-tietoturvasanasto

Turvallisuuskomitea. Suomen kyberturvallisuusstrategia. Helsinki 2013. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/

Sisäministeriö 14/2017. Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Helsinki 2017. https://julkaisut.valtioneuvosto.fi/handle/10024/79866

Turvallisuuskomitea. Suomen kyberturvallisuusstrategia 2019. Helsinki 2019. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Euroopan komissio. The EU's Cybersecurity Strategy in the Digital Decade. Bryssel 2020. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade

Oikeustapaukset

Korkein oikeus

KKO 1974 -II-82

KKO 2002:112

KKO 2003:36

KKO 2017:95

KKO 2021:64

KKO 2022:23

Hovioikeudet

Helsingin hovioikeus 16.7.2021 tuomio 21/130856 asiassa R 20/523

Helsingin hovioikeus 24.08.2018 tuomio 18/134245 asiassa R 17/1769

Käräjäoikeudet

Helsingin käräjäoikeus 23.05.2018 tuomio 18/122097 asiassa R 18/4485

Pohjanmaan käräjäoikeus 17.12.2018 tuomio 18/156295 asiassa R 18/1062

Helsingin käräjäoikeus 26.07.2019 tuomio 19/132211 asiassa R 19/5139

Keski-Suomen käräjäoikeus 15.09.2020 tuomio 20/133023 asiassa R 20/118

LYHENTEET

HE	Hallituksen esitys
KKO	Korkein oikeus
LaVM	Lakivaliokunnan mietintö
OECD	Organisation for Economic Co-operation and Development
PeVL	Perustuslakivaliokunnan lausunto
SEU	Sopimus Euroopan unionin toiminnasta
SQL	Structured Query Language, tietokantojen ohjelmointikieli
VPN	Virtual Private Network, verkkoliikenteen salaustekniikka

1 JOHDANTO

1.1 Aiheen esittely

Viimeisten vuosikymmenten aikana tapahtunut teknologinen kehitys on mahdollistanut monessa yhteydessä tietojenkäsittelyn siirtämisen ajasta ja paikasta riippumattomaksi digitaaliseen verkkoon. Teknologisen kehityksen seurauksena myös arkaluonteista ja taloudellisesti arvokasta tietoa on siirtynyt sähköisen tiedonkäsittelyn piiriin. Digitalisoituminen ei ole kuitenkaan vaikuttanut tiedonkäsittelyn yleisiin uhkakuviin ja sen suojeltaviin oikeushyviin. Tiedon eheys, arkaluonteisten tietojen käytön rajaaminen ja suoja ulkopuoliselta tunkeutumiselta ovat myös tärkeitä aiheita siirryttäessä digitaaliseen ympäristöön. Tietoverkkorikosten tarkastelun kannalta painopisteenä on teknologian tarkastelu tekovälineenä, kohteena tai ympäristönä.[1] 1990-luvun alussa tietotekniikkaan liitännäiset rikokset olivat selitettävissä ja tutkittavissa nykyään perinteiseksi määriteltävinä rikoksina, kuten petosrikoksina tai vahingontekona. Tietokone katsottiin rikoksentekovälineeksi, kuten tiirikka tai ase.[2]

Nykyisin tietoverkkorikokset on mahdollista jakaa tietoverkkoympäristöön kohdistuviin rikoksiin ja tietoverkkoympäristöä hyväksi käyttäen tehtyihin rikoksiin. Tietoverkkoympäristöön kohdistuva rikos voi esiintyä ainoastaan tietoverkoissa tai tietojärjestelmässä, joten tietomurto on tietoverkkoympäristöön kohdistuva rikos. Tietoverkkoympäristöä hyväksi käyttäen tehty rikos käsittää laajemman joukon mahdollisia rikoksia. Kyse on perinteisemmistä rikoksista, kuten petoksista, joissa rikos tapahtuu digitaalisessa ympäristössä.[3]

Tietoverkkorikosten esiintyvyyden voidaan odottaa kasvavan lähivuosina, joten ilmiötä on merkityksellistä myös tutkia enenevissä määrin. Euroopan komissio arvioi COVID-19-pandemian seurauksena 40 % Euroopan unionin alueella olevista työntekijöistä siirtyneen keväällä 2020 etätöihin.[4] Etätöihin siirtymisen seurauksena tärkeämpää ja arkaluontoisempaa tietoa on käsitelty verkon välityksellä, mikä voi tehdä tietomurroista ja muista tieto- ja viestintärikoksista aikaisempaa houkuttelevampia rikoskohteita. Arvion mukaan myös yksi kahdeksasta unionin

[1] SM 14/2017, s. 10.
[2] Li, 2008, s. 112.
[3] SM 14/2017, s. 10.
[4] European Comission: The EU's Cybersecurity Strategy in the Digital Decade.

alueella olevasta yrityksestä on joutunut kyberhyökkäyksen kohteeksi.[5] Tietomurto kuuluu kyberhyökkäyksiin.

Kyberrikoksia on tutkittu toistaiseksi vähän rikosoikeudellisesta näkökulmasta. Väitetysti ensimmäinen suomalainen tutkimus aihepiiristä oli oikeustieteen tohtori *Antti Pihlajamäen* väitöskirja ”Tietojenkäsittelyrauhan rikosoikeudellinen suoja" vuodelta 2004.[6] Lähivuosina oikeudellisissa aikakausijulkaisuissa on esiintynyt artikkeleita, jotka käsittelevät yleisesti tieto- ja viestintärikoksia.[7]

Kyberrikollisuuden määritteleminen tulee aloittaa kyberkäsitteen määrittelystä. Sana ”kyber” tarkoittaa nykymerkityksessään digitaalista maailmaa.[8] Käsitettä käytetään harvoin kuitenkaan sellaisenaan, vaan se on etuliitteenä puhuttaessa digitaaliseen maailmaan liittyvistä käsitteistä, kuten kyberrikollisuudesta, -turvallisuudesta tai -ympäristöstä. Osana yhteiskunnan turvallisuusstrategiaa ensimmäisen kerran vuonna 2013 laadittu Suomen kyberturvallisuusstrategia määrittelee kyberturvallisuuden tavoitetilaksi, jossa kybertoimintaympäristö on luotettava ja sen toiminta on turvattu.[9] Vuonna 2019 kyberturvallisuusstrategiasta julkaistiin päivitetty versio, joka määrittelee kansalliset tavoitteet strategisina linjauksina kybertoimintaympäristön kehittämiseksi.[10]

Käsitellessä kyberrikoksiin liittyviä ilmiöitä tulee lisäksi huomioida, että kyberturvallisuudessa on puhuttu yleisesti digitaalisen ympäristön muutoksesta ”Web 1.0” -käsitteestä ”Web 2.0” -käsitteeseen.[11] Web 1.0 -käsite sisälsi internetin ensimmäiset palvelut ja laajemman käytettävyyden 1990-luvulla. Web 2.0 sisältää erilaiset 2000-luvulla lanseeratut sosiaalisen median palvelut, kuten Facebookin, Instagramin ja YouTuben. Internetin palveluiden muutos on edellyttänyt myös lainsäätäjiltä reagointia tieto- ja viestintärikosten tapahtumiseen uudenlaisissa palveluissa, kuin mitä lain valmistelun aikana on ajateltu.

[5] European Comission: The EU’s Cybersecurity Strategy in the Digital Decade.
[6] Helsingin Sanomat: ”Muistot: Antti Pihlajamäki”.
[7] *Nevalainen, Sami*: ”Kyberrikokset ja Suomen rikosoikeus” Defensor Legis N:o 2/2019 sekä *Paasonen, Jyri – Aaltonen, Mikko – Luomala, Mikko*: ”Kyberrikokset tuomioistuimissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset”. Defensor Legis N:o 4/2021.
[8] Limnéll, ym., 2014, s. 29.
[9] Suomen kyberturvallisuusstrategia 2013, s. 13.
[10] Suomen kyberturvallisuusstrategia 2019, s. 4.
[11] Limnéll, ym., 2014, s. 17.

1.2 Tietomurto Suomen rikoslaissa

Rikoslain (39/1889) 38 luvun 8 §:n 1 momentin mukaan tietomurrosta määrätään:

> ”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.”

Rikoslain 38 luvun 8 §:n 2 momentin mukaan tietomurrosta tuomitaan myös se, joka oikeudettomasti ottaa selon tietojärjestelmässä olevasta tiedosta tai datasta teknisen erikoislaitteen avulla tai muuten teknisin keinoin ohittaen turvajärjestelmän, käyttäen tietojärjestelmän haavoittuvuutta tai muuten ilmeisen vilpillisin keinoin. Rikoksen yritys on säädetty rikoslain 38 luvun 8 §:n 3 momentin perusteella rangaistavaksi. Rikoslain 38 luvun 8 §:n 4 momentin mukaan pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla lainsäädännössä säädetty ankarampaa tai yhtä ankaraa rangaistusta.

Tietomurtosäännös sisältää kaksi erillistä kriminalisointia. Rikoslain 38 luvun 8 §:n 1 momentin on katsottu koskevan tietojärjestelmään tunkeutumista. Rikoslain 38 luvun 8 §:n 2 momentti kriminalisoi tietojärjestelmän ulkopuoliselta tarkkailulta tilanteissa, jotka eivät kuulu salakuuntelun tai salakatselun soveltamisalaan.[12] Tietojärjestelmän tietojenkäsittelyltä edellytetään sähköisyyttä tai muuta vastaavaa teknistä keinoa, joten säännöksen soveltamisalaan eivät kuulu fyysiset, perinteiset tietorekisterit. Rikostunnusmerkistössä edellytetään myös oikeudetonta tunkeutumista, joka tarkoittaa, että luvallinen pääsy tietojärjestelmään tai julkisen tietojärjestelmän käyttö ei ole kriminalisoitua. Tunkeutumista ja ulkopuolista tarkkailua ei ole määritelty tyhjentävästi. Lain esitöissä on todettu, että rikoksen täyttymisen kannalta turvajärjestelyn läpäisemistavalla ei ole merkitystä.[13] Rikoslain 38 luvun 8a § määrittelee törkeän tietomurron rikostunnusmerkistön. Jos tietomurto tehdään osana rikoslain 6 luvun 5 §:n 2 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai erityisen suunnitelmallisesti ja tietomurto on kokonaisuutena arvostellen törkeä, tekijä tulee tuomita törkeästä tietomurrosta. 8a §:n 2 momentin mukaan rikostunnusmerkistön täyttyessä tekijä tulee tuomita törkeästä tietomurrosta

[12] Lappi-Seppälä, ym., 2022.
[13] HE 94/1993 vp., s. 155.

sakkoon tai enintään kolmen vuoden vankeusrangaistukseen. 8a §:n 3 momentin mukaan törkeän tietomurron yritys on rangaistava.

Törkeää tekomuotoa koskeva sääntely lisättiin rikoslakiin Euroopan unionin tietojärjestelmiin kohdistuvista hyökkäyksistä annetun puitepäätöksen (2005/222/YOS) vaatimuksen perusteella. Törkeän tietomurron rikostunnusmerkistö tulee sovellettavaksi tilanteissa, jossa tietomurto on tehty esimerkiksi osana järjestäytyneen rikollisryhmän toimintaa.[14] Erityisen suunnitelmallisuuden vaatimuksen on katsottu tarkoittavan esimerkiksi sitä, että tietomurtoa on valmisteltu poikkeuksellisin toimenpitein tai kiinnijäämisen estämiseksi on ryhdytty erityisiin toimiin.[15]

Perusoikeuksien näkökulmasta tietomurtoa koskevilla rikossäännöksillä suojellaan ensimmäisenä yksityisyyden suojaa. Suomen perustuslaissa (731/1999) yksityiselämän suojaa sääntelee lain 10 §. Sen mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Yksityiselämän suoja on määriteltynä myös Euroopan ihmisoikeussopimuksen 8 artiklassa. Yksityiselämän piirin määrittely on vaikeaa, mutta oikeuskäytännön perusteella on katsottavissa, että yksityiselämän piiriä tulee tulkita laajasti.[16] Perustuslain 10 § sääntelee myös luottamuksellisen viestinnän suojasta, jonka mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Tietomurtorikosten kannalta perusoikeuksista voidaan painottaa yksityisyyden suojaa. Lainsäädännössä on mahdollistettu rajatuin kriteerein henkilön yksityisyyden rikkominen rikosten selvittämiseksi.

Tietomurron rikossääntelyllä suojeltaviin perusoikeuksiin voidaan katsoa kuuluvan myös perustuslain 15 §:n mukainen omaisuuden suoja. Omaisuuden suojan piiriin katsotaan kuuluvan varsinaisen omistusoikeuden lisäksi esimerkiksi varallisuusarvoiset immateriaalioikeudet.[17] Näin ollen omaisuuden suoja ei rajoitu vain fyysisiin esineisiin, vaan mikäli tietojärjestelmässä olevalle tiedolle on määriteltävissä varallisuusarvoa, se nauttii väistämättä omaisuuden suojaa. Tietojärjestelmä on myös jonkin tahon omistama, joten voidaan katsoa, että merkitystä ei ole ainoastaan tietojärjestelmän sisällöllä. Mikäli tietojärjestelmä on erilaisin teknisin tai fyysisin järjestelyin rajatun joukon käytössä, on myös tällä tapaa kyse omaisuuden turvaamisesta muutoinkin kuin pelkän järjestelmän sisällön osalta.

[14] Lappi-Seppälä, ym., 2022.
[15] Lappi-Seppälä, ym., 2022.
[16] Innanen, ym., 2012, s. 13.
[17] HE 309/1993 vp., s. 62.

1.3 Tutkimuskysymys

Tutkimuksen tutkimuskysymyksenä on selvittää mitä haasteita rikoslaissa määritellyn tietomurtorikoksen ja törkeän tietomurtorikoksen määrittelyyn, tutkintaan ja tuomitsemiseen liittyy. Tarkoituksena on selvittää, mitä tietomurtorikokset ovat, mihin niiden sääntely perustuu, miten rikoslain yleiset opit tulee huomioida käsiteltäessä tietomurtorikoksia, miten tietomurron rikossäännökset ovat lainkonkurrenssissa muun lainsäädännön suhteen ja mitä haasteita tietomurtorikosten tutkintaan liittyy. Tutkimuksessani hyödynnän rikoslainopillista näkökulmaa.

Johdannon jälkeisessä poikkitieteellisessä luvussa kaksi tarkastelen tietomurtorikosten kannalta relevantteja teknisiä käsitteitä ja erilaisia tapoja toteuttaa oikeudeton tunkeutuminen tietojärjestelmään. On tärkeää ymmärtää lainsäädäntöön sidoksissa oleva tekninen käsitteistö lainsäädännön tehokkaaksi arvioimiseksi. Käsittelen toisessa luvussa lisäksi tietomurtorikosten lukumäärällistä kehitystä ja siihen liittyviä syitä. Tutkimus on siis tältä osin myös kriminologinen, sen perehtyessä rikosten laadulliseen ja määrälliseen kehitykseen. Perehdyn tutkimuksessani myös tuomioistuinten tietomurroista antamiin tuomioihin, joten tutkimuksessa arvioidaan myös oikeudellista ratkaisutoimintaa.[18] Tapauksia arvioidessa tulee kuitenkin huomioida tapauskohtaiset erityisolosuhteet.

Kolmannessa luvussa tarkastelen tietomurtorikoksia rikoslain yleisten oppien kannalta. Yleisten oppien ohella tarkastelen myös tietomurtorikoksista annettavien rangaistusten mittaamista ja konfiskaatiota tietomurtorikoksen turvaamistoimenpiteenä. Neljännessä pääluvussa tarkastelen lainkonkurrenssia rikoslain tietomurtosäännöksien näkökulmasta. Perusväitteenä on tietomurtosäännöksille rikoslaissa asetettu toissijaisuus suhteessa muihin rikossäännöksiin, jos teosta on muualla laissa säädetty ankarampi tai samanlainen rangaistus. Perusväitteen tueksi tarkastelen keskeisimpiä tietomurron suhteen lainkonkurrenssissa olevia rikossäännöksiä ja määrittelen lainkonkurrenssille tunnusmerkkejä, joiden avulla on mahdollista määritellä lainkonkurrenssitilanteiden rajoja.

Viidennessä pääluvussa käsittelen tietomurtorikosten tutkintaan liittyviä haasteita. Luvussa käsittelen tietomurtorikosten esitutkintaa, sen toimittamista sähköisessä toimintaympäristössä ja kuinka esitutkinnan turvaamiseen käytettäviä pakkokeinolain mukaisia pakkokeinoja on

[18] Häyhä, 1997, s. 17.

mahdollista hyödyntää tietomurtorikosten tutkinnassa. Tarkastelen myös tietomurtorikoksia koskevaa kansainvälistä sääntelyä. Kuudennessa luvussa käsittelen yhteenvetona tutkielmani tuloksia ja esitän pohdintoja aihepiiristä sekä tietomurtorikollisuuden kehityksestä tulevaisuudessa.

1.4 Tutkimusmetodi ja oikeuslähteet

Tutkimuksen pääasiallinen tutkimusmetodi on oikeusdogmatiikka, eli lainopillinen tutkimus, mikä systematisoi voimassa olevaa oikeutta. Metodi toimii työkaluna, joka tuottaa tietoa määrätystä kohteesta.[19] Metodin pääasiallisena kohteena on tietomurtoa koskeva kansallinen lainsäädäntö. Kansallisen lainsäädännön lisäksi perehdyn kansainvälisen oikeuden näkökulmaan erityisesti Euroopan unionin ja Euroopan neuvoston lainsäädäntötyön kannalta, joka on vaikuttanut kansalliseen tieto- ja viestintärikosten sääntelyyn.

Tutkielman tavoitteena on analysoida tietomurtoa rikoslainopin keinoin. Rikoslainopin tehtävänä on rikosoikeudellisten normien systematisointi ja tulkinta.[20] Tulkinnan lähtökohtana on säädösteksti, tarkastelussa otetaan huomioon myös lainvalmisteluaineisto ja oikeustiede. Tarkastelussa fyysisen maailman kontekstiin säädetystä lainsäädännöstä haetaan ratkaisuja digitaaliseen ympäristöön.

Sähköiset järjestelmät ja digitaalinen tietojenkäsittely ovat jatkuvassa kehityksessä. Kehitys on kiihtynyt erityisesti 1990-luvun jälkeen, kun tieto- ja viestintärikokset lisättiin rikoslakiin osana rikoslakiin toteutettua kokonaisuudistusta. Jatkuvan kehityksen myötä voimassa oleva oikeus on jännittyneessä tilanteessa siihen todellisuuteen, jossa oikeusnormeja sovelletaan.[21] Tarkastelen tutkimuksessa myös tuomioistuimen tuomioita, joten tutkimuksessa tarkastellaan oikeudellista jännitettä tuomioistuimen tietomurrosta antamien tuomioiden kautta. Tämän myötä arvioin myös oikeudellista ratkaisutoimintaa ja sen muutoksia tietomurtorikoksissa. Ratkaisutoimintaa arvioitaessa tulee kuitenkin pitää mielessä jokaisen tapauksen erityisolosuhteet. Tutkimuksen pääpaino on kuitenkin oikeusjärjestyksen asetetuissa normeissa, eikä oikeudellisen menettelyn arvioinnissa.

[19] Häyhä 1997, s. 24.
[20] Lappi-Seppälä 1997, s. 192.
[21] Häyhä, 1997, s. 16.

Oikeuslähteiden keskinäiseen määrittelyyn käytän emeritusprofessori *Aulis Aarnion* oikeuslähdeoppia. Oikeuslähdeoppi määrittelee hyväksytyt oikeuslähteet, niiden keskinäisen arvojärjestyksen ja kuinka oikeuslähteitä tulee käyttää.[22] Oikeuslähdeopin keskeinen osa on käsitys siitä, mikä on oikeuslähteiden keskinäinen järjestys ja painoarvo ristiriitatilanteissa.[23] Aarnio jakaa oikeuslähteet vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin.

Vahvasti velvoittaviin oikeuslähteisiin kuuluvat ensimmäisenä kansallisen oikeuden ulkopuoliset normistot, mikä sisältää Eurooppaoikeuden sitovat osat, Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen määrätyt prejudikaatit ja Euroopan ihmisoikeussopimuksen normit.[24] Lisäksi vahvasti velvoittaviin oikeuslähteisiin kuuluvat kansallisen oikeuden normistot, joita ovat lait ja lakien nojalla annetut alemman asteiset normit, kuten asetukset, kansallisen oikeuden osaksi saatetut kansainväliset sopimukset, perustuslain perusoikeudet ja systeemiperusteet. Vahvasti velvoittaviin oikeuslähteisiin kuuluu myös maan tapa.

Heikosti velvoittaviin oikeuslähteisiin kuuluvat lainsäätäjän tarkoitus, toisin sanoen lakien esityöt ja lainvalmisteluaineisto, sekä ennakkoratkaisut, joita antavat korkeimmat tuomioistuimet Suomessa. Sallittuihin oikeuslähteisiin kuuluvat käytännölliset argumentit, eettiset ja moraaliset perusteet, yleiset oikeusperiaatteet, oikeustieteen vallitseva mielipide ja vertailevat argumentit. Kiellettyinä oikeuslähteinä Aarnion opissa pidetään lain ja hyvän tavan vastaisia sekä avoimen puoluepoliittisia argumentteja.[25]

Aarnion oikeuslähdeopin velvoittavuus rakentuu tuomarin ratkaisutoiminnan ympärille.[26] Mikäli tuomari ei noudata ratkaisutoiminnassaan vahvasti velvoittavia oikeuslähteitä, hän voi syyllistyä virkavirheeseen. Heikosti velvoittavan oikeuslähteen syrjäyttäminen ei tuo tuomarille virkavastuuta, sallitut oikeuslähteet ovat lähinnä velvoittavien oikeuslähteiden vahvistamista ja argumentoinnin tukemista varten.

Korkeimpien oikeuksien ratkaisujen asema oikeuslähteenä on katsottu olevan jännitteinen. Ratkaisut eivät ole alemman tuomioistuimen näkökulmasta muodollisesti sitovia, mutta

[22] Saarenpää, 1997, s. 264.
[23] Husa, 2020, s. 973.
[24] Aarnio, 2011, s. 82.
[25] Aarnio, 2011, s. 83.
[26] Aarnio, 2011, s. 84.

tosiasiallisesti ennakkopäätöksillä on vaikutus alempien tuomioistuinten toimintaan.[27] Käytettäessä heikosti velvoittaviin oikeuslähteisiin kuuluvia ennakkoratkaisuja oikeuslähteenä, ratkaisut on mahdollista kategorisoida deklaratiivisiin ja demonstratiivisiin ennakkopäätöksiin. Deklaratiivisten ennakkopäätösten oikeusohje on rinnastettavissa lain säännökseen. Demonstratiivisten ennakkopäätösten oikeusohje toimii esimerkkinä tuomioistuimen ratkaisuharkinnassa huomioon otettavista seikoista.[28] Tutkimuksessani hyödynnän kategorisointia ja tarkastelen ennakkopäätöksiä demonstratiivisesta kulmasta, mitä seikkoja ennakkopäätöksistä on otettavissa huomioon ratkaisuharkinnan kannalta.

Aarnion oikeuslähdeoppi ei ota ennakkoratkaisujen lisäksi kantaa muiden tuomioistuinten antamien tuomioiden asemaan oikeuslähteenä. Oikeuskirjallisuudessa on esitetty, että hovioikeuksien ratkaisujen tosiasiallinen merkitys ja asema oikeuslähteenä ovat muodollista asemaansa merkittävämpiä.[29] Hovioikeuden ratkaisut ovat todellisuudessa valtaosa lainvoimaiseksi jäävistä ratkaisuista.[30] Tarkastelen myös alempien tuomioistuinten tapauksia ja hyödynnän samaa demonstratiivista lähestymistä myös alempien tuomioistuinten tuomioiden tarkastelussa.

Hankkiakseni alempien tuomioistuinten tuomioita tarkasteltavaksi, lähetin tietopyyntökyselyn Helsingin, Turun, Itä-Suomen, Vaasan ja Rovaniemen hovioikeuksiin. Tietopyynnöissä pyysin tuomioistuimia lähettämään heidän antamiaan tuomioita tietomurrosta ja törkeästä tietomurrosta vuosina 2016–2021. Tietopyynnön perusteella vastaanotin hovi- ja käräjäoikeuksien tuomioita Helsingin ja Vaasan hovioikeuksista, sekä Helsingin, Itä-Uudenmaan, Keski-Suomen ja Pohjanmaan käräjäoikeuksista yhteensä 16 kappaletta. Hovioikeuksien kahdeksasta tuomiosta kuusi oli Helsingin hovioikeuden tuomioita, ja kaksi Vaasan hovioikeuden. Käräjäoikeuksien tuomioista viisi oli Helsingin käräjäoikeuden tuomioita. Loput kolme käräjäoikeuden tuomiota sijoittuivat yksittäin muihin käräjäoikeuksiin. Itä-Suomen ja Rovaniemen hovioikeus ei käsitellyt yhtään tietomurtoa tai törkeää tietomurtoa määriteltynä ajanjaksona. Turun hovioikeus ei vastannut ollenkaan sähköpostitse lähetettyyn tietopyyntöön.

[27] Husa, 2020, s. 984.
[28] Kemppinen, ym., 2020, s. 1042.
[29] Kalkela, ym., 2021, s. 234.
[30] Kalkela, ym., 2021, s. 234.

Vastaanottamani tuomiot mahdollistivat rikosten ja niiden tuomioiden syvällisemmän analysoinnin tilastotutkimuksen ohella. Tapauskohtainen tarkastelu konkretisoi abstraktin rikossäännöksen todellisuuteen ja osoittaa lainsäädännön ongelmakohtia demonstratiivinen lähtökohta huomioiden. Lähdeaineistona olevien oikeustapausten tehtävänä on siis osaltaan tarkoitus toimia muuta argumentointia tukevana oikeuslähteenä.

Yleisellä tasolla tarkastellen lähdeaineisto on osin poikkitieteellistä aiheen teknisestä luonteesta johtuen. Tekninen sanasto ja ilmiöt käsitellään vaadittavalla tasolla aiheen kannalta, joka edellyttää tietotekniikkaan liittyvää käsitteistöä. Kyse on rikosten tunnusmerkistöihin liittyvien merkittävien seikkojen systematisoinnista. Rikosoikeus ylipäänsä on yhteydessä muihinkin kuin oikeustieteellisiin aspekteihin sen tehtävän, yhteiskuntarauhan turvaamisen myötä.[31]

[31] Lappi-Seppälä, 1997, s. 189.

2 Tietomurto käsitteenä

2.1 Tietomurtosääntelyn historia

Tieto- ja viestintärikoksien nykymuotoon johtavan sääntelyn kehityksen voidaan katsoa alkaneen 1980-luvulla. Taloudellisen yhteistyön ja kehityksen järjestö, Organisation for Economic Co-operation and Development, määritteli tietokoneliitännäisiä rikoksia käsittelevässä raportissaan ensimmäisenä käsitteen tietokonerikos.[32] Tietokonerikoksen käsite ja ehdotus sen rangaistavuudesta määriteltiin sisältämään kattavasti laiton, epäeettinen tai luvaton käytös, joka oli yhteydessä automatisoituun tietojenkäsittelyyn tai datan käsittelyyn.[33] Raportin yhteenvedossa järjestön jäsenmaita suositeltiin kriminalisoimaan raportissa ehdotetut ja kuvaillut teot.[34] Myös Euroopan neuvoston asettama asiantuntijakomitea aloitti 1980-luvulla komiteatyön, jonka tavoitteena oli selvittää tietokonerikoksia ja tarkastella tietokonerikosten eri ilmenemismuotoja, tavoitteenaan kehittää jäsenmaille ohjeistusta niiden käsittelyyn.[35]

Ensimmäiset rikokset, joihin automatisoitu tietojenkäsittely liittyi, ilmenivät 1970- ja 1980-lukujen taitteessa. Rikoksiin liittyi useasti pankkitoiminta ja tarkoitus saada petoksen keinoin perusteettomasti rahaa, harhauttamalla tietojenkäsittelyä eri keinoin.[36] Tässä vaiheessa tietokone tai tietojärjestelmä katsottiin enemmän rikoksentekovälineeksi, kuin rikoksen kohteeksi. Lukuun ottamatta petosrikoksia, yleisesti tietokoneisiin liittyviä rikoksia, erityisesti tietomurtoja ja muita hakkerointirikoksia pidettiin nuorison hauskanpitona ja tekijän oman osaamisen haastamisena ilman konkreettista hyödyn tavoittelua. Vuoden 1984 loppuun mennessä Suomessa oli kirjattu 21 rikosta, joihin liittyi automatisoitu tietojenkäsittely.[37]

Rikoslain erityisen osan toinen osittaisuudistus tuli voimaan 1.9.1995.[38] Osittaisuudistuksen toisessa vaiheessa rikoslain (39/1889) 38 luku uudistettiin kattamaan tieto- ja viestintärikokset. Tieto- ja viestintärikosten uudistuksen vaikuttimena toimi Euroopan neuvoston asettaman

[32] OECD, 1986, s. 29.
[33] OECD, 1986, s. 69.
[34] OECD, 1986, s. 69.
[35] European Committee on Crime Problems, 1990, s. 9.
[36] Sieber, 1986, s. 8.
[37] Sieber, 1986, s. 32.
[38] Matikkala, 2013, s. 93.

asiantuntijakomitean tietokonerikoksia koskeva suositus.[39] Suosituksen perusteella tietokonerikollisuutta pidettiin uutena ilmiönä, joka on mahdollistanut uusia rikoksentekomahdollisuuksia ja mahdollistanut myös uusia piirteitä perinteisenä pidetyille rikoksille.[40] Suositus piti kuitenkin automaattista tietojenkäsittelyä ja siihen liittyviä rikoksia osana rikollista kehitystä, eikä kokonaan uudenlaisena ilmiönä.

Ennen 1990-luvun rikoslain erityisen osan osittaisuudistusta tieto- ja viestintärikosten sääntely oli hajaantuneena rikoslain lukuihin. Uudistuksen myötä sääntely oli yhdessä paikassa. Uudistus oli osa suurempaa rikoslain uudistusta, jonka tavoitteena oli kokonaisvaltainen rikoslain yhtenäistäminen.[41] Suojeltavaksi oikeushyväksi katsottiin suojautuminen ulkopuolista tunkeutumista vastaan, joka hallituksen esityksessä rinnastettiin kotirauhaan. Tietomurron osalta rikoslaissa haluttiin säätää rangaistavaksi tietojärjestelmän luvattoman käytön ja siellä toimimisen lisäksi tunkeutuminen järjestelmään. Perusteluissa tämän katsottiin suojaavan erityisesti tietokonerauhaa, eli tietojärjestelmiä ulkopuolista tunkeutumista vastaan.[42] Tietokonerauhasta tulee kuitenkin erottaa sellainen tarkkailu, joka on katsottavissa salakuunteluksi tai salakatseluksi. Kyseisiä rikoksia säätelevät rikoslain 24 luvun 5 ja 6 §:t. Tietokonerauhan käsitteen määrittelyn ja varmentamisen lisäksi jälkikäteen voidaan katsoa, että tietomurron säätäminen rangaistavaksi on varmistanut, että Suomesta ei ole tullut suotuisaa paikkaa toteuttaa tietokonerikoksia, etenkin niiden kansainvälinen luonne huomioiden. Toisessa vaiheessa uudistetun rikoslain säädökset tulivat voimaan 1.9.1995.

Kansallinen tieto- ja viestintärikoksia koskeva sääntely koki ensimmäisen kerran huomattavia muutoksia 2000-luvulla kansainvälisen lainsäädäntökehityksen myötä, osin kansainvälisen yhteistyön perusteella. Vuonna 2006 tieto- ja viestintärikoksiin kohdistunut rikoslain uudistus päivitti kansallisen lainsäädännön huomioimaan yhtäaikaisesti sekä Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen[43], että Euroopan Unionin puitepäätöksen vaatimukset tietojärjestelmiin kohdistuvista hyökkäyksistä.[44] Hallituksen esitys totesi puitepäätöksen 2005/222/YOS sisältävän määräyksiä samoista asioista, kuin mitä yleissopimus sisälsi.[45] Puitepäätöksen tavoitteena oli parantaa viranomaisen tietojärjestelmiin kohdistuvien

[39] HE 94/1993 vp., s. 17.
[40] HE 94/1993 vp., s. 18.
[41] HE 94/1993 vp., s. 13.
[42] HE 94/1993 vp., s. 155.
[43] Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus 60/2007
[44] Euroopan unionin neuvosto, 2005/222/YOS.
[45] HE 153/2006 vp., s. 1.

hyökkäyksiin liittyvää yhteistyötä,[46] yleissopimuksen säännellessä yleisemmin tietotekniikkarikollisuutta.

Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus on kansainvälinen yleissopimus, joka on ratifioitava tai hyväksyttävä ja saatettava osaksi kansallista lainsäädäntöä.[47] Tietoverkkorikollisuutta koskevan yleissopimuksen voimaansaattamisen seurauksena lainsäädäntöön lisättiin uusia tietotekniikkarikosten tekomuotoja, kuten törkeä tietomurto. Yleissopimus osaltaan lisäksi selvensi tietomurron käsitettä. Sopimuksen 2 artiklan mukaan luvaton tunkeutuminen edellyttää pääsyä tietojärjestelmään tai sen osaan. Tunkeutumiselta edellytetään tahallisuutta ja rikos tulee tehdä turvajärjestely murtamalla.

Yleissopimus määritteli erityisesti myös tietoverkkorikollisuudessa käytettäviä pakkokeinoja ja viranomaisten toimivaltaa tietoverkkorikollisuuden torjunnassa ja tutkinnassa. Pakkokeinot koskevat erityisesti tallennettuun dataan kohdentuvaa etsintää, takavarikkoa ja tiedustelua. Lisäksi yleissopimus määrää sopimusosapuolten keskinäisestä oikeusavusta tietoverkkorikollisuuden tutkinnassa. Sopimuksen puitteissa vaadittu suomalainen jatkuvasti tavoitettavissa oleva yhteyspiste on tasavallan presidentin tietoverkkorikollisuutta koskevan yleissopimuksen voimaansaattamisasetuksen 60/2007 3 §:n perusteella keskusrikospoliisi.

2010-luvulla tietoverkkorikosten kansalliseen sääntelyyn vaikutti Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksistä (tietoverkkorikosdirektiivi). Direktiivi korvasi myös aikaisemmin annetun Euroopan unionin neuvoston puitepäätöksen 2005/222/YOS. Direktiivin oikeusperustana on Euroopan unionin toiminnasta tehdyn sopimuksen 83 artikla, missä todetaan tietokonerikollisuuden olevan yksi rikollisuuden aloista, joilla voidaan toteuttaa rikostunnusmerkistöjä ja seuraamuksia koskevia lähentämistoimenpiteitä.[48]

Uuden direktiivin 9 artikla määritteli direktiivin soveltamisalaan kuuluville rikoksille, kuten laittomalle tunkeutumiselle tietojärjestelmään vähimmäisvaatimuksen rikoksista määrättäville seuraamuksille. Tämän myötä direktiivin kansallinen voimaansaattaminen edellytti tietomurron ja törkeän tietomurron enimmäisrangaistuksien korottamista aikaisemmista.

[46] Melander, 2015, s. 481.
[47] Melander, 2015, s. 30.
[48] Melander, 2015, s. 480.

Enimmäisrangaistusten korottaminen mahdollisti useampien pakkokeinolain pakkokeinojen käyttämisen entiseen verrattuna. Lainmuutoksen jälkeen käytettävissä olevien pakkokeinolain pakkokeinojen edellytyksenä on määritelty, että ankarin rangaistus on vähintään kaksi vuotta vankeutta.

Lisäksi tietomurron rikossäännöksen tunnusmerkistöä muutettiin direktiivin perusteella kattamaan järjestelmään oikeudettoman pääsyn lisäksi pääsyyn tietojärjestelmässä olevaan tietoon ja tiedon hankkimiseen järjestelmässä olevasta datasta. Lainvalmisteluaineisto käsitteli myös tietomurron lainkonkurrenssitilanteita suhteessa muihin tieto- ja viestintärikoksiin, määrittelemällä tietomurron mahdolliseksi valmisteluteoksi suhteessa esimerkiksi datavahingontekoon tai tietoliikenteen häirintään.[49] Datavahingonteko on määritelty rikoslain 35 luvun 3 a §:ssä. Kyse on tiivistettynä tietojärjestelmään tallennetun datan tärvelemisestä. Tietoliikenteen häirinnän määritelmä on rikoslain 38 luvun 5 §:ssä. Tietoliikenteen häirinnässä on lyhyesti kyse postiliikenteen tai tele- tai radioviestinnässä käytettävän laitteen toiminnan oikeudettomasta estämisestä tai häirinnästä. Lainkonkurrenssissa tietomurron tunnusmerkistö väistyy suhteessa näihin tunnusmerkistöihin.

2.2 Tietomurron tekninen käsitteistö

Tietomurto on kyberrikos, jossa on kyse oikeudettomasta tunkeutumisesta tietojärjestelmään missä teknisin keinoin käsitellään tai säilytetään dataa. Tietojärjestelmä on määriteltävissä tietoverkkorikosdirektiivin 2 artiklan kohdan a perusteella laitteeksi tai toisiinsa kytketyiksi laitteiksi, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten. Toisin sanoen kyse on toisiinsa kytketyistä tietokoneista. Tietomurto on mahdollista toteuttaa teknisin apuvälinein, tietoverkossa tai yksinkertaisimmillaan esimerkiksi arvaamalla käyttäjätunnus ja salasana oikein. Henkilön teossa käyttämä tietokone tai muu tekninen laite on rikoksentekoväline, lisäksi yleisesti rikoksen täyttymisen edellytyksiksi voidaan katsoa internet-yhteys sekä kohteena oleva tietojärjestelmä.

Datan määritelmä löytyy kansallisen lainsäädännön tasolla pakkokeinolain (806/2011) 7 luvun 1 §:stä. Datalla tarkoitetaan tietoa, joka on teknisessä laitteessa, tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla. Tietoverkkorikosdirektiivin 2 artiklassa data

[49] HE 232/2014 vp., s. 12.

määritellään sellaisten tosiseikkojen, tietojen tai käsitteiden esitykseksi, joka soveltuu käsiteltäväksi tietojärjestelmässä. Datalle ei siis anneta merkittäviä laadullisia kriteereitä, vaan dataa on käytännössä kaikki sähköiselle alustalle tallehdittu tieto.

Oikeustieteen professori *Xingan Li* on vienyt ajatuksen datan määritelmästä pidemmälle väitöskirjassaan ”Cybercrime and deterrence: networking legal systems in the networked information society”, ja jakaa sähköiselle alustalle tallennettavan datan viiteen luokkaan. Ensimmäinen luokka on digitaalinen informaatio, millä on positiivista arvoa. Arvo voi perustua datan luotettavuuteen, yksityisyyteen tai taloudelliseen hyödynnettävyyteen, lisäksi datan arvo on riippuvainen sen eheydestä ja levinneisyydestä. Mikäli data tuhoutuu tai sitä käytetään luvattomasti, arvo on menetetty. Toisena määriteltynä luokkana on data, minkä arvo on neutraalia. Neutraaliarvoisen datan on mahdollista olla positiivisesti tai neutraalisti arvokasta, riippuen sen käyttötarkoituksesta. Listaus sähköpostiosoitteista ei sisällä sellaisenaan arvokasta tietoa, mutta on käytettävissä esimerkiksi mainosviestien lähettämiseen. Mainosviestien lähettämisellä on mahdollista luoda välillisesti arvoa.[50]

Kolmantena luokkana on arvoton data. Arvottomalle datalle ei ole mahdollista määritellä lainkaan arvoa. Arvoton data ei sisällä informaatiota, joka olisi hyödynnettävissä positiivisesti. Arvottomalle sähköiselle informaatiolle on nähtävissä lähinnä negatiivisia käyttötarkoituksia. Arvottoman datan käsittely tietojärjestelmän käyttäjien näkökulmasta on ajan tuhlausta. Lin mukaan neljäntenä luokkana on negatiivista arvoa sisältävä data, joka on katsottavissa haitalliseksi ja epäjärjestystä aiheuttavaksi. Negatiivinen data ei väitetysti ole olemassa ilman ihmisvuorovaikutusta. Negatiivisen datan levittäminen ja käyttö voi aiheuttaa myös varallisuusvahinkoja. Esimerkki haitallisesta datasta ovat tietokonevirukset. Tietokonevirukset aiheuttavat häiriöitä ja haittaa kohteeksi joutuvassa päätelaitteessa, lisäksi ne ovat aina ihmisen kehittämiä. Myös muu vastaava lainsäädännössä laittomaksi katsottu aineisto sähköiseen muotoon tallennettuna voi olla negatiivisen arvon omaavaa dataa.[51]

Viides ja viimeinen Lin väitöskirjassa esiteltävä dataluokka on lainsäädännöllisessä mielessä katsottavissa kiistanalaiseksi, koska sitä kohdellaan eri tavoin eri maiden lainsäädännössä. Kyse on lähinnä sananvapauden ja vapaan ilmaisun kriteerein arvioitavasta informaatiosta

[50] Li, 2008, s. 70.
[51] Li, 2008, s. 72.

sähköisellä alustalla, mikä voidaan arvioida eri tavoin ja eri näkökulmista, riippuen käsillä olevan valtion lainsäädännöstä.[52]

Tietomurron näkökulmasta merkityksellisintä on Lin väitöskirjan mukaisesti ensimmäisen luokan data, eli positiivisesti arvokas data sen sisältämän arvon perusteella. Positiivisesti arvokkaalle datalle on määriteltävissä suojeltavaksi oikeushyväksi omaisuuden suoja, sen sisältäessä arvoa, joka voidaan menettää. Lopulta kyse on subjektiivisesta arviosta datan laadusta. Teknisesti kaikki data tallentuu samalla tavalla tietojärjestelmään, eikä käytännössä sähköisen tietojärjestelmän ominaisuuksilla ole merkitystä rangaistavuuden kannalta. Suomalainen lainsäädäntö on neutraali datan laadulle, rangaistavuuden perustuessa sähköisen tietojärjestelmän oikeudettomaan käyttöön. Suojeltava oikeushyvä on tietojenkäsittelyrauha, joka ei ole riippuvainen käsiteltävälle tiedolle määritellystä arvosta. Tietomurtoon liittyvissä sekä seurannaisissa rikoksissa merkitystä voi kuitenkin olla myös datan arvolla. Yksityiselämää loukkaava tiedon levittäminen ei voi perustua arvottomaan dataan, koska levitettävän tiedon tulee aiheuttaa rikoslain 24 luvun 8 §:n mukaan vahinkoa, kärsimystä tai uhriin kohdistuvaa halveksuntaa. Henkilön kannalta yhdentekevän tiedon levittäminen ei aiheuta rikoslain edellyttämää vahinkoa tai kärsimystä.

Yhdysvaltojen lainsäädännön käsitys datan määritelmästä sisältää erilaisen tavan ja näkemyksen määritellä datan käsite sekä tietomurtorikos. Yhdysvalloissa lainsäädäntö on tekniikkaneutraalia tietojärjestelmään tunkeutumisen kohteen kannalta. Tietokone tai vastaava digitaalista tietoa sisältävä laite vertautuu perinteiseen fyysistä tietoa sisältävään alustaan, kuten esimerkiksi kirjeeseen tai arkistokaappiin.[53] Tietokone on vain kohde, joka sisältää tietoa.

Tietomurrossa murtautumistoimenpiteiden kohteena oleva tietojärjestelmä on yhteydessä tietoverkkoon, yleensä globaaliin internet-verkkoon. Vaihtoehtoisesti tietojärjestelmä on osa rajatumpaa sisäverkkoa, johon voi olla yhteydessä vain määritellyistä paikoista. Tietoverkko kokonaisuutena muodostuu useasta eri kerroksesta, jossa eri tekniikoiden yhdistelmällä informaatio liikkuu sähköisten laitteiden välillä. Tietoverkon eri tasoissa on kyse viestin ohjaamisesta oikeaan paikkaan, tiedon salaamisesta muilta verkon käyttäjiltä sekä käyttäjän tunnistamisesta. Tietoverkkoa on mahdollista käyttää nykyaikana tavanomaisen tietokoneen lisäksi monilla laitteilla, esimerkiksi älypuhelimella, joten käsittelyn selkeyttämiseksi puhun seuraavaksi

[52] Li, 2008, s. 73.
[53] Oerlemans, 2017, s. 345.

päätelaitteesta puhuessani sähköisestä välineestä, jolla on mahdollisuus ottaa yhteyttä tietoverkkoon ja toimia siellä.

Tietomurtorikoksen edellytysten kannalta voidaan tietojärjestelmän toiminnallisilla ominaisuuksilla katsoa olevan merkitystä. Tietojärjestelmän rooli voi olla nykyään moninainen, koska data voi olla perinteiseksi miellettävien rekisterimerkintöjen lisäksi esimerkiksi videokuvaa tai sosiaalisen median tilapäivityksiä ja muita vastaavia tietoja. Rikoksen keskiössä on oikeudeton tunkeutuminen tietojärjestelmään, joten sen sisältämän tiedon laadulla ei ole merkitystä rangaistavuuden kannalta. Tietomurtorikoksen kannalta relevanttia on tietojärjestelmän toiminta. Mikäli tietojärjestelmä ei ole käytössä, oikeudeton tunkeutuminen ei lähtökohtaisesti ole mahdollista.[54] Tunkeutumisen kohteena oleva tietojärjestelmä ja sen sisältämät tiedot voivat toimia alustana myös muille rikoksille, jos tietojärjestelmän tietoja käytetään muiden rikosten toteuttamiseen, kuten esimerkiksi yksityiselämää loukkaavan tiedon levittämiseen.

Tietoverkossa liikkuminen jättää digitaalisia jälkiä tietojärjestelmän eri kerroksiin, joita yhdistelemällä on mahdollista yksilöidä päätelaitteella sähköisessä ympäristössä toimiva henkilö. Tällaisia tietojärjestelmään tallentuvia tietoja ovat esimerkiksi verkossa liikenteen oikeaan laitteeseen ohjaava, tietoverkkoon yhdistettäessä päätelaitteelle määräytyvä IP-osoite. IP-osoite on verrattavissa puhelinnumeroon tai postiosoitteeseen, joka ohjaa tietoliikenteen oikealle päätelaitteelle.[55] IP-osoitteen lisäksi päätelaite on erikseen yksilöitävissä varmuudella valmistajan määrittämällä uniikilla MAC-osoitteella. MAC-osoite on laitteen muuttumaton tunnus, kun taas laitteen IP-osoite vaihtuu yhdistettäessä uudelleen tietoverkkoon.

Erityisesti IP-osoitetta on käytetty tieto- ja viestintärikoksissa johtolankana rikoksen selvittämiseen, selvittämällä IP-osoitteen asiakastieto tietoliikennepalveluntarjoajalta. Käytännössä IP-osoitteella selvitettävät tilaajatiedotkaan eivät välttämättä ole kuitenkaan suora johtolanka rikoksen tekijästä. Yhteyden tilaajatietoihin voi olla merkittynä täysin eri henkilö, kuin joka on yhteyden todellinen käyttäjä tietomurtoa toteutettaessa. Palveluntarjoajan kannalta tilaajatietojen pääasiallinen käyttö liittyy esimerkiksi laskutuksen toteuttamiseen ja vianselvitykseen. Pääasiallinen käyttötarkoitus ei ole tietojen tallentaminen viranomaiskäyttöön mahdollisten rikoksen selvittämisen varalta.[56]

[54] Li, 2008, s. 128.
[55] Shipley, 2014, s. 43.
[56] Innanen, ym., 2012, s. 80.

Tietomurtorikoksen toteuttava taho voi olla täysin ulkopuolinen henkilö, järjestelmän toinen käyttäjä tai muuten järjestelmän kanssa tekemisissä ollut henkilö. Tahallinen tietomurtorikos edellyttää lähtökohtaisesti kohteena olevan järjestelmän tuntemusta. Mikäli järjestelmätuntemus ei perustu ennakolta tietojärjestelmän parissa työskentelyyn, rikoksen valmisteleva osuus voi olla ajallisesti huomattavasti pidempi ja vaativampi osasuoritus matkalla rikoksen täyttymiseen. Sosiaalisen median palveluiden kehittyminen ja käyttäjämäärän kasvu on laajentanut tietomurron henkilöiden profiilin määritelmää. Sosiaalisen median palveluissa on lopulta kyse tietojärjestelmistä, joihin palvelun käyttäjät tallentavat dataa. Erilaisia sosiaalisen median palveluita myös käytetään nykyisin paljon, joten alustana sosiaalinen media on potentiaalinen tietomurtorikoksille.

2.3 Tavoista toteuttaa tietomurto

Tietomurron perustuessa järjestelmän käyttäjästä johtuviin heikkouksiin, lähtökohtaisesti tietomurron tavoitteena on saada oikeudettomasti haltuun tietojärjestelmään kirjautumisen mahdollistavat tunnukset. Heikkoudet tietojärjestelmän turvallisuudessa eivät perustu teknisiin toimenpiteisiin, vaan henkilöllisiin seikkoihin. Tunnusten hankinta voi tapahtua sosiaalisin keinoin, kuten puhtaasti tunnusten vakoilulla tai tietojen kalastelemisella sähköisessä järjestelmässä tai sen ulkopuolella. Tunnukset ovat myös vain voineet kulkeutua henkilön tietoon ilman erityisiä toimenpiteitä. Käyttäjästä johtuva heikkous voi kuitenkin selvitä myös osin teknisin keinoin, esimerkiksi väsytyshyökkäyksellä.

Väsytyshyökkäyksessä perusajatuksena on kaikkien mahdollisten salausavainten järjestelmällinen kokeilu oikean löytämiseksi.[57] Tällöin tietomurron onnistuminen perustuu määrälliseen toimintaan laadullisen toiminnan sijasta, mikä edellyttää muihin tapoihin verrattuna enemmän aikaa. Väsytyshyökkäystä on myös mahdollista kutsua sanakirjahyökkäykseksi, joka kuvastaa omalta osaltaan tietomurron tekotapaa. Väsytyshyökkäys on mahdollista toteuttaa ohjelmallisesti tai yksinkertaisimmillaan arvaamalla salasanaa oikein kirjautumiskehotteessa, mikäli tunnus on riittävän heikko, eikä järjestelmä rajoita kirjautumisyritysten määrää huomattavasti. Ohjelmallisesti toteutettuna väsytyshyökkäys kokeilee järjestelmällisesti tietokonealgoritmilla, joka perustuu esimerkiksi sanakirjan sisältävään tiedostoon, mahdollisia salasanoja ja niiden yhdistelmiä. Ohjelmallinen väsytyshyökkäys on huomattavasti nopeampaa, kuin henkilön

[57] VAHTI 4/2008, s. 140.

itsenäisesti ilman avustavaa ohjelmistoa suorittama salasanan arvailu. Väsytyshyökkäyksen onnistuminen perustuu siihen, kuinka paljon henkilöllä on käytettävissä aikaa ja kuinka vaikeaa kirjautumiskehotteen saavuttaminen on tai onko sen käyttöä rajoitettu.

Tietojärjestelmään oikeudettomaan pääsyyn tarvittavien tunnusten tai tietojen hankinta on mahdollista toteuttaa myös tarkkailemalla henkilöä tai toteuttamalla tietojenkalastelua. Tietojenkalastelussa tietojärjestelmän käyttäjä huijataan syöttämään omat tunnuksensa esimerkiksi väärennetylle kirjautumissivulle tai antamaan kirjautumistiedot jollain muulla perusteettomalla verukkeella.[58] Tarkkailu voi tapahtua fyysisesti tarkkailemalla henkilöä, esimerkiksi seuraamalla hänen kirjautumistaan tietojärjestelmään tai asettamalla vakoiluohjelmisto henkilön käyttämälle päätelaitteelle. Mikäli tietojärjestelmään tunkeutumisen esitekona on yksityisyyttä loukkaava teko, rikoksen esitutkintaan tulee kiinnittää erityistä huomiota myös valmistelutekojen osalta.

Käyttäjän heikkouteen perustuva hyökkäys on mahdollista toteuttaa myös kokonaan ilman tietoteknistä tietämystä. Katson tapaukset, joissa rikoksen uhrin salasana on ennalta tiedossa tai arvattavissa, kuuluvan käyttäjän heikkouteen perustuvien tietomurtojen luokkaan. Käyttäjätunnuksen ja salasanan arvaaminen on käytännössä ainoa keino tunkeutua oikeudettomasti tietojärjestelmään ilman tietoteknistä erityistietämystä. Käyttäjän heikkouteen perustuvassa hyökkäyksessä on mahdollista, että itse tietojärjestelmä ja sen omistaja eivät ole varsinaisesti rikoksen täysimääräisessä uhriasemassa, jos käyttäjätiliin tunkeutuminen perustuu esimerkiksi kirjautumistietojen vakoilemiseen tai arvaamiseen, eikä varsinaiseen tietojärjestelmän haavoittuvuuden tai puutteen hyödyntämiseen tietomurrossa.

Väsyttämällä tapahtuvan tietomurtoyrityksen onnistumista ovat vaikeuttaneet nykyisin eri tahojen yleisesti salasanoille vaatimat erikoiskriteerit. Salasanan tulee kriteerien perusteella sisältää esimerkiksi numeroita, erikoismerkkejä tai suuria kirjaimia. Paras tapa suojautua onkin välttää yleisiä salasanoja. Mitä pidempi ja monimutkaisempi salasana on, sitä vaikeampi se on arvata. Väsytyshyökkäys on ehkäistävissä tietojärjestelmän ylläpitäjän näkökulmasta esimerkiksi kirjautumisyritysten määrällisellä rajaamisella, kaksivaiheisella tunnistautumisella ja käyttämällä kuvavarmennusta osana kirjautumista,[59] jolloin salasanan arvaus hidastuu huomattavasti. Kaksivaiheinen tunnistautuminen voi vaatia esimerkiksi kirjautumisen hyväksymisen

[58] Fortinet: ”Types of Cyber Attacks”.
[59] Fortinet: ”What is a Brute Force Attack?”.

käyttäjän hallussa olevalla erillisellä laitteella, kuten älypuhelimella. Tämän myötä pelkkä kirjautumistietojen hallussapito ei riitä oikeudettomaan tunkeutumiseen tietojärjestelmään. Kuvavarmennuksessa käyttäjän tulee tunnistaa hänelle näytettävästä kuvasta kysyttyjä yksityiskohtia, kuten kirjaimia tai numeroita, mitä tekoäly ei toistaiseksi pysty itse tekemään.

Vaihtoehtoisesti tietomurto voi perustua ja kohdentua käyttäjään perustuvien heikkouksien sijasta itse järjestelmään ja sen ominaisuuksiin. Ohjelmallisesti toteutettavassa tietomurrossa on kyse tietoteknistä erityistietämystä vaativasta toiminnasta, jossa hyödynnetään erilaisia tietomurtoon soveltuvia ohjelmistoja ja tiedossa olevia tietoturva-aukkoja, joiden avulla järjestelmä saadaan toimimaan halutulla tavalla oikeudetta. Ohjelmallisesti toteutettava tietomurto on prosessi, joka edellyttää ennen varsinaista tietojärjestelmään tunkeutumista suunnittelua ja valmistelevia toimenpiteitä. Tietojärjestelmästä selvitetään ensimmäisenä hyökkäyssuunnitelman laatimiseksi, mitä ohjelmistoja ja tekniikoita tietojärjestelmä sisältää.[60] Tiedonhankinnan jälkeen on mahdollista suorittaa tietojärjestelmän uhka-analyysi ja tietomurron varsinainen suunnittelu. Uhka-analyysin tavoitteena on löytää järjestelmästä heikkouksia, joiden avulla tietomurto on mahdollista toteuttaa. Suunnitteluvaiheen jälkeen varsinainen tietomurto voidaan aloittaa, jolloin rikos siirtyy selkeästi valmistelusta yritysvaiheeseen.

Tapoja toteuttaa tietomurto ohjelmallisesti on useita erilaisia, mutta yksi nykyisin yleisimpiä tapoja toteuttaa tietomurto on SQL-injektio, joka syöttää murtautujan kannalta suotuisia ohjelmistokäskyjä tietojärjestelmään. Murtautujan tietojärjestelmään lähettämässä kyselyssä lähetetään myös muita, kuin tavanomaiseen viestintään liittyviä tietoja, jotka tietojärjestelmä tulkitsee muuna kuin tavanomaisena kyselynä ja reagoi myös niihin tavanomaisen tietojenkäsittelyn yhteydessä.[61] Yksinkertaistettuna ohjelmistokäsky voi olla esimerkiksi järjestelmään sisäänkirjautuminen, jossa ohjelmistokäskyjen syöttämisessä hyödynnetään tietojärjestelmässä olevaa heikkoutta, joka mahdollistaa käskyn antamisen ilman käskyjen syöttöoikeuden varmentamista. Ohjelmallisesti murtautuminen voi tapahtua myös hyödyntämällä erilaisia puutteita tai haavoittuvuuksia järjestelmässä. Haavoittuvuudella tarkoitetaan tietojärjestelmän tai sen osan heikkoutta, jota voidaan hyödyntää tunkeutumisessa.[62] Haavoittuvuus tai puute voi esiintyä esimerkiksi käyttäjän tietojärjestelmän pääsynhallinnassa, jolloin murtautuja hankkii itselleen oikeudet toimia järjestelmässä. Tietojärjestelmä on myös voitu konfiguroida väärin. Tämän myötä

[60] Wylie, ym., 2021, s. 24.
[61] OWASP Foundation, 2017.
[62] VAHTI 4/2008, s. 107.

vääristä asetuksista aiheutuva haavoittuvuus perustuu liian heikkoon järjestelmän suojautumiseen ulkoisilta uhilta.[63]

Tehokas suojautuminen ohjelmallisilta murtautumiskeinoilta edellyttää tietojärjestelmän omistajalta tai ylläpitäjältä tietoteknistä erityistietämystä tai sellaisen hankintaa palveluna ulkopuoliselta toimijalta. Toisaalta haavoittuvuuksilta suojautuminen voi olla samanaikaisesti hyvin yksinkertaista, tietojärjestelmän ohjelmien ja muiden toiminnallisten komponenttien päivittäminen aktiivisesti viimeisimpään versioon pitää omalta osaltaan huolen, että hyökkääjä ei voi käyttää jo korjattuja ja yleisesti tiedossa olevia puutteita tietojärjestelmässä hyökkäykseen. Näin ollen voidaan myös katsoa, että osa tietomurtorikosten rikostentorjunnasta on tietojärjestelmän omistajan vastuulla. Mitä vähemmän hyökkääjällä on käytettävissään esimerkiksi haavoittuvuuteen perustuvia tietoturva-aukkoja tietojärjestelmässä, sitä epäsuotuisemmat olosuhteet hänellä on toteuttaa tietomurtorikos.

Tutkimuksen tapausaineiston tapauksissa tietomurrot eivät olleet ohjelmallisesti toteutettuja tietomurtoja, vaan oikeudeton tunkeutuminen tapahtui käyttäjään perustuvilla heikkouksilla. Tapauksissa, joissa tietomurto on myönnetty[64] tai katsottu selvitetyksi[65], on mainittuna vastaajan tienneen uhrin kirjautumistiedot tietojärjestelmään, tai muuten selvittäneen kirjautumistiedot käyttämällä uhrille kuuluvaa tietovälinettä.

2.4 Asianomistajan merkityksestä tietomurrossa

Suomessa rikosprosessi perustuu ajatukselle siitä, että kaikki rikokset ovat virallisen syytteen alaisia ja rikollisten rangaistusvastuun toteuttaminen kuuluu valtiolle.[66] Lähtökohtaisesti päätös syytteen nostamisesta esitutkinnan perusteella kuuluu viralliselle syyttäjälle. Asiasta on kuitenkin poikkeuksena määritelty asianomistajarikokset, jotka oikeudenkäynnistä rikosasiassa määrätyn lain (689/1997) 1 luvun 14 §:n perusteella edellyttävät asianomistajan rangaistusvaatimusta asiassa. Rikosasian esitutkinnassa asianomaisiksi ovat määriteltävissä esitutkintalain (805/2011) 2 luvun 5 §:n mukaan asianomistaja, rikoksesta epäilty ja muu henkilö, jonka

[63] OWASP Foundation Top 10, 2017, s. 6.
[64] Keski-Suomen KO R 20/118, Helsingin KO R 18/4485.
[65] Helsingin HO R 20/523, Pohjanmaan KO R 18/1062.
[66] Helenius, ym., 2021, s. 358.

oikeuksiin, etuihin tai velvollisuuksiin rikos ja sen selvittäminen voivat vaikuttaa. Asianomistaja on määriteltävissä loukatun oikeushyvän haltijaksi.

Rikoksen henkilöllinen aspekti on määriteltävissä monella tapaa. Rikoksen uhriksi ja asianomistajaksi on ensimmäisenä katsottavissa yksittäinen henkilö, jonka tietojärjestelmään tallennetut tiedot ovat rikoksen kohteena. Yksittäisen henkilön joutuessa tietojärjestelmässä tietomurron uhriksi, kyse voi olla vain yksittäiseen tietojärjestelmän osaan, kuten käyttäjätiliin tunkeutumisesta.

Toisena uhrina ja asianomistajana voidaan katsoa olevan koko tietojärjestelmää ylläpitävä taho, erityisesti tilanteissa, jos tietomurto kohdistuu kokonaiseen tietojärjestelmään yksittäisen käyttäjätilin tai käyttäjän tietojen sijasta. Tietojärjestelmän ylläpitäjän näkökulmasta on aiheellista painottaa luottamuksellisen viestinnän suojan lisäksi omaisuuden suojaa loukattavien oikeushyvien näkökulmasta. Tietojärjestelmän ylläpitäjä tai omistaja hallitsee tietojärjestelmää, johon tunkeudutaan ja kenen oikeuksia tilanteessa rikotaan.

Toisaalta viitaten esitutkintalain 2 luvun 5 §:ään, tietojärjestelmän omistaja tai ylläpitäjä on katsottavissa lähes aina vähintään asianosaiseksi tietomurtorikoksessa. Vaikka itse tietomurron toteuttamistavalla ei olisi merkitystä tietojärjestelmän ylläpitäjän kannalta, eikä hänen oikeutensa lähtökohtaisesti olisi loukattuna, jos tietomurto perustuu esimerkiksi käyttäjän heikkouteen itse tietojärjestelmän sijasta, tietojärjestelmän omistaja tai ylläpitäjä voi suurella todennäköisyydellä joutua osaksi esitutkintaa, jolloin rikoksen selvittämisellä on vaikutuksia kyseisen tahon oikeuksiin, etuihin ja velvollisuuksiin.

Erityisesti tapauksissa, joissa kokonainen tietojärjestelmä joutuu tietomurron kohteeksi, koko tietojärjestelmää ylläpitävän tahon lisäksi tulee huomioida, että kaikki tietojärjestelmään tietoja tallentaneet henkilöt ovat myös loukatun oikeushyvän haltijoita, toisin sanoen asianomistajia. Oikeuskirjallisuudessa on esitetty, että tilanteissa, joissa rikos kohdistuu suureen henkilöjoukkoon, yksittäisen henkilön etujen ei välttämättä katsota tulevan samalla tapaa loukatuksi.[67] Esitutkintalain 7 luvun 2 §:n mukaan asianomistajan kuulusteleminen voidaan jättää tämän omasta ilmoittautumisesta tapahtuvaksi, mikäli asian laatu edellyttää sitä asianomistajien suuren lukumäärän tai muun vastaavan syyn vuoksi. Tämän myötä yksittäisen asianomistajan tulee

[67] Fredman, ym., 2020, s. 173.

erityisesti suurien tietomurtojen tapauksessa olla itse oma-aloitteinen tietäessään omien oikeuksiensa tulleen loukatuiksi tietomurron yhteydessä.

Mikäli asianomistaja on vajaavaltainen, asianomistajarikoksissa oikeudenkäynnistä rikosasioissa annetun lain 1 luvun 4 §:n mukaan oikeus syyttämispyynnön tekemiseen on vajaavaltaisen edunvalvojalla tai muulla laillisella edustajalla. Mikäli vajaavaltaisuus johtuu alaikäisyydestä, oikeus on vajaavaltaisen huoltajalla. Lain 1 luvun 4 §:n 2 momentin mukaan, jos rikos kohdistuu omaisuuteen, jota henkilö saa yksin hallita tai oikeustointa, jonka tekemiseen vajaavaltaisella on kelpoisuus, syyteoikeus on lain tarkoittamalla vajaavaltaisella. Lisäksi on huomioitava lain 4 §:n 3 momentti, minkä mukaan, jos alaikäinen henkilö on täyttänyt 15 vuotta, hänellä on huoltajan ohella oikeus tehdä itsenäisesti syyttämispyyntö hänen henkilöönsä kohdistuneen rikoksen perusteella. Esitetyn perusteella vajaavaltaiseen kohdistuvassa tietomurtorikoksessa sekä huoltaja, laillinen edustaja että vajaavaltainen itse voivat käyttää puheoikeuttaan syyttämispyynnön tekemiseen. Osaltaan merkitystä on sillä, katsotaanko oikeudeton tunkeutuminen tietojärjestelmään henkilöön kohdistuvaksi rikokseksi, vai onko tietojärjestelmään tallennetuissa tiedoissa kyse henkilön hallitsemasta omaisuudesta.

Helsingin hovioikeuden tapauksessa R 20/523 yhtenä rikosnimikkeenä oli tietomurto nuorena henkilönä. Tapauksessa sekä tekijä että rikoksen uhri olivat lain edessä vajaavaltaisia. Tapauksessa ei otettu erikseen kantaa puhevallan käyttöä koskeviin kysymyksiin. Toisaalta oikeuskäsittelyn toisena käsiteltävänä rikosnimikkeenä oli tietomurron lisäksi henkilöön kohdistuva rikos, yksityiselämää loukkaava tiedon levittäminen, minkä perusteella alaikäinen henkilö on voinut käyttää puhevaltaa tapauksessa itsenäisesti. Oikeuskirjallisuudessa on katsottu, että jos useampi henkilö voi tehdä syyttämispyynnön vajaavaltaisen tapauksessa, asiassa riittää, kun yksi mahdollisista puhevallan käyttäjistä käyttää oikeuttaan.[68]

Tietomurto on määritelty lainsäädännössä asianomistajarikokseksi. Asianomistajarikoksessa on kyse rikoksesta, joka etenee rikosprosessiin vain rikoksen uhrin vaatimuksesta.[69] Yhtäältä asianomistajarikoksissa asianomistaja voi missä tahansa tutkinnan vaiheessa vaatia toimenpiteiden keskeyttämistä, jolloin asian käsittely keskeytyy.[70] Virallisen syytteen alaisessa rikoksessa syyttäjä nostaa syytteen asianomistajan tahdosta riippumatta ja tutkinta tulee saattaa

[68] Fredman, ym., 2020, s. 298.
[69] Nuutila, 1997, s. 8.
[70] Fredman, ym., 2020, s. 293.

loppuun asianomistajan vaatimuksista huolimatta. Tietomurtorikoksissa teko kohdistuu pääasiassa yksityiseen tahoon, jolloin viranomaiseen liitettävä julkinen kiinnostus selvittää rikos on vähäinen.[71] Oikeuskirjallisuudessa on katsottu, että nykyisin asianomistajarikokselta edellytetään nimenomaista syyteoikeutta ilmentävää lainkohtaa rikoslaissa, jotta rikoksen voidaan katsoa olevan asianomistajarikos.

Tietomurron ja törkeän tietomurron syyteoikeus on määritelty lähtökohtaisesti asianomistajalle rikoslain 38 luvun 10 §:n 2 momentissa. Sen mukaan tietomurto on yksi useammasta 38 luvussa mainitusta rikoksesta, missä syyttäjä ei saa nostaa syytettä, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi. Asianomistajarikoksia koskevasta pääsäännöstä poiketen syyttäjä voi nostaa asianomistajan sijaan syytteen tietomurrosta, jos tapauksessa on kyse erittäin tärkeästä yleisestä edusta tai rikoksentekijä on rikoksen tehdessään yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa. Lisäksi syyttäjä voi nostaa syytteen tietomurrosta ilman asianomistajan suostumusta, jos erittäin tärkeä yleinen etu vaatii sitä.

Käytännössä tietomurtorikoksen kannalta asianomistajarikoksen aseman määrittelee myös se, että syyttäjällä ei ole useinkaan käytännön mahdollisuutta saada tietoonsa tietomurtorikosta. Edellytyksenä on, että loukatun oikeushyvän haltija, kuten tietojärjestelmän omistaja tai tietomurron kohteeksi joutunut henkilö ilmoittaa rikoksesta esitutkintaviranomaiselle, käytännössä poliisille. Näin ollen ainoa mahdollinen tilanne, jossa syyte tietomurrosta voitaisiin nostaa omaaloitteisesti, olisi tilanne, jossa muun rikoksen tutkinnan yhteydessä löytyy aineistoa, joka on katsottavissa hankituksi tietomurtorikoksella. Esitutkintalain 3 luvun 4 §:n 2 momentin mukaan asianomistajarikoksen esitutkinta saadaan aloittaa, vaikka rangaistusvaatimusta ei ole tehty, jos asianomistaja ei ilmeisesti vielä tiedä rikoksesta, eikä tutkintaa voida siirtää vaarantamatta rikoksen selvittämistä. Tutkinta tulee kuitenkin lopettaa, jos asianomistaja ei vaadi rangaistusta saatuaan tiedon rikoksesta.

Tapaus Helsingin käräjäoikeus 26.07.2019, R 19/5139 osoittaa harvinaisen esimerkin tilanteesta, jossa asianomistaja ei ollut ilmoittanut tietomurtorikosta tutkittavaksi, vaan esitutkintaviranomainen oli aloittanut tietomurtorikoksen selvittämisen muun rikoksen tutkinnan yhteydessä. Tietomurtorikoksen arviointi eteni tapauksessa oikeudenkäyntiin saakka. Teonkuvauksen mukaan syytetyn hallusta löytyi muun tutkinnan yhteydessä USB-muistitikulle

[71] HE 94/1993 vp., s. 158.

tallennettuna yritykselle kuuluvia tietoja, joita yritettiin hyödyntää petosrikoksessa. Tapauksessa syntyi varteenotettava epäily tietomurrosta, koska asiassa ei ollut esitettävissä loogista selitystä sille, kuinka tiedot olivat päätyneet syytetyn haltuun. Asiassa oli selvitetty, että yrityksen tietojärjestelmästä oli kopioitu tiedostoja, mutta oikeudeton toiminta ei ollut yhdistettävissä varmuudella syytettyyn, vaikka tiedot olivatkin hänen hallussaan ja asiassa oli olemassa epäilys tekijästä. Syyte tietomurrosta hylättiin, koska asiassa oli olemassa varteenotettava epäilys ja mahdollisuus toisen henkilön suorittamasta oikeudettomasta tunkeutumisesta tietojärjestelmään, syytetyn sijasta.

2.5 Tietomurto lukuina

Suomessa poliisin tietoon ilmoitettujen tietomurtorikosten määrä on ollut 2010-luvulla nousussa. Tilastokeskuksen tietojen mukaan vuonna 2012 viranomaisen tietoon tuli 472 tietomurtotapausta, kun vuonna 2019 tietomurtotapauksia viranomaisen tietoon tuli 772 tapausta. Verrattaessa vuotta 2019 vuoteen 2021 viranomaisten tietoon tulleiden tietomurtorikosten määrä kaksinkertaistui kahdessa vuodessa. Osaltaan tietomurtorikoksiin liittyvä merkittävä kasvu on selitettävissä vuosikohtaisesti yksittäisellä merkittävällä rikoksella, jossa murtauduttaessa yksittäiseen tietojärjestelmään rikoksen uhreja on huomattava määrä. Vuonna 2020 Psykoterapiakeskus Vastaamo joutui tietomurron kohteeksi, jossa terapiakeskuksen tietojärjestelmään tunkeuduttiin, minkä seurauksena mahdollisesti 40 000 potilastietoa on joutunut rikollisiin käsiin.[72] Arvio potilastietojen määrästä perustuu Vastaamon potilastietokannan suuruuteen, joten toistaiseksi ei ole ollut täyttä varmuutta siitä, kuinka monta henkilöä on tosiasiallisesti tietomurtorikoksen asianomistajana.

kpl	472	575	337	343	401	414	485	778	1083	1475
Vuosi	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021

Viranomaisen tietoon tulleet rikokset rikosnimikkeellä tietomurto ja törkeä tietomurto vuosina 2012–2021[73]

[72] YLE: Vastaamon tietomurtotapaus.
[73] StatFin, Rikos- ja pakkokeinotilasto, Viranomaisen tietoon tulleet rikokset, Tietomurto 38:8 § ja Törkeä tietomurto 38:8a §, 2012–2021.

kpl	3	3	4	4	4	3	2	2	3
Vuosi	2012	2013	2014	2015	2016	2017	2018	2019	2020

Tuomioistuinten antamat ensimmäisen asteen rangaistukset rikosnimikkeellä tietomurto ja törkeä tietomurto vuosina 2012–2020[74]

Tietomurrosta ja törkeästä tietomurrosta oikeudessa syyksi luettujen tuomioiden määrä on huomattavasti alhaisempi, kuin tarkastellessa viranomaisen tietoon tulleiden tietomurtorikosten määrää. Asiassa vaikuttavina seikkoina voivat olla niin rikoksen selvittämiseen, rikosprosessiin kuin oikeudenkäyntiin liittyvät seikat. Esitutkintalain 3 luvun 3 §:n perusteella poliisin on toimitettava esitutkinta, kun on olemassa epäilys rikoksesta. Peruste suorittaa esitutkinta ei ole korkea, järkevästi perusteltu rikosilmoitus rikosedellytykset täyttävästä teosta on katsottu oikeuskirjallisuudessa riittäväksi indisioksi esitutkinnan suorittamiselle.[75] Pelkkä väite tapahtuneesta rikoksesta ei ole kuitenkaan riittävä epäilys.

Lisäksi asiassa on huomioitava, ettei esitutkintaviranomaisena toimiva poliisi ole sidottu rikosilmoituksessa ilmoitettuun rikosnimikkeeseen.[76] Mikäli toinen rikosnimike on soveltuvampi kuin tietomurto tai sen törkeä tekomuoto, poistuu rikos tietomurtoa koskevasta tilastosta ja siirtyy muun nimikkeen alle. Sisäministeriön raportin mukaan nykymuodossaan yleisesti tietoverkkorikollisuuden tilastointi on puutteellista, eikä siitä ole mahdollista tuottaa täysin luotettavia tilastoja.[77] Näin ollen pelkkä tuomittavan päärikoksen perusteella suoritettava selvitys ei anna täydellistä kuvaa tietomurtorikosten todellisesta esiintyvyydestä.

Tuomioiden vähäisyys suhteessa rikosepäilyihin on selitettävissä myös osaksi sillä, että rikoksen tekijää ei välttämättä saada selvitettyä tai tavoitettua. Mikäli rikoksen tekijän jäljet johtavat ulkomaille, tapauksen selvittäminen edellyttää kansainvälistä yhteistyötä toisen valtion viranomaisten kanssa, joka omalta osaltaan vaikeuttaa rikoksen selvittämistä tai voi tehdä sen ylitsepääsemättömäksi. Vaikka tekijä saataisiinkin selvitettyä, toinen valtio voi suhtautua

[74] StatFin, Rangaistukset rikoksittain, käräjäoikeudet ja hovioikeus ensimmäisenä oikeusasteena, Tietomurto 38:8 § ja Törkeä tietomurto 38:8a §, 2012–2020.
[75] Helenius, ym. 2021, s. 304.
[76] HE 222/2010 vp., s. 177.
[77] SM 14/2017, s. 23.

pidättäytyväisesti omalla lainkäyttöalueellaan olevan henkilön luovuttamiseen toiseen valtioon tuomittavaksi rikoksesta.

Mikäli rikoksesta epäilty on tavoitettu, tuomioistuinkäsittelyyn etenemisessä tulee huomioida myös itse rikoksen todennäköisyys ja kuinka pitävästi asia on voitu selvittää. Oikeudenkäynnistä rikosasioissa annetun lain 1 luvun 6 § edellyttää syytteen nostamiseen todennäköisiä syitä epäillyn syyllisyyden tueksi. Syytekynnyksen täyttymistä voidaan arvioida numeraalisena arvona 0–1 asteikolla. Asteikolla 0 tarkoittaa, että todennäköisyyttä ei ole olemassa ja määriteltäessä todennäköisyydeksi arvo 1, asiasta on täysi varmuus. Syytekynnyksen ylittyminen edellyttää numeraalisena arvona 0.75 todennäköisyyttä,[78] jolloin vaatimus on huomattavasti korkeampi kuin esitutkinnan vaatimus syystä epäillä rikosta.

Tuomio vastavuoroisesti edellyttää oikeudenkäymiskaaren (4/1734) 17 luvun 3 §:n perusteella, ettei rikoksesta syytetyn syyllisyydestä jää varteenotettavaa epäilyä. Varteenotettavan epäilyn puuttuminen tarkoittaa, että tilanteessa ei ole järkevää mahdollisuutta vaihtoehtoiselle tapahtumakululle. Tietomurrosta annettujen tuomioiden perusteella on mahdollista määritellä varteenotettavan epäilyn kriteerejä erityisesti teknisen todistusaineiston kannalta. Merkitystä on varmuudella. Kuinka pitävästi esimerkiksi päätelaitteen IP-osoite on yhdistettävissä epäiltyyn tekijään ja onko asiassa esitetty vaihtoehtoista tapahtumainkulkua, joka selittäisi tietojärjestelmään tallentuneen IP-osoitteen yhdistämisen kyseiseen henkilöön.

Helsingin hovioikeuden tuomiossa R 17/1769 syytetty oli tuomittu alemmassa oikeusasteessa tietomurrosta hänen käyttäessään asianomistajan tietokonetta. Teonkuvauksen mukaan henkilö oli kirjautunut luvatta asianomistajan sähköposti- ja sosiaalisen median tileille. Riidatonta asiassa oli se, että tietojärjestelmiin oli kirjauduttu luvatta syytetyn toimesta. Kysymys oli siitä, oliko luvaton kirjautuminen tapahtunut tietomurron tunnusmerkistön edellyttämällä tavalla ohittamalla turvajärjestely vai oliko asia selitettävissä toisella tapaa. Käräjäoikeus ei ollut pitänyt uskottavana selitystä tietokoneen automaattisesta kirjautumisesta asianomistajan käyttäjätileille, hovioikeuteen toimitetun asiantuntijalausunnon perusteella oikeus katsoi, että asiassa oli jäänyt varteenotettava epäily oikeudettomasta tunkeutumisesta tietojärjestelmiin. Syyte tietomurrosta hylättiin.

[78] Helenius, ym., 2021, s. 347.

3 Tietomurto, rikoslain yleiset opit ja rikosoikeudellinen seuraamusjärjestelmä

3.1 Tahallisuudesta

Oikeustieteen alakohtaiset yleiset opit voidaan käsittää perustyökaluiksi oikeudellisen tiedon järjestämiseen, käsittelyyn ja ongelmien tunnistamiseen.[79] Yleisten oppien avulla luodaan järjestys aihealueen hallintaa varten. Rikoslain yleisen osan luvut 1–10 voidaan katsoa lakiin kirjatuiksi rikoslain yleisiksi opeiksi. Luvut eivät kuitenkaan ole tyhjentävä esitys rikosoikeuden yleisistä opeista, vaan niitä arvioitaessa tulee tukeutua myös muuhun oikeustieteeseen, joka tukee kirjoitettua lainsäädäntöä. Rikosoikeudella on katsottu kuitenkin olevan oma tulkintaoppinsa, joka poikkeaa siviilioikeudesta, sekä julkisoikeudesta.[80] Muodollinen lainsäädäntö on etusijalla muihin oikeuslähteisiin nähden, mutta tulkinnassa tulee huomioida myös lainvalmisteluaineisto ja lainsäädäntöön liittyvä oikeuskäytäntö.

Rikoslain 3 luvun 6 §:n mukaan tekijä on aiheuttanut tunnusmerkistön mukaisen seurauksen tahallaan, jos hän on tarkoittanut aiheuttaa seurauksen tai pitänyt sen aiheutumista varmana tai hyvin todennäköisenä. Tahallisuuden määritelmä ulottuu myös tilanteisiin, joissa seurausta pidetään tarkoittamaansa seuraukseen varmasti liittyvänä. Säännöksestä on siis johdettavissa tahallisuuden jakautuminen tarkoitustahallisuuteen, varmuustahallisuuteen ja todennäköisyystahallisuuteen.[81]

Tahallisuuden alaraja on määritelty oikeuskirjallisuudessa rikoslain 3 luvun 6 §:n kolmannen kriteerin, todennäköisyystahallisuuden, mukaisesti. Tahallisuuden on katsottu täyttyvän, jos tekijä tekohetkellä mieltää todennäköiseksi sen, että hänen teostaan voi aiheutua rikoslaissa määritelty seuraamus.[82] Käytännössä henkilö on siis tehnyt ennen toimiin ryhtymistä todennäköisyysarvioinnin seurausten täyttymisestä ja pitää seurausta vähintään todennäköisenä eikä pelkästään mahdollisena. Seurauksen pitämistä todennäköisenä on esitetty tarkoittavan sitä, että tekijä pitää todennäköisempänä seurauksen täyttymistä kuin täyttymättä jättämistä, jolloin

[79] Saarenpää, 1997, s. 264.
[80] Frände, 2012, s. 46.
[81] Frände, 2012, s. 109.
[82] Hyttinen, 2016, s. 919.

seuraukselle on vähintään 50 % todennäköisyys.[83] Kokemussääntöjen perusteella on arvioitu, että mitä pidempään tekijällä kuluu aikaa teon toteuttamiseen ja mitä haastavampaa se on, sitä paremmin henkilön tulisi käsittää tekojensa tahallisuus, kun hänellä on aikaa arvioida tekoaan sen suorittamisen aikana.[84]

Tietomurrossa kyse olisi siis tilanteesta, jossa henkilö tietoisesti pyrkii tunkeutumaan tietojärjestelmään ja pitää tavoitteensa täyttymistä enemmän kuin sattumalta mahdollisena. Mitä pidempään tunkeutuminen tietojärjestelmään kestää, sitä suuremmalla todennäköisyydellä henkilön tulisi käsittää toimiensa tahallisuus. Tarkoitustahallisuudessa teon onnistuminen tai epäonnistuminen ei muuta tahallisuuden laatua, kunhan tarkoituksena on ollut nimenomaisesti tehdä kielletty teko ja sen eteen on toimittu tietoisesti.[85]

Varmuustahallisuudessa henkilö pitää rikoslain 3 luvun 6 §:n perusteella seurauksen aiheutumista varmana tai tarkoittamaansa seuraukseen varmasti liittyvänä. Seurausta ei varsinaisesti tavoitella, mutta tekijä ymmärtää tavoitteeseensa liittyvän myös kielletyn seurauksen aiheutumisen.[86] Seuraustodennäköisyyden arviointi tulee tehdä tekijän näkökulmasta, kuinka uskottavana itse tekijä pitää tunnusmerkistön täyttymistä.[87] Varmuustahallisuudessa kohteena oleva kielletty seuraus voi olla jonkin toisen teon edellytys, tai siihen liittyvä oheisseuraus. Oikeudeton tietojärjestelmään tunkeutuminen voi olla edellytyksenä esimerkiksi datavahingonteon toteutumiselle.

Tietomurtoa koskevan rikoslainsäädännön esitöissä tietomurtorikokselta on edellytetty tahallisuutta. Tunkeutujan on tiedettävä tunkeutuvansa tietojärjestelmään tai sen salattuun osaan oikeudettomasti.[88] Tunkeutumiselle ei kuitenkaan vaadittu erillistä tarkoitusta tai perustetta, vaan rangaistavuus haluttiin ulottaa myös ilman suoranaista hyötymistä tapahtuvaan tunkeutumiseen.

Tahallisuutta käsitellään rikoslain 4 luvussa myös vastuuvapautusperusteiden kautta. Rikoslain 4 luvun 1 § käsittelee tunnusmerkistöerehdystä. Jos tekijä tekohetkellä ei ole selvillä kaikista

[83] Nuotio, 2017, s. 977.
[84] Kalkela, ym., 2021, s. 238.
[85] Nuutila, 1997, s. 218.
[86] Nuutila, 1997, s. 219.
[87] Nuotio, 2017, s. 985.
[88] HE 94/1993 vp., s. 155.

tilanteeseen vaikuttavista asioista, joita tunnusmerkistön toteutuminen edellyttää tai tekijä erehtyy sellaisesta, teko ei ole katsottavissa tahalliseksi. Tekijän tulee jollain tapaa käsittää väärin tekoon liittyvät olosuhteet. Erehdys voi perustua esimerkiksi hyökkäyskohteesta erehtymiseen tai oman tekonsa kausaliteetin väärinymmärrykseen. Mikäli tunnusmerkistöerehdys tapahtuu kieltoerehdyksen kautta, kyseessä on rikoslain 4 luvun 2 §:n mukaan tilanne, jossa henkilö erehtyy tekonsa lainvastaisuudesta.[89] Oikeuskirjallisuudessa kieltoerehdyksen lainkohtaa on kommentoitu mahdollisena rikoksen anteeksiantoperusteena, jolla ei kuitenkaan ole vaikutusta varsinaiseen tahallisuuskysymykseen.[90]

Tietomurron kannalta mahdollinen tunnusmerkistöerehdys voisi olla hyökkäyksen kohteesta erehtyminen. Henkilön on tarkoitus suorittaa oikeudeton tunkeutuminen kohteeseen A, mutta hän kirjoittaa pitkähkön IP-osoitteen väärin ja aloittaakin tunkeutumisen kohteeseen B. Koska tietomurto tapahtuu internetin välityksellä, mahdolliset havainnointikeinot tietomurron kohteesta voivat jäädä vähäisemmiksi, kuin murtautuessa fyysisessä maailmassa tavoiteltuun kohteeseen. Erehdyksellä ei kuitenkaan ole merkitystä tahallisuuden ja sitä myötä rangaistavuuden kannalta. Tietomurtosäännös suojelee kaikkia järjestelmiä oikeudettomalta tunkeutumiselta, joten merkitystä tahallisuuden kannalta ei ole sillä, vaikka tekijä erehtyisi kohteesta. Merkitystä on tarkoituksella tunkeutua oikeudettomasti tietojärjestelmään.

Nykyisin erilaiset kaupalliset toimijat tarjoavat tietoturvapalveluita, joista yksi osa on asiakkaan auditointi eli selvitys ja arviointi siitä, täyttääkö organisaatio sille asetettuja vaatimuksia. Osaksi tietoturvallisuuden auditointia voi kuulua haavoittuvuustestaaminen, jossa tietoisesti koetetaan todellisin murtautumiskeinoin selvittää tietoturvallisuuden heikkouksia organisaatiossa. Näin ollen loukatun suostumuksen tarkastelu on merkityksellistä käsiteltäessä tietomurtoa rikoslain yleisten oppien kannalta. Loukatun suostumus voi poistaa rikoksen tunnusmerkistön mukaisuuden, jos se taho, kenellä on oikeus määrätä suojellusta oikeushyvästä, sallii oikeushyvää vastaan hyökkäämisen.[91] Vaihtoehtoisesti, mikäli suostumuksen puute ei ilmene teon rangaistavuuden edellytyksenä, loukatun suostumus voi poistaa teolta oikeudenvastaisuuden.[92] Tietomurtoa koskeva kriminalisointisäännös rikoslain 38 luvun 8 §:ssä määrittelee kriminalisoinnin

[89] Nuutila, 1997, s. 234.
[90] Nuutila, 1997, s. 234.
[91] Frände, 2012, s. 136.
[92] Hahto, 2004, s. 243.

oikeudettoman tunkeutumisen kautta, joten tietomurrossa suostumuksen arviointi tapahtuu tietomurrossa rikoksen tunnusmerkistön perusteella, täyttyykö oikeudeton tunkeutuminen.

Loukatun suostumusta ei ole kirjattu lainsäädäntöön, mutta oikeuskirjallisuudessa on katsottu itsemääräämisoikeuteen kuuluvan oikeus määrätä omista oikeushyvistä myös niitä loukkaavasti.[93] Loukatun suostumus rajoittuu yksilön pätevän suostumuksen vaikutuspiirissä oleviin tekoihin. Mikäli loukkauksen kohteena on jokin muu kuin yksityinen etu, toisin sanoen yhteinen etu tai valtion etu ja intressit, ei loukatun suostumus päde.[94]

Mikäli tietomurrossa tunkeutumisen kohde sallii omasta tahdostaan tunkeutumisen määrätyin ehdoin tietojärjestelmään ja lupa on tekijän tiedossa, ei kyseessä olisi tunnusmerkistön mukainen tietomurtoteko. Oikeuttamisperusteen hyväksyttävyyden kannalta tulee kuitenkin arvioida yksittäistapauksessa luvan sisältöä tarkemmin. Loukatun suostumuksen tulee olla oikeudellisesti pätevä. Oikeuskirjallisuudessa on katsottu suostumuksen pätevyyden edellyttävän, että suostumuksen antajalla tulee olla loukattavan oikeushyvän haltijuus ja määräysvalta. Tämän lisäksi suostumus tulee antaa vapaaehtoisesti ja suostumuksen antajan tulee olla yleisesti kelvollinen antamaan suostumus asiassa. Merkitystä on myös suostumuksen voimassaololla ja täsmällisyydellä.[95]

Mikäli lupa on annettu ainoastaan tietojärjestelmään tunkeutumiseen, se ei anna lupaa tarkastella järjestelmässä olevia tietoja, mikäli tunkeutuminen onnistuu. Taholle A annettu yksilöllinen lupa tunkeutua tietojärjestelmään ei toimi vastuuvapausperusteena tahon B tunkeutuessa tietojärjestelmään. Ajallisen ulottuvuuden kannalta laveasti yksilöity suostumus järjestelmään tunkeutumiseen ei voi olla avoin valtakirja toteuttaa järjestelmään tunkeutuminen pitkälle tulevaisuuteen ulottuvalla ajanjaksolla. Loukatun suostumus vahinkoseuraukseen voi vaikuttaa myös mahdollisen vahingonkorvausvastuun muodostumiseen. Mikäli suostumuksen perusteella teko on sallittu rikosoikeudellisessa mielessä, yleisesti myöskään vahingonkorvausvastuulle ei ole edellytyksiä.[96]

[93] Hahto, 2004, s. 239.
[94] Hahto, 2004, s. 240.
[95] Hahto, 2004, s. 247.
[96] Hahto, 2004, s. 281.

Ottaen huomioon edellä mainitut loukatun suostumukselle asetettavat kriteerit, joidenkin yritysten tietojärjestelmiinsä kohdistamat[97] ”Bug Bounty”-ohjelmat ovat haastavia tarkastellessa oikeuttamisperusteen hyväksyttävyyden kriteerien kestävyyttä. Bug Bountyssä perusajatuksena toimija haastaa hakkereita etsimään ohjelmavirheitä sekä haavoittuvuuksia toimijan järjestelmistä ja käytettävistä ohjelmistoista.[98] Mikäli ohjelmaan osallistunut taho raportoi toimijalle tietoturvallisuuteen liittyvistä seikoista, jotka eivät olleet toimijan tiedossa, asiasta maksetaan yleisesti palkkiota. Tietyissä määrin asiassa voidaan katsoa olevan kyse tietomurron yrityksestä. Toimijalla on loukatun suostumuksen perusteella oikeus määrätä hallinnassaan oleviin tietojärjestelmiin kohdistuvasta bug bountystä, mutta suostumuksen ajallinen ulottuvuus ja tekijöiden määrittely ovat haastavia. Yleisesti haaste on julkisesti saatavilla internetissä, lisäksi ohjelmat eivät ole ajallisesti rajoitettuja.

3.2 Yrityksestä

Rikoslain 5 luku käsittelee rikoksen yritystä ja osallisuutta. Rikoslain 5 luvun 1 §:n mukaan teko on edennyt rikoksen yritykseksi, kun tekijä on aloittanut rikoksen tekemisen ja saanut aikaan vaaran rikoksen täyttymisestä. Rikoksen jäädessä yritykseksi, teon tunnusmerkistö ei siis ole täyttynyt kokonaan. Tietomurron rikostunnusmerkistössä oikeudeton sisäänpääsy järjestelmään tai oikeudeton selon ottaminen järjestelmään tallennetusta tiedosta tai datasta jää saavuttamatta.

Rikoslain 6 luvun 8 §:n mukaan rikoksen jäädessä yritykseen, rangaistus määrätään lievennetyltä rangaistusasteikolta. Lievennetty rangaistusasteikko on pykälän 2 momentin mukaan enintään kolme neljännestä rikoksesta säädetyn vankeus- tai sakkorangaistuksen enimmäismäärästä ja vähintään säädetyn rangaistuslajin vähimmäisrangaistus. Jotta rikoksen yrityksestä voidaan rangaista, tulee yritys olla säädettynä nimenomaan rangaistavaksi. Sekä tietomurto että törkeä tietomurto on määrätty myös yrityksen osalta rangaistavaksi. Tietomurron yrityksen osalta lievennetyksi rangaistusasteikoksi muodostuu vähintään sakkorangaistus ja enintään puolitoista vuotta vankeutta. Törkeän tietomurron yrityksestä voitaisiin siis tuomita vähintään sakkorangaistus ja enintään kaksi vuotta ja kolme kuukautta vankeutta.

[97] Kyberturvallisuuskeskus, ”Bug Bounty -ohjelmien avulla tietoturvaongelmat voi kääntää PR-voitoiksi”.
[98] Wylie, ym., 2021, s. 123.

Oikeuskirjallisuudessa rikoksen yrityksen rangaistavuuteen on katsottu riittävän todennäköisyystahallisuus.[99] Tämä ilmenee myös rikoslain 3 luvun 6 §:stä, joka määrittelee tahallisuuden. Tällöin tekijä pitää tunnusmerkistön mukaisen seurauksen aiheutumista tekohetkellä varsin todennäköisenä.

Rajattaessa rikoksen yritystä ajallisesti, kyse on valmistelun ja tunnusmerkistön mukaisen toiminnan päättymisen välisestä ajanjaksosta. Rikoksen valmistelu on rangaistavaa vain, jos se on erikseen määrätty rikoslaissa rangaistavaksi.[100] Rikoslaissa rangaistavaksi määrättyjä valmistelutoimenpiteitä ovat esimerkiksi rikoslain 11 luvun 2 §:n mukainen joukkotuhonnan valmistelu ja 16 luvun 5 §:n yleisen järjestyksen aseellisen rikkomisen valmistelu. Kyse on siis rikoslain sisällä hyvin vakavista rikoksista, eikä tietomurron valmistelua ole kriminalisoitu rikoslaissa. Tietomurron yrityksen rangaistavuuden arvioimiseksi, on kuitenkin aiheellista arvioida myös tietomurron valmistelun päättymisen ja rikoksen yrityksen alkamisen ajankohtaa.

Pääsäännön mukaan rikos on niin kauan yritys, kunnes rikoksen tunnusmerkistö on täyttynyt. Tietomurron tapauksessa tunnusmerkistö täyttyy luvattomalla pääsyllä tietojärjestelmään. Rangaistava yritys on pääsääntöisesti käsillä silloin, kun yrityksen alkupiste on saavutettu, eli rikoksen yritys on alkanut.[101] Korkein oikeus on arvioinut tietomurron yritystä tapauksessa KKO 2003:36. Tapauksessa tuomioistuimen arvioitavana oli kysymys tietomurron yrityksen tunnusmerkistön täyttymisestä ja siihen liittyvän vahingonkorvauksen sovittelemisesta. Alemmissa oikeusasteissa käräjäoikeus oli hylännyt syytteen tietomurron yrityksestä, hovioikeus oli tuominnut syytetyn tietomurron yrityksestä, perustellen kantansa siihen, että syytetyllä ei ollut muuta perustetta toimintaansa, kuin tietomurron yritys.

Tapauksessa syytetty oli teonkuvauksen mukaan syyllistynyt tietomurron yritykseen skannatessaan osuuskunnan omistaman tietojärjestelmän tietoliikenneportteja. Porttiskannaus tarkoittaa tietoverkossa tapahtuvaa, tietokoneessa avoinna olevien digitaalisten tietoliikenneporttien tutkimista ja etsimistä lähettämällä niihin ohjelmallisesti tietoa ja tulkitsemalla annettuja vastauksia.[102] Yksinkertaistettuna, porttiskannausta voi verrata fyysisessä maailmassa toimintaan,

[99] Nuutila, 1995, s. 149.
[100] Nuutila, 1995, s. 157.
[101] Frände, 2012, s. 224.
[102] VAHTI 4/2008, s. 76.

jossa naapurustossa liikkuva murtovaras kokeilee, ovatko talojen ovet lukittuina vai avoinna, minkä perusteella murtovaras tekee murtautumispäätöksen.

Korkein oikeus katsoi hovioikeudessa syytetyn toiminnan selvitetyksi. Syytetty oli käyttänyt porttiskannausohjelmaa. Tapauksessa syytetty kiisti syyllistyneensä tietomurron yritykseen. Syytetty katsoi toiminnallaan pyrkineensä toteamaan yksittäisessä tietojärjestelmässä olevat avoimet palvelut, eikä tavoitelleensa tietojärjestelmän luvatonta käyttöä. Toisaalta avointen palvelujen toteamisella ei ole merkitystä. Oikeudeton pääsy tietojärjestelmään ei vaadi välttämättä turvajärjestelyn murtamista, sillä keskiössä on pääsy tietojärjestelmään ilman lupaa. Avoimetkaan palvelut eivät ole välttämättä tarkoitettu jokaisen käytettäväksi. Korkein oikeus piti hovioikeuden tuomion lopputuloksen voimassa.

Arvioitaessa tapausta ensimmäisenä tietoteknisestä näkökulmasta, pelkkä porttiskannaus ei sinänsä mahdollista luvatonta pääsyä tietojärjestelmään. Skannaus on enemmänkin osasuoritus tietomurtorikoksessa. Ohjelmallinen porttiskannaus palauttaa positiivisen tai negatiivisen vastauksen, jonka perusteella asiaan perehtynyt henkilö voi jatkaa järjestelmään tunkeutumista. Skannauksen jälkeen käsillä on vasta tieto, mitä kautta tietojärjestelmään voidaan ottaa yhteyttä toisella sovelluksella. Mikäli porttiskannaus olisi tapauksessa onnistunut, syytetty olisi voinut löytää skannauksen tuloksen perusteella keinon päästä tietojärjestelmään oikeudetta. Tässä suhteessa kyse on nimenomaisesti tietomurron yrityksestä. Korkein oikeus lausui porttiskannausohjelmasta, ettei sellaisen käyttö ole tarpeellista syytetyn kuvailemaan sallittuun toimintaan, avoimien palvelujen toteamiseen. Avointen palvelujen toteaminen voi tapahtua ilman porttiskannausta suoralla yhteydenotolla tietojärjestelmään.

Tapauksessa annettiin painoarvoa myös syytetyn tietotekniselle asiantuntemukselle, jonka myötä syytetyn olisi tullut käsittää vaaran aiheutuminen ja mahdollisuus aiheuttaa suurtakin vahinkoa omalla toiminnallaan. Korkein oikeus ei kuitenkaan lausunut ratkaisussaan kuinka suuri todennäköisyys tietojärjestelmään pääsemiselle oli tekohetkellä, pitäessään hovioikeuden tuomion voimassa.

Korkeimman oikeuden tapauksen perusteella tietomurron yrityksestä luopuminen voi olla haastavaa. Rikoslain 5 luvun 2 §:n mukaan yrityksestä ei rangaista, jos tekijä on vapaaehtoisesti luopunut rikoksen täyttämisestä tai muuten estänyt tunnusmerkistössä tarkoitetun seurauksen syntymisen. Toisaalta hallituksen esityksessä tieto- ja viestintärikoksista, rangaistavaksi

tietomurron yritykseksi on määritelty jo yritys selvittää järjestelmän suojana oleva käyttäjätunnus tai muu vastaava järjestely, jos teon tarkoituksena on suorittaa oikeudeton tunkeutuminen tietojärjestelmään.[103] Esitys tukeutuu lokimerkintöjen tärkeyteen rajanvedossa, viitaten teknisiin keinoihin erottaa satunnaiset pyrkimykset päästä järjestelmään sisälle järjestelmällisestä murtautumisesta. Porttiskannaus voi yleisesti katsoen olla ensimmäisiä askeleita tietomurron suorittamisessa. Näin ollen yrityksen rangaistavuuden kynnys on viritetty hyvin matalalle.

Yrityksestä luopuminen poistaa sellaisenaan rangaistusvastuun ainoastaan tilanteissa, että tekijä luopuu vapaaehtoisesti yrityksestä.[104] Rikoslain 5 luvun 2 §:n 4 momentin mukaan, jos yritys sisältää jo jonkin toisen rikoksen, tekijä ei vapaudu rangaistusvastuusta kokonaisuudessaan. Esitetyn perusteella tietojärjestelmän suojaustason vahvuudellakaan ei ole merkitystä teon rangaistavuuden kannalta. Viime kädessä rikoksen yrityksestä luopumisen tulee tapahtua vapaaehtoisesti, eikä ulkoisten seikkojen johdosta. Tapauksessa KKO 2002:112 rikoksentekijä oli keskeyttänyt törkeän varkauden yrityksen hänen nähdessään vartiointiliikkeen auton. Korkein oikeus katsoi, että tässä tapauksessa yrityksestä ei ollut luovuttu vapaaehtoisesti, vaan ulkoinen este oli vaikuttanut teosta luopumiseen. Korkein oikeus ei muuttanut hovioikeuden tuomion lopputulosta. Tekijä tuomittiin rangaistukseen törkeän varkauden yrityksestä.

Digitaalisen maailman kannalta ulkoinen este voisi perustua esimerkiksi internet-yhteyden palveluntarjoajan tiedusteluun tai huomautukseen internet-yhteydessä seuratusta liikenteestä. Sähköisen viestinnän palveluista annetun lain (917/2014) 143 §:n perusteella viestinnän välittäjällä, tässä tapauksessa palveluntarjoajalla, on oikeus käsitellä välitystietoja väärinkäytösten havaitsemiseksi maksullisessa palvelussa. Ulkoinen este voisi tietomurtorikoksen tilanteessa olla myös käsillä, jos tunkeutumisen kohteena oleva tietojärjestelmä lopettaa toimintansa kesken yrityksen. Vaikka tietomurron edellytyksenä onkin toiminnassa oleva tietojärjestelmä, kokemusperusteisesti ei ole tavatonta, että tietojärjestelmä jumittuu, erityisesti jos tietojärjestelmässä tehdään toimia, jotka eivät kuulu sen normaaliin käyttöön.

On myös mahdollista arvioida kelvotonta tietomurron yritystä. Kelvottomassa yrityksessä rikoksella tavoitellun seurauksen syntyminen ei ole mahdollista.[105] Tietomurrossa kelvottomaksi yritykseksi voidaan katsoa tilanne, jossa luvaton pääsy tietojärjestelmään ei ole mahdollista.

[103] HE 94/1993 vp., s. 156.
[104] Nuutila, 1995, s. 156.
[105] Nuutila, 1995, s. 153

Kelvotonta yritystä voi arvioida täytäntöönpanovaatimuksen ja vaaravaatimuksen kautta.[106] Täytäntöönpanovaatimuksessa tekijän edellytetään aloittavan vähintään yhden rikoksen tunnusmerkistöön kuuluvan toimen. Vaaravaatimus on rikoslain 5 luvun 1 §:n 2 momentissa, jonka mukaan rikoksen yritykseltä edellytetään vaaraa rikoksen täyttymisestä. Vaaravaatimuksessa toimelta vaaditaan tiettyä todennäköisyyttä ja mahdollisuutta tapahtua. Oikeuskirjallisuudessa asian on katsottu tarkoittavan, ettei satunnaiset vaaran aiheutumisen estävät syyt tee yrityksestä kelvotonta.[107]

Tietomurrossa satunnainen estävä syy voisi perustua esimerkiksi rikoksentekijän internet-yhteyden toimimattomuuteen tai käytettävien tietomurtotekniikoiden yhteensopimattomuuteen kohteena olevan järjestelmän kanssa. Lainvalmistelutöissä on määritelty, ettei kyse ole tietomurron yrityksestä, kun henkilö erehdyksissä tavoittelee kirjautumista tietojärjestelmään, mihin hänellä ei ole käyttöoikeutta.[108]

Korkein oikeus on käsitellyt tapauksessa KKO 2021:64 rikoksen yrityksen vaaravaatimuksen todennäköisyyden edellytyksiä. Korkein oikeus katsoi rikoksen täyttymisen vaaran jääneen törkeän pahoinpitelyn yrityksessä asiassa esitetty selvitys huomioiden epätodennäköiseksi, jolloin vaaravaatimus ja syyllisyys rangaistavaan yritykseen eivät olleet täyttyneet. Korkein oikeus katsoi, että mikäli vaaravaatimus jää teoreettiselle tasolle, ei kyse ole rikoslain 5 luvun 1 §:n 2 momentin mukaisesta rikoksen täyttymisen vaarasta. Korkein oikeus katsoi tapauksessa, ettei vahingonkorvausvaatimuksellekaan ollut perusteita, koska syyte hylättiin vaaravaatimuksen vuoksi. Tapauksesta on katsottavissa, että vaaravaatimuksen arviointi tulee kuitenkin suorittaa tapauskohtaisesti, eikä se ole täysin arvioitavissa etukäteen.

Tiivistettynä, rangaistavan tietomurron yrityksen kynnys on oikeuskäytännön ja lainvalmistelumateriaalin perusteella asetettu hyvin alhaiseksi. Esitetyn perusteella tekijän tarkoitusperillä ei ole merkitystä rangaistavuuden kannalta, vaan rangaistavaa on jo pelkkä kokeilumielessä tapahtuva oikeudettoman käytön tavoittelu. Oikeudettoman käytön tavoittelulta, toisin sanoen rikoksen yritykseltä edellytetään kuitenkin täytäntöönpanovaatimusta ja vaaravaatimusta. Vaaravaatimuksen tulee täyttyä muutenkin kuin teoreettisessa mielessä.

[106] Frände, 2012, s. 228.
[107] Tapani, ym., 2019, s. 474.
[108] HE 94/1993 vp., s. 156.

3.3 Osallisuudesta rikokseen

Rikoslain erityisen osan rikostunnusmerkistöt ovat lähtökohtaisesti kirjoitettuna muotoon, jossa rikokseen syyllistyy yksi tekijä. Käytännössä asia ei kutenkaan ole yksiselitteinen, vaan yksittäiseen rikokseen voidaan tarvita tosiasiallisesti useamman henkilön yhteispanos. Suomen rikoslainsäädännössä yhteen tekoon voidaan katsoa syyllistyvän useampi henkilö, perustuen joko tekijäkumppanuuteen tai olemalla osa järjestäytyneen rikollisryhmän toimintaa. Tekijäkumppanuus perustuu rikoksen toteuttamiseen yhdessä. Rikoslain 5 luvun 3 § määrittelee tekijäkumppanuuden siten, että jos kaksi tai useampi tekee yhdessä tahallisen rikoksen, kumpaakin rangaistaan rikoksen tekijänä. Rikoksesta tuomitaan kaikki tekijät, vaikka rikos olisi onnistunut vain tekijöiden suorittaman yhteistoiminnan seurauksena.[109]

Mikäli tekijän toiminta on katsottavissa kokonaisuuteen nähden vähäiseksi, henkilö voi syyllistyä avunantoon rikoksessa.[110] Yllytyksessä on kyse rikoslain 5 luvun 5 § perusteella tilanteesta, jossa yllyttäjä taivuttaa toisen tahalliseen rikokseen tai sen yritykseen. Tietomurron ja muiden tieto- ja viestintärikosten erityispiirteenä voi katsoa olevan, että rikokseen osallisuus ei vaadi välttämättä fyysistä yhdessäoloa, digitaalinen tapahtumaympäristö huomioiden. Rikos on mahdollista suunnitella ja toteuttaa tietoverkon välityksellä, tekijät voivat tosiasiallisesti tietää vain toistensa nimimerkin.

Rikoskumppanuus voi tekijäkumppanuudessa perustua yhdistettyyn rikokseen, missä rikoksen täyttämisen edellytyksenä on eri osatekojen täyttyminen. Vaihtoehtoisesti rikoskumppanuuteen liittyvä vastuu perustuu muulla tavalla rikokseen osallistumiseen.[111] Esimerkkinä muulla tavalla rikokseen osallistumisesta, tapauksessa KKO 1974 -II-82 henkilö tuomittiin törkeästä varkaudesta tekijänä, hänen osallistuessaan varkauteen sekä suunnittelijana että pakoauton kuljettajana.

Tietomurrossa tekijät voisivat jakaa erillisten osatekojen täyttyminen voisi tapahtua siten, että ensimmäinen tekijä suorittaa valmistelevat toimenpiteet ja luo yhteyden tunkeutumisen kohteena olevaan tietojärjestelmään, minkä jälkeen toinen tekijä suorittaa itse tietojärjestelmään

[109] Tapani, ym., 2019, s. 511.
[110] Nuutila, 1997, s. 340.
[111] Frände, 2012, s. 243.

tunkeutumisen. Molemmat osasuoritukset ovat olennaisia rikoksen täyttymisen kannalta, eikä pelkästään yhden henkilön panos riitä tietomurron toteuttamiseen.

Rikoslain 5 luvun 6 §:n mukaan avunannosta voidaan tuomita se, joka ennen rikosta tai sen aikana neuvoin, toimin tai muilla tavoin auttaa tahallisesti toista tahallisen rikoksen tai sen rangaistavan yrityksen tekemisessä. Avunannosta tuomitaan lievennetyltä rangaistusasteikolta. Rikoslain 6 luvun 8 §:n perusteella syyllistymisestä avunantoon tuomitaan enintään kolme neljännestä rikoksesta säädetystä vankeusrangaistuksen tai sakkojen enimmäismäärästä. Avunannolle ei ole määritelty laadullisia kriteereitä, joten teoriassa mikä tahansa arkinenkin teko voisi käydä avunannosta, mikäli se edistää rikoksen tekemistä ja toteutumista. Näin ollen avunantoa voidaan lähtökohtaisesti arvioida matalalla kynnyksellä.[112] Aivan mikä tahansa toiminta ei kuitenkaan ole katsottavissa avunannoksi rikokseen, vaan Suomen rikosoikeudessa avunannon rangaistavuuden perustana on kausaliteetti. Avunantajan tulee tahallisella toiminnallaan myötävaikuttaa päätekijän rikolliseen toimintaan.[113]

Avunannon laveasta määrittelystä huolimatta myös myötävaikuttamiselle on rajansa, eikä mikä tahansa tekijän päämääriä edistävä toimi voi olla katsottavissa avunannoksi rikokseen. Avunantajalta vaaditaan tahallisuutta omien toimiensa suhteen, toisin sanoen hänen tulee olla tietoinen avun pyytäjän rikollisista tarkoitusperistä. Näin ollen tietomurtorikoksissa esimerkiksi henkilö, joka myy päätekijälle tietokoneen, ei syyllisty lähtökohtaisesti avunantoon. Tilannetta tulisi arvioida uudelleen, mikäli tietokoneen myyjä on selkeästi tietoinen ostajan tarkoituksesta suorittaa tietomurto hänen myymällään tietokoneella.

Lainvalmisteluaineistossa tietoverkkorikoksissa hyödynnettävä ohjeistus on nähty vähemmän vaaraa aiheuttavaksi toiminnaksi, kuin valmiin tietomurrossa hyödynnettävän ohjelman levittäminen.[114] Tietomurto-ohjeen valmistamista ei ole nähty rangaistavana toimintana. Osaltaan näkemykselle voidaan hakea perustetta siitä, ettei ohjeen levittäminen ole yhtä haitallista, kuin valmiin murtotyökalun tai tietokoneviruksen levittäminen. Ohjetta tulee osata hyödyntää, jotta siitä on apua tietomurron toteuttamisessa.

[112] Tapani, ym., 2019, s. 533.
[113] Luoto, 2018, s. 42.
[114] HE 153/2006 vp., s. 59.

Ohjeistaen tehtävässä avunannossa voidaan kuitenkin katsoa olevan merkitystä henkilön tietoisuudella. Mikäli henkilö tarjoaa ohjeistusta tarkoituksenaan mahdollistaa oikeudeton tunkeutuminen tietojärjestelmään, eli tietomurto ja hän on tietoinen esimerkiksi ohjeistamalla toteutettavan tietomurron kohteesta, voisi henkilön rangaistusvastuu tulla tosiasiallisesti arvioitavaksi myös tuomioistuimessa. Avunantajan oman rangaistusvastuun arviointi avunannon tekohetkellä on haastavaa. Avunantaja joutuu arvioimaan oman tekonsa toteutumishetkellä tulevaisuutta, mitä päätekijä tulee kokonaisuudessaan tekemään.[115] Mikäli päätekijä päättääkin tehdä muuta, kuin mitä avunantaja on mieltänyt tapahtuvaksi, avunannon arviointi on vaikeampaa. Avunannosta tuomitseminen tuomioistuimessa tietomurtorikosten kannalta voi kuitenkin olla muutenkin haastavaa, ottaen huomioon sen, ettei syyllisyydestä tule jäädä tässäkään tilanteessa järkevää epäilyä.

Tuomioistuimien ratkaisujen perusteella voidaan esittää kysymys, milloin esimerkiksi sosiaalisen median tilille murtautumisessa voisi syyllistyä avunantoon. Ratkaisukäytännön ja yllä esitetyn perusteella on esitettävissä, että henkilöiden yhteistuumin suorittama salasanan arvaaminen olisi katsottavissa vähintäänkin avunannoksi. Samanaikaisesti on myös arvioitava rikoskumppanuuden mahdollisuutta, jossa merkitystä on yhteisymmärryksessä toimimisella. Avunantajan ja rikoskumppanin on oltava tietoinen oman tekemisensä merkityksestä osana rikoksen toteutumista, missä toinen tietää käyttäjätunnuksen tai tarjoaa toiselle osapuolelle salasanaa. Tapauksen arvioinnissa tulee huomioida myös ajallinen yhteys. Tilanteessa, missä itse oikeudeton tunkeutuminen on jo tapahtunut yhden henkilön toimesta ja vasta tietojärjestelmän sisältöä tarkastellaan yhdessä, kyseeseen voivat tulla avunannon sijaan jo muut rikosnimikkeet, kuin itse tietomurto ja tietojärjestelmään tunkeutuminen.

Arvioitaessa yllytysvastuuta rikosoikeudessa, on todettavissa, että yllyttäminen on rikosoikeudellisessa mielessä moitittavuudeltaan verrattavissa tekijävastuuseen.[116] Rangaistusta mitattaessa rikoksesta voidaan siis antaa yllyttäjälle sama tuomio, kuin tekijälle. Yllytys antaa tekijälle syyn tehdä teko, ottamatta kantaa siihen, haastaako tietomurtorikoksessa yllyttäjä tekijän tietotekniset taidot vai herättääkö yllyttäjä tekijän kiinnostuksen kohteena olevan tietojärjestelmän tietoihin. Tilanne on erilainen verrattaessa avunantoon, jossa päätekijä on suunnitellut teon itse ja avunantaja vain myötävaikuttaa sen toteutumiseen suunnitelman mukaisesti.[117]

[115] Luoto, 2018, s. 129.
[116] Tapani, ym., 2019, s. 512.
[117] Luoto, 2018, s. 128.

3.4 Rangaistuksen mittaamisesta

Määritettäessä rangaistusta, suhteellisuusperiaate edellyttää eri törkeysasteen rikoksista annettavien rangaistusten eroavan oikeasuhtaisella tavalla toisistaan ja että rangaistus on rikoslain 6 luvun 4 §:n vaatimalla tavalla oikeudenmukainen suhteessa rikoksen vahingollisuuteen, vaarallisuuteen ja tekijän syyllisyyteen.[118] Rikoslain 38 luvun 8 §:n mukaan tietomurrosta annettavan rangaistuksen asteikko on vähintään sakkorangaistus ja enintään kaksi vuotta vankeutta. Törkeän tietomurron rangaistusasteikko on sakkorangaistuksesta enintään kolmeen vuoteen vankeutta. Rangaistuksen mittaamista koskevat yleiset säännökset ovat rikoslain 6 luvussa. Ainoana poikkeuksena tulee huomioida rikoslain 2 luvun 1 §, joka määrittelee päiväsakkojen vähimmäismääräksi yhden ja enimmäismääräksi 120. Yhteisen rangaistuksen määräämisestä määrätään rikoslain 7 luvussa.

Määrättäessä rangaistusta, tuomioistuimen tulee perinteisesti ensimmäisenä tehdä valinta sovellettavan rangaistuslajin suhteen. Tietomurron tapauksessa valinta tapahtuu sakkojen ja vankeusrangaistuksen välillä. Vankeusrangaistuksen osalta tulee huomioida mahdollisuus määrätä sekä ehdoton, että ehdollinen vankeusrangaistus. Rikoslain 6 luvun 9 §:n perusteella enintään kahden vuoden vankeusrangaistus voidaan määrätä ehdollisena vankeusrangaistuksena, ellei rikoksen vakavuus, tekijän syyllisyys tai aikaisempi rikollisuus edellytä ehdotonta vankeutta. Rangaistuksen mittaamista koskevan rikoslain yleisiä oppeja koskevan uudistuksen hallituksen esityksessä todetaan, että määrittäessä rangaistusta tulee ensin määrittää rangaistuslaji, jonka jälkeen hienosäädetään rangaistuksen määrää.[119]

Oikeustieteen tohtori *Heikki Kemppinen* on esittänyt väitöskirjassaan ”Rangaistuksen määräämisen perusteleminen” uuden näkemyksen, jonka mukaan rangaistuksen määrääminen tulee aloittaa vahvistamalla rangaistusasteikko. Ensimmäinen kysymys on, tuomitaanko rangaistus normaalilta vai lievennetyltä asteikolta.[120] Rangaistuslajin valinta tapahtuu vasta, kun rangaistusasteikko ja mahdollinen rangaistuksen tuomitsematta jättäminen on selvitetty.[121]

[118] Lappi-Seppälä, 2000, s. 312.
[119] HE 44/2002 vp., s. 169.
[120] Kemppinen, 2021, s. 12.
[121] Kemppinen, 2021, s. 12.

Aikaisempi rikollisuus on yksi rikoslain 6 luvun 5 §:ssä määrittelemistä rangaistuksen koventamisperusteista. Muita rangaistuksen koventamisperusteita ovat rikoksen toiminnan suunnitelmallisuus, rikoksen tekeminen osana järjestäytyneen rikollisryhmän toimintaa, tekeminen palkkiota vastaan ja rikoksen tekemisen perustuminen erityisiin tuomittaviin vaikuttimiin, kuten rotuun, ihonväriin tai vakaumukseen. Arvioitaessa suunnitelmallisuutta mahdollisena rangaistuksen koventamisperusteena, tulee huomioida törkeän tietomurron tunnusmerkistö rikoslain 37 luvun 8 a §:ssä. Jos tietomurto tehdään erityisen suunnitelmallisesti ja on kokonaisuutena arvostellen törkeä, tietomurto voidaan tuomita törkeänä tietomurtona. Suunnitelmallisuus on huomioituna jo rikoslaissa, mikä kaventaa suunnitelmallisuuden käyttöä pelkästään perussäännöksen perusteella annettavan rangaistavuuden mittaamisessa. Lisäksi tietomurtorikoksen menestyksekäs toteuttaminen vaatii lähtökohtaisesti suunnitelmallisuutta, mikä tulee ottaa huomioon asetettaessa suunnitelmallisuuden kriteereitä. Oikeuskirjallisuudessa on esitetty, että rikoksen suunnitelmallisuuden käyttöä yhtäaikaisesti sekä törkeän tekomuodon valintaperusteena että rangaistuksen koventamisperusteena tulee välttää.[122] Suunnitelmallisuuden käyttöön rangaistuksen koventamisperusteena tulee suhtautua kriittisesti tuomittaessa tietomurrosta.

Rangaistuksen lieventämisperusteet ovat määriteltyinä rikoslain 6 luvun 6 §:ssä. Lieventämisperusteita ovat rikoksen tekemiseen vaikuttanut huomattava painostus, uhka tai muun kaltainen seikka, rikokseen johtanut voimakas inhimillinen myötätunto, poikkeuksellinen tai äkkiarvaamaton houkutus, asianomistajan huomattava myötävaikutus tai vastaava seikka, joka on heikentänyt tekijän kykyä noudattaa lakia tai jos tekijän ja asianomistajan välillä on saavutettu sovinto, tai tekijä on muuten pyrkinyt vaikuttamaan rikoksen vaikutuksiin tai sen selvittämiseen. Lisäksi rangaistusta voidaan lieventää yleisten rangaistuksen vähentämisperusteiden[123], kuten alaikäisyyden tai alentuneen syyntakeisuuden perusteella. Rikosten vaikutusten estämisen tai poistamisen osalta oikeuskirjallisuudessa on esitetty, että lieventämisperusteen käyttö on sidoksissa tekijän vapaaehtoisuuteen ja aikaan. Mitä myöhäisemmässä vaiheessa rikoksen seuraamuksiin pyritään vaikuttamaan, sen vähäisempi on mahdollisuus tuomita asiassa lievennetyltä asteikolta.[124]

Toisaalta yhteistyöhalukkuus rikoksen selvittämisessä myös kiinnijäämisen jälkeen voi vaikuttaa rikoksesta annettavaan rangaistukseen. Tietomurtorikoksissa kyse voi olla esimerkiksi

[122] Lappi-Seppälä, 2000, s. 342.
[123] Frände, 2012, s. 384.
[124] Lappi-Seppälä, 2000, s. 358.

tekijän myötävaikutuksesta esitutkintaan osoittamalla käytetyt tietomurtotekniikat ja turvallisuuspuutteet kohteena olleessa järjestelmässä. Tekijä voi myös pelkän esitutkinnan selvittämisen myötävaikuttamisen sijasta tunnustaa teon, joka voidaan katsoa lievissä rikoksissa riittäväksi näytöksi rikoksen selvittämisen kannalta.[125] Tunnustuksen ajankohdalla on merkitystä, mikäli tunnustaminen ajoittuu niin, että siitä ei ole enää hyötyä rikoksen selvittämisessä, huojennus voi jäädä vähäiseksi tai sitä ei ole ollenkaan.[126] Tutkimusaineistossa Helsingin käräjäoikeuden tapauksessa R 18/4485 ja Keski-Suomen käräjäoikeuden tapauksessa R 20/118 tietomurrot olivat myönnetty oikeuskäsittelyissä oikeaksi, jolloin ajankohdalla ei enää ollut merkitystä rikoksen selvittämisen kannalta, eikä myöntämisellä näin ollut vaikutusta rangaistusseuraamukseen.

Rikoslain 6 luvun 8 § määrittelee tilanteet, joiden perusteella teon rangaistusasteikkoa voidaan lieventää. Rangaistusasteikkoa voidaan lieventää, mikäli rikos on tehty alle 18-vuotiaana, teko on jäänyt yritykseen, tuomittava on syyllistynyt avunantoon tai muuten selkeästi vähempään osallisuuteen. Lisäksi lieventämistä voidaan harkita tilanteissa, joissa on vastuuvapautusperusteiden kaltaisia olosuhteita. Tuomittaessa lievennetyltä rangaistusasteikolta, henkilölle voidaan tuomita enintään kolme neljännestä enimmäisrangaistuksesta. Rangaistusasteikon lieventämisen jälkeen tulee arvioida rangaistuksen koventamis-, lieventämis- ja kohtuullistamisperusteet uuden rangaistusasteikon sisällä. Rikoslain 6 luvun 8 §:n 2 momentin mukaan, mikäli rikos tehdään alle 18-vuotiaana, tekijälle saa tuomita enintään kolme neljännestä vankeus- tai sakkorangaistuksen enimmäismäärästä. Ottaen huomion rikosoikeudellisen vastuun alaikärajan 15-vuotta, enimmäisrangaistuksen tuomitseminen kolme neljännestä mallin mukaisesti on mahdollista tuomittaessa tekijä 15–17-vuotiaana tehdyistä rikoksista. Rangaistusasteikon lieventämisessä on osaltaan kyse siitä, että tavanomaisesti tuomittava rangaistus olisi tuomitun kannalta kohtuuton tai poikkeuksellisen hankala.[127]

Rikosoikeudessa on puhuttu normaalirangaistusajattelusta, jonka perusteella on määriteltävissä rikokselle oikeuskäytännössä vakiintunut keskimääräinen rangaistuslinja, jota voidaan pitää rangaistuksen määrittelyn lähtökohtana.[128] Ajattelu antaa painoarvoa oikeuskäytännölle

[125] Linna, 2019, s. 278.
[126] Linna, 2019, s. 278.
[127] Frände, 2012, s. 385.
[128] Melander, 2015, s. 194.

rangaistuksen mittaamisen perusteena. Tyypillisestä rikoksesta tulisi tuomita normaalirangaistus, mikäli asiassa ei ole syitä poiketa rangaistuksesta lieventävin tai ankaroittavin perustein.[129]

Normaalirangaistuksen määrittelyn on esitetty olevan haasteellista,[130] koska asiaan ei yleensä oteta tuomioissa kantaa, onko jokin tuomioistuimen määräämä rangaistus normaalirangaistuksen mukainen. Normaalirangaistuksen on esitetty soveltuvan määritettäessä valintaa sakkorangaistuksen ja vankeuden välillä.[131] Aiemmin tarkasteltujen oikeustapausten ja tilastojen perusteella tietomurron yleisin rangaistusmuoto on sakkorangaistus. Rangaistuksen määrän arviointia hankaloittaa tapauksissa annettu yhteisrangaistus useasta eri rikoksesta.

Helsingin hovioikeuden tuomiossa R 20/523 nuorena henkilönä tehty tietomurto oli tapaus huomioiden erikseen yksilöity lähtökohtaisesti 15 päiväsakon suuruiseksi rangaistukseksi.[132] Tapauksessa oli erityisesti kiinnitetty huomiota tietomurron suunnitelmallisuuteen, käyttäjätilin haltuunoton kestäessä useamman päivän. Tuomion yhteinen rangaistus oli neljäkymmentä päiväsakkoa tietomurrosta, yksityiselämää loukkaavan tiedon levittämisestä ja pahoinpitelystä nuorena henkilönä.

Erityisenä huomiona rikoslain 6 luvun 5 §:n rangaistuksen koventamisperusteista tulee huomioida 5 §:n 1 momentin 2 kohta järjestäytyneestä rikollisuudesta. Rikoslain 6 luvun 5 §:n 2 momentin mukaan järjestäytyneellä rikollisryhmällä tarkoitetaan vähintään kolmen henkilön muodostamaa tietyn ajanjakson koossa pysyvää yhteenliittymää, joka yhteistuumin tekee rikoksia, joista säädetty enimmäisrangaistus on vähintään neljä vuotta vankeutta. Rikoslain 17 luvun 1 a § sisältää erillisen rangaistussäännöksen järjestäytyneen rikollisryhmän toimintaan osallistumisesta, jonka perusteella rikollisryhmän toimintaan osallistuminen on rangaistavaa.

Kansainvälisestä näkökulmasta tarkasteltuna Suomen rikoslain vaatimus perustuu Yhdistyneiden kansakuntien kansainväliseen järjestäytyneen rikollisuuden vastaiseen yleissopimukseen[133], johon viitataan usein Palermon sopimuksena.[134] Palermon sopimuksessa järjestäytyneen rikollisuuden määritelmä on rajattu rikoksiin, joiden enimmäisrangaistus on vähintään

[129] Sutela, 2020, s. 220.
[130] Kemppinen, 2021, s. 38.
[131] Kemppinen, 2021, s. 36.
[132] Helsingin hovioikeus R 20/523, s. 8.
[133] SopS 20/2004.
[134] Kimpimäki, 2015, s. 447.

neljä vuotta vankeutta. Sama määritelmä löytyy myös Euroopan unionin puitepäätöksestä 2008/841/YOS, jossa yksi järjestäytyneen rikollisuuden soveltamisalan rajoituksista on vähintään neljän vuoden enimmäisrangaistus.

Myös muut Suomen rikoslain järjestäytyneen rikollisryhmän määritelmäkriteerit perustuvat edellä mainittuun kansainväliseen sääntelyyn. Järjestäytyneen rikollisryhmän määritelmässä merkitystä on myös toiminnan pysyvyydellä. Viikon toiminnassa ollut rikollisten yhteenliittymä ei ole katsottavissa vielä järjestäytyneeksi rikollisryhmäksi, mutta vuoden toiminnassa ollut ryhmittymä on katsottavissa järjestäytyneeksi ryhmäksi, jolla on myös oma hierarkiansa ja työnjako ryhmän kesken.[135]

Tietomurron ja törkeän tietomurron enimmäisrangaistukset alittavat järjestäytyneelle rikollisuudelle määritellyn rangaistavuuden rajan, törkeän tietomurron rangaistusmaksimin ollessa kolme vuotta. Rangaistuksen mittaamisen lisäksi asialla on merkitystä aiemmin käsitellyn tekijäkumppanuuden kannalta. Ottaen huomioon lainsäädännössä järjestäytyneen rikollisryhmän toiminnalle asetettavat vaatimukset, tuomitseminen tietomurtorikoksista siten, että tietomurtorikokset ovat rikollisryhmän päärikoksia ja järjestäytynyt rikollisuus on rangaistuksen koventamisperuste, ei ole mahdollista. Erillisen arvioinnin kohteena ovat tilanteet, jossa tietomurtorikoksia tehdään osana järjestäytyneen rikollisryhmän toimintaa. Nykyisin erityisesti vaativammissa ja törkeämmissä tietomurroissa on kyse järjestäytyneestä hakkeriryhmistä, mutta esitetyn perusteella hakkeriryhmän toimintakin on lähtökohtaisesti tuomittavissa tekijäkumppanuutena, rangaistuksen koventamisperusteena tulisi soveltaa erityistä suunnitelmallisuutta järjestäytyneen rikollisuuden sijasta.

3.5 Konfiskaatiosta

Esitutkinnassa oikeudenkäynnin kannalta todistusarvoa omaavien esineiden takavarikointi on mahdollista pakkokeinolain 7 luvun mukaisesti. Takavarikko voi perustua pakkokeinolain 7 luvun 1 §:n mukaan siihen, että takavarikon kohdetta voidaan käyttää todisteena rikosasiassa, se on viety joltakulta rikoksella tai se tuomitaan menetetyksi. Takavarikossa voidaan siis katsoa olevan kyse osaltaan esimerkiksi rikosprosessin turvaamisesta.

[135] HE 153/2006 vp., s. 67.

Takavarikko muuttuu konfiskaatioksi, mikäli rikoksesta tuomittu henkilö tuomitaan menettämään rikoksentekovälineensä valtiolle turvaamistoimenpiteenä. Oikeuskirjallisuudessa konfiskaation tarkoituksena on katsottu olevan kielto- ja käskynormien noudattamisen tehostaminen ja rangaistuksen kaltainen yleis- ja erityisestävä vaikutus.[136] Konfiskaatiolla estetään uusien rikosten tekemistä.[137] Menettämisseuraamuksen lajeja ovat arvo- ja esinekonfiskaatio. Arvokonfiskaatiossa on kyse tietyn rahamäärän menettämisestä, esinekonfiskaatio tarkoittaa esineen tai muun omaisuuserän menettämistä.[138] Tietomurtorikosten kannalta relevantti konfiskaatio on esinekonfiskaatio. Konfiskaatiolajeilla ovat omat erityiset edellytykset, jotka tulee ottaa huomioon menettämisseuraamuksesta määrättäessä.[139]

Rikoslain 10 luvun 4 § määrää rikoksentekovälineen menettämisestä. Valtiolle menetetyksi voidaan tuomita rikoksen tekemisessä käytetty ampuma- tai teräase, muu hengenvaarallinen väline, tai muu esine tai omaisuus, jonka hallussapito on rangaistavaa. Lisäksi menetetyksi voidaan tuomita myös esine tai omaisuus, jota on käytetty tahallisen rikoksen tekemisessä ja esine tai omaisuus, joka on yksinomaan tai pääasiallisesti tahallista rikosta varten hankittu tai erityisen sovelias tahallisen rikoksen tekemiseen. Lisäksi menettämisseuraamusta arvioitaessa tulee rikoslain 10 luvun 4 §:n 3 momentin mukaan kiinnittää huomiota mahdollisuuteen ehkäistä uusia rikoksia. Menettämisseuraamus voidaan määrätä rikoslain 10 luvun 1 §:n 2 momentin perusteella myös tilanteessa, kun rangaistavaksi säädetyn teon tekijä on alle 15-vuotias tai mikäli tekijä on toiminut syyntakeettomana. Mikäli tapauksessa syyte jätetään nostamatta tai syyte hylätään, menettämisseurausta ei ole mahdollista määrätä.[140]

Tietojärjestelmään tunkeutuminen tai muu sähköisessä ympäristössä tehtävä rikos vaatii teknisen laitteen, joka useimmiten on perinteinen tietokone. Lähtökohtaisesti tietokoneen hallussapito ei ole rangaistavaa, joten arvioinnin keskiössä on konfiskaation mahdollisuus ehkäistä uusia rikoksia tai toimen ulottaminen nimenomaan rikoksen tekemiseen soveliaisiin välineisiin. Hallituksen esityksessä menettämisseuraamuksia koskevan lainsäädännön uudistamisesta mainitaan välinekonfiskaation kohteena esimerkiksi tietokoneohjelmat.[141] Tietokoneohjelma voi esityksen mukaan olla suunniteltu tai muunneltu tietoliikennerikosta varten. Muita

[136] Viljanen, 2007, s. 23.
[137] Viljanen, 2007, s. 23.
[138] Rautio, 2017, s. 269.
[139] Rautio, 2017, s. 274.
[140] Viljanen, 2007, s. 35.
[141] HE 80/2000 vp., s. 26.

tietomurtoon erityisesti soveltuvia välinekonfiskaation kohteita on tekniset erityislaitteet, esimerkiksi ohjelmistoradiot. Ohjelmistoradio mahdollistaa langattoman tietoliikenteen kuuntelemisen ja murtamisen.

Korkein oikeus on ottanut kantaa menettämisseuraamukseen tapauksessa KKO 2017:95, joka koskee sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapitoa ja levittämistä. Tietomurtorikosten kannalta tapauksessa on kiinnostavaa tietokoneen ja sähköisten tallennusmedioiden menettämisseuraamus rikoksen tekovälineenä. Tapauksessa syyttäjä vaati ensisijaisesti kannettavan tietokoneen ja ulkoisen tallennusvälineen menetettäväksi valtiolle, tietokoneella sijainneen laittoman materiaalin lisäksi. Toissijaisena syyttäjä vaati ulkoisen tallennusvälineen menettämistä valtiolle ja kannettavan tietokoneen sisällön ylikirjoittamista ennen palauttamista kannettavan omistajalle.

Korkein oikeus arvioi ratkaisussaan, että tietokone ja ulkoinen levyasema ovat olleet välttämättömiä välineitä rikoksen toteuttamisen kannalta, jolloin laitteita pidetään rikoslain mukaisina rikoksentekovälineinä. Samalla korkein oikeus totesi, että kyseisessä tapauksessa tietokonetta oli käytetty myös muuhun, kuin laittomaan toimintaan ja että internetyhteydellä varustettu tietokone on yleisesti käytössä oleva ja tarpeellinen kulutushyödyke.

Menettämisseuraamus määrättiin korkeimman oikeuden tuomiossa raukeamaan, jos laitteista hävitetään laiton materiaali omistajan kustannuksella. Vaikka kyse on erityyppisestä rikollisuudesta, kuin tieto- ja viestintärikoksista, on kyse teknisestä välineestä. Argumentointi on siten sovellettavissa yleisemmin siltä kannalta, miten menettämisseuraamusta tulisi käsitellä sen kohdentuessa tietokoneeseen.

Menettämisseuraamus uusien rikosten ehkäisemiseksi ei ole lähtökohtaisesti relevanttia tietomurrossa, koska uusi vastaava laite on mahdollista hankkia helposti uudelleen. Myös korkein oikeus katsoi päätöksessään KKO 2017:95, että tietokone on yleisesti käytössä oleva ja asioiden hoitamisen kannalta tarpeellinen hyödyke, jonka uudelleen hankkiminen ei ole vaikeaa, jolloin yleisesti menettämisseuraamuksella ei voida vaikuttaa rikoksentekijän syyllistymiseen uusiin rikoksiin. Mitä edullisempaa ja vaivattomampaa menettämisseuraamuksen kohteena olevien välineiden hankinta uudelleen on, sitä heikompi on konfiskoinnin vaikutus.[142] Korkeimman

[142] Viljanen, 2007, s. 25.

oikeuden ratkaisussa menettämisseuraamus kohdistuikin lopulta laittomaan materiaaliin, eikä tietokonetta tai tallennusvälinettä tuomittu valtiolle menetetyksi, vaan menettämisseuraamus määrättiin tapauksessa raukeamaan, kunhan laiton materiaali on poistettu ylikirjoittamalla tallennusväline luotettavasti.

Suhteessa korkeimman oikeuden käsittelemään tapaukseen voidaan todeta tietoteknisten laitteiden olevan korostetussa avainasemassa tietomurtorikoksen toteuttamisessa. Tietomurron toteuttamisen kannalta tietokone tai muu vastaava laite on suuressa osassa tapauksia välttämätön. Toisaalta tietokonetta voidaan käyttää myös laillisiin toimiin. Tietokoneen korvaaminen uudella ei ole kallista tai haastavaa, joten rikoksentekovälineen menettämisseuraamus ei sinänsä ole tehokasta uusien rikosten estämiseksi.

Tietokoneelle tallennetut murtautumiseen käytettävät ohjelmat vaativat korostettua tietoteknistä osaamista, eikä niille ole lähtökohtaisesti laillista käyttötarkoitusta. Tietomurrossa käytettyjen laitteiden sisältöä voitaisiin tuomita menetetyksi ehdollisena, kuten korkeimman oikeuden tapauksessa. Menettämisseuraamus raukeaisi, jos laitteista poistettaisiin rikoksen toteuttamiseen käytetyt ohjelmat. Data on sinänsä erityinen objekti määrättäessä konfiskaatiosta, koska sitä ei ole olemassa yksinään, vaan sen olemassaolo on riippuvainen jostain fyysisestä kohteesta.[143] Fyysinen kohde on esimerkiksi jokin tallennusmedia, mihin data on tallennettu.

Mikäli menettämisseuraamuksen arvioinnin kohteena olisi jokin muu tietomurrossa käytetty laite, kuten digitaalisten signaalien kuunteluun ja analyysiin tarkoitettu langaton vastaanotin, arviointiprosessin tuloksena voisi olla koko laitteen menettäminen valtiolle. Merkitystä on erityisesti sillä, onko menettämisseuraamuksen arvioinnin kohteena olevalle esineelle muita kuin laittomia käyttötarkoituksia ja kuinka vaikeaa uuden vastaavan laitteen hankinta on. Tarkastelun kohteena olleiden tuomioistuinten tuomioiden perusteella menettämisseuraamusta ei ole määrätty turvaamistoimenpiteenä tarkastelluissa tuomioissa. Tarkastelun kohteina olleissa tuomioissa ei ole myöskään yksilöity tietomurtoon käytettyjä laitteita, joten perusteluja menettämisseuraamuksen määräämättä jättämiselle ei ole määriteltävissä tarkastelluista tuomioista.

[143] Rautio, 2017, s. 278.

4 Lainkonkurrenssi tietomurrossa

4.1 Toissijaisuus ja lainkonkurrenssi

Rikoslain erityisen osan rikosten tunnusmerkistöt on kirjoitettu abstraktiin muotoon, joten rikosprosessissa tapahtunutta tekoa verrataan rikoslain yleismuotoiseen tunnusmerkistöön. Vertaamisen perusteella arvioidaan, soveltuuko tunnusmerkistö käsillä olevaan tekoon. Abstraktiudesta voi seurata myös tilanne, jossa useampi kuin yksi tunnusmerkistö soveltuu arvioinnin kohteena olevaan tekoon, eikä arvioija voi olla varma, mikä tunnusmerkistö soveltuu parhaiten tapaukseen. Tilanteessa on kyse lainkonkurrenssista, jolloin on mahdollisuus soveltaa tapaukseen kaikkia sopivia tunnusmerkistöjä, tai valita yksi rikostunnusmerkistö, jota sovelletaan tapaukseen.

Lainkonkurrenssi on tunnistettu lainsäädäntötyössä. Lakivaliokunta on lausunut rikoslain rikostunnusmerkistöjen laatimisesta, että lainkonkurrenssitilanteita tulisi olla mahdollisimman vähän.[144] Samanaikaisesti rikoslainsäädäntö ei kuitenkaan sisällä yksiselitteisiä oikeusnormeja lainkonkurrenssitilanteita varten, vaan konkurrenssitilanteiden ratkaisuohjeet perustuvat oikeuskäytäntöön ja oikeustieteen tutkimukseen. Lainkonkurrenssitilanteita on mahdollista jaotella subordinaatioon, subsidiariteettiin ja oikeushyvien suojeluintressiin.[145]

Subordinaatiotilanteessa käsiteltävä rikostyyppi sisältyy kokonaan toisen rikostyypin sisään.[146] Rikostyypit ovat sisäkkäisiä esimerkiksi tilanteessa, jossa yhdestä teosta on laissa useampia törkeysasteita. Näin ollen törkeä tietomurto sisältää tietomurron tekomuodon. Subordinaation voi katsoa koskevan myös rikoksen esi- ja jälkitekoja, koska niistä ei yleisesti katsota olevan tarpeen määrätä erillistä rangaistusta, vaan niiden katsotaan sisältyvän tuomittuun rikokseen.[147] Saman periaatteen mukaisesti rikoksen valmistelun voidaan katsoa kuuluvan tuomittuun rikokseen. Esi- ja jälkiteot ovat tällöin myötärangaistuja osana päätekoa.

[144] LaVM 22/1994 vp., s. 5.
[145] Tapani, ym. 2019, s. 568.
[146] Frände, 2012, s. 274.
[147] Luoto, 2022, s. 411.

Tietomurron tapauksessa lainkonkurrenssi on lähtökohtaisesti ratkaistu subsidiariteetilla, eli toissijaisuudella, kirjoittamalla toissijaisuuslauseke rikossäännökseen. Rikoslain 38 luvun 8 §:n 4 momentti määrää tietomurtosäännöstä sovellettavaksi vain sellaiseen tekoon, josta ei ole muualla laissa määrätty ankarampaa tai yhtä ankaraa rangaistusta. Lähtökohtana on rikossäännösten välinen rangaistusasteikkojen vertailu. Subsidiariteettilausekkeen perusteella tarkastelua ei tule kuitenkaan ulottaa ainoastaan rangaistusasteikon tarkasteluun, merkitystä on myös tunnusmerkistön soveltuvuudella. Subsidiariteetin perusteella tietomurtoa voi luonnehtia yleiseksi hakkerointirikokseksi, joka syrjäytyy, mikäli joku toinen säännös soveltuu paremmin teon tunnusmerkistöön.

Oikeushyvien suojeluintressin perusteella arvioitavassa lainkonkurrenssissa kyse on tilanteesta, jossa kaksi eri tunnusmerkistöä suojaa samaa oikeushyvää, eikä molempia katsota tarpeelliseksi soveltaa. Tilanteessa valitaan parhaiten soveltuva tunnusmerkistö. Toisaalta jos tunnusmerkistöjen suojelukohteet ovat erilaiset, ei oikeushyvien suojeluintressin punnintaa ole tarpeen tehdä. Tieto- ja viestintärikosten suojelukohde on järjestelmään tallennetussa tiedossa, datassa. Oikeuskirjallisuudessa on katsottu merkittävänä tarkastella lainkonkurrenssitilanteissa sitä, suojellaanko tarkastelun kohteena olevilla rikossäännöksillä yksilöllisiä vai yhteisiä oikeushyviä.[148] Oikeushyvien kannalta tulee myös tarkastella sitä, ovatko päällekkäisillä rikossäännöksillä suojeltavat edut erilaisia vai osittain yhteneväisiä.[149]

Tapauksessa Helsingin hovioikeus R 20/523 tuomioistuin ei aiemmin esitetyn tapauksen perusteella lähtökohtaisesti huomioinut lainkonkurrenssia, tuomitessaan henkilön tietomurrosta ja yksityiselämää loukkaavan tiedon levittämisestä.[150] Toissijaisuuslausekkeen perusteella tietomurron tulisi väistyä suhteessa yksityiselämää loukkaavan tiedon levittämiseen. Vaikka tapahtumat sinänsä liittyvät toisiinsa ja tietomurrolla saatua materiaalia käytetään toisessa rikoksessa, kyseessä eivät ole yksi ja sama teko,[151] vaikka tapahtumainkulun mielessä teko on jatkumoa edelliseen. Tietomurrolla suojellaan tiedon eheyttä ja luotettavuutta, yksityiselämää loukkaavan tiedon levittäminen tai kunnianloukkaus suojelee henkilökohtaista koskemattomuutta.

[148] Piippo, 2022, s. 646.
[149] Piippo, 2022, s. 647.
[150] Helsingin HO 16.7.2021, R 20/523, s. 11.
[151] Tapani ym. 2019, s. 570.

Lähtökohtaisesti siis tarkastellessa rikossäännöksien välistä lainkonkurrenssia, tulee asiassa tarkastaa subordinaatiotilanne, toissijaisuuslausekkeen läsnäolo ja mihin toissijaisuuden arviointi on lainsäädännössä määritetty. Lisäksi tulee kiinnittää erityistä huomiota suojeluintressien päällekkäisyyksiin. Käsittelen seuraavaksi tietomurron asemointia mahdollisissa lainkonkurrenssitilanteissa.

4.2 Luvaton käyttö

Mikäli luvaton toiminta tietojärjestelmässä ei rajoitu pelkästään järjestelmään tunkeutumiseen tai tietojärjestelmässä olevan tiedon selonottamiseen, henkilö voi syyllistyä rikoslain 28 luvun 7–9 §:ien mukaiseen luvattomaan käyttöön. Rikoslain 28 luvun 7 § määrittelee luvattomaksi käytöksi tilanteen, jossa tekijä käyttää luvattomasti toisen irtainta omaisuutta, kiinteää konetta tai laitetta. Luvattoman käytön vähimmäisrangaistus on sakkorangaistus ja enimmäisrangaistus yksi vuosi vankeutta. Rikoslaki sisältää luvattomasta käytöstä myös törkeän ja lievän tekomuodon.

Törkeä luvaton käyttö edellyttää rikoslain 28 luvun 8 §:n perusteella, että luvattomassa käytössä tavoitellaan huomattavaa taloudellista hyötyä tai aiheutetaan rikoksen uhrille olosuhteet huomioiden erityisen tuntuvaa vahinkoa tai haittaa. Luvattoman käytön tulee olla kokonaisuutena arvostellen törkeä. Törkeän luvattoman käytön vähimmäisrangaistus on sakkorangaistus ja enimmäisrangaistus kaksi vuotta vankeutta.

Lievä luvaton käyttö on rikoslain 28 luvun 9 §:n mukaan kyseessä, kun luvaton käyttö on kokonaisuutena arvostellen vähäinen huomioiden sen, että rikos ei ole omiaan aiheuttamaan merkittävää vahinkoa tai haittaa, tai rikoksessa on muita vähäisyyteen vaikuttavia seikkoja. Luvattomasta käytöstä tuomittava rangaistus on sakkorangaistus.

Tietomurron ja luvattoman käytön välistä konkurrenssia on määritelty lain esitöissä. HE 94/1993 vp mukaan, jos rikos on edennyt tietojärjestelmään tunkeutumisen lisäksi tietojen käyttämiseen saakka, tekoon tulisi soveltaa luvattoman käytön tunnusmerkistöä.[152] Esitöissä esitetyn näkemyksen selkeys on kuitenkin nähdäkseni riippuvainen tietojärjestelmän sisällön laadusta. Mikäli tietojärjestelmän sisältö koostuu esimerkiksi maksumuurin takana olevasta

[152] HE 94/1993 vp., s. 156.

tiedosta, luvaton käyttö ja siitä saatava hyöty on mahdollista määritellä rahallisesti ja soveltuva rikossäännös on selkeä. Mikäli kohteena oleva tietojärjestelmä sisältää esimerkiksi henkilötietoja tai sosiaalisen median sisältöä, lainkonkurrenssin määrittely on haastavampaa.

Luvattoman käytön ja tietomurron välisen suhteen arvioinnissa on kuitenkin huomioitava esimerkiksi Keski-Suomen käräjäoikeuden tapaus R 20/118, jossa rangaistusvaatimuksena on ollut edelleen tietomurto, eikä luvaton käyttö, vaikka tietojärjestelmässä otettiin selkoa sen sisällöstä. Tapauksessa syytetty oli teonkuvauksen mukaan tunkeutunut oikeudettomasti henkilön sosiaalisen median tileille ja lukenut henkilön yksityisiä Instagram-keskusteluja.

Lainkonkurrenssin määrittely voi olla haastavaa, mikäli teko on jäänyt yritysasteelle ja tapausta arvioidaan luvattoman käytön näkökulmasta. Kuten edellä on mainittu, rikoslain 6 luvun 8 §:n mukaan rikoksen jäädessä yritykseen, rangaistus määrätään lievennetyltä rangaistusasteikolta. Lievennetty rangaistusasteikko on pykälän 2 momentin mukaan enintään kolme neljännestä rikoksesta säädetyn vankeus- tai sakkorangaistuksen enimmäismäärästä ja vähintään säädetyn rangaistuslajin vähimmäismäärän. Rikoslain 38 luvun 8 §:n perusteella tietomurron yrityksessä rangaistuksen enimmäismäärä on tämän myötä 1,5 vuotta vankeutta. Luvaton käyttö määritellään rikoslain 28 luvun 7 §:ssä, jossa enimmäisrangaistukseksi on määrätty vuoden vankeusrangaistus. Luvattoman käytön yrityksestä tuomittava enimmäisrangaistus olisi siis yhdeksän kuukauden vankeusrangaistus.

Näin ollen, mikäli tilanteessa lainkonkurrenssin arvion kohteena oleva rikos on jäänyt yritysasteelle, tietomurron yrityksen perusteella annettava tuomio voi olla ankarampi, kuin jos asiasta tuomitaan luvattoman käytön yrityksenä. Tuomion antamisen kannalta merkitystä on syytetyn toiminnan tarkoitusperillä. Mikäli henkilön tavoitteena oli ainoastaan tunkeutua tietojärjestelmään, asiassa tulisi tuomita tietomurron yrityksen mukaan. Mikäli henkilön tarkoitusperiin kuuluu pelkän tunkeutumisen lisäksi taloudellisen hyödyn tavoittelu tai tietojärjestelmän tosiasiallinen luvaton käyttö, asiassa tulisi tuomita rangaistus luvattoman käytön yrityksen perusteella. Mikäli syytetty ei itse halua selvittää omia tarkoitusperiään asiassa, lainkonkurrenssin ratkaiseminen konkreettisetkin tosiseikat huomioiden voi olla haastavaa.

Luvattoman käytön suojeluobjektina on omaisuuden suoja ja luvattoman käytön kohteena olevaan asiaan liittyvät taloudelliset intressit. Tietomurron rangaistavuudella suojellaan tietojärjestelmän ja tiedon luottamuksellisuutta. Mikäli molemmat intressit edellyttävät suojelua,

keskinäistä arvojärjestystä voi arvioida esimerkiksi luvattoman käytön vahingollisuudella. Mikäli luvaton käyttö jää vähäiseksi suhteessa tietojärjestelmään tunkeutumiseen, rangaistus voitaisiin määrätä tietojärjestelmään tunkeutumisen perusteella tietomurrosta.[153]

4.3 Yritysvakoilu

Yritysvakoilua koskeva rikossäännös sijaitsee rikoslain 30 luvun 4 §:ssä. Sen mukaan joka oikeudettomasti hankkii tiedon toiselle kuuluvasta liikesalaisuudesta tunkeutumalla ulkopuoliselta suljettuun paikkaan tai ulkopuolisilta suojattuun tietojärjestelmään, hankkimalla haltuunsa tai jäljentämällä asiakirjan tai muun tallenteen tai muulla rinnastettavalla tavalla, tai käyttämällä teknistä erikoislaitetta, on tuomittava 30 luvun 4 §:n 2 momentin mukaan yritysvakoilusta vähimmäisrangaistuksena sakkorangaistukseen tai enimmäisrangaistuksena kahden vuoden vankeusrangaistukseen. Myös yritysvakoilun yritys on määrätty rangaistavaksi. Yritysvakoilun kannalta huomionarvoista on se, että tekijä voi olla suhteessa yritykseen täysin ulkopuolinen henkilö, tai yrityksen palveluksessa oleva henkilö, kenellä ei ole luvallista pääsyä vakoilun kohteena oleviin tietoihin.[154]

Yritysvakoilun kannalta suojeluintressinä on tiedon koskemattomuus.[155] Yritysvakoilun kohteena olevan uhrin intressissä on pitää kohteena oleva tieto salattuna, koska sen paljastuminen aiheuttaa taloudellista vahinkoa elinkeinotoiminnassa.[156] Yritysvakoilun ja tietomurron lainkonkurrenssin kannalta merkittävää on kuitenkin se, että rikos tapahtuu tunkeutumalla tietojärjestelmään. Tietomurto voi kohdistua vain tietojärjestelmään tunkeutumiseen, yritysvakoilu voi kohdistua ulkopuolisilta suojattuun tietojärjestelmään tai ulkopuolisilta suojattuun paikkaan.[157]

Rikoslain erityisen osan toista osittaisuudistusta koskeva hallituksen esitys on ottanut kantaa tilanteeseen, missä tietojärjestelmään tunkeutuminen tapahtuu yritysvakoilua varten. Esityksen mukaan tietomurtoa koskevat säännökset syrjäytyvät rikoslain yritysvakoilua koskevan sääntelyn edellä.[158] Asiassa on kuitenkin huomioitava hallituksen esityksestä kulunut aika, miltei kolmekymmentä vuotta. Lisäksi oikeuskirjallisuudessa on katsottu myös korkeimman oikeuden

[153] HE 232/2014 vp., s. 12.
[154] Frände, ym., 2018, s. 727.
[155] Lappi-Seppälä, ym., 2022.
[156] Lappi-Seppälä, ym., 2022.
[157] Frände, ym., 2018, s. 729.
[158] HE 94/1993 vp., s. 156.

ennakkopäätösten perusteella, että lainkonkurrenssi tulee arvioida tapauskohtaisesti ja tosiseikat huomioiden.[159] Suojeluintressin osalta on katsottavissa osittainen samankaltaisuus tietomurron ja yritysvakoilun kesken. Kummankin tavoitteena voidaan katsoa olevan rajatulle joukolle tarkoitetun tiedon suojaaminen ulkopuolisilta toimijoilta, joilla ei ole oikeutta kyseiseen tietoon. Yritysvakoilun ja tietomurron rangaistussäädökset ovat yhtä suuret, minkä perusteella tietomurtosäännös syrjäytyy ottaen huomioon syrjäytymisen myös tilanteissa, joissa muualla laissa on säädetty yhtä ankara rangaistus.

Suojeltavien etujen ja rangaistussäännösten perusteella tilanne voi vaikuttaa selkeältä, tietomurto väistyisi yritysvakoilua koskevan rangaistussäännöksen edeltä. Kuvitteellisessa tilanteessa on kuitenkin mahdollista arvioida, voiko erilliset asianomistajat asiassa vaikuttaa lainkonkurrenssin soveltuvuuteen.[160] Tietojärjestelmään tunkeutuvan henkilön tavoitteena on ollut ottaa selvää yrityssalaisuudesta, jonka asianomistajana on sitä hallitseva yritys. Nykyisin on kuitenkin hyvin mahdollista, että yritys ostaa tietojärjestelmänsä ja muut IT-palvelut ostopalveluna ulkopuoliselta taholta, jolloin tietojärjestelmä ei ole suoraan yrityksen omaisuutta, vaan hän on hankkinut käyttöoikeuden siihen ja tallentaa tietojaan järjestelmään. Tällöin tietojärjestelmän omistaa tietojärjestelmäpalveluja tarjoava taho, minkä järjestelmään itse tunkeutuminen kohdistuu, joten asianomistajia voisi olla kaksi. Oikeuskirjallisuudessa on esitetty, ettei lainkonkurrenssille ole perusteita, jos tilanteessa on loukattu eri asianomistajia.[161]

Asian lopullista ratkaisua lainkonkurrenssin osalta tulisi arvioida sen kannalta, tuleeko toiseen asianomistajaan kohdistuva tietomurto riittävästi rangaistuksi yritysvakoilua koskevan rikossäännöksen perusteella, jossa pääasiallisena asianomistajana on tiedot omistava yritys. Tilanteessa tulisi myös arvioida, koituisiko tilanteesta toisaalta liian suuri rangaistus syytetylle, jos hänet tuomitaan sekä tietojen yritysvakoilusta tiedot omistavaa ensimmäistä asianomistajaa kohtaan, että tietomurrosta itse tietojärjestelmäpalvelun omistavaa toista asianomistajaa kohtaan. Oikeuskirjallisuudessa lainkonkurrenssin argumenttina on esitetty, ettei yhden rikossäännöksen soveltamisen jälkeen tapauksessa jää jäljelle enempää vääryyttä, jonka perusteella tulisi soveltaa toistakin säännöstä.[162] Rikosoikeudellisen vastuun, lainkonkurrenssin ja rangaistuksen

[159] Kallio, 2018, s. 31.
[160] Kallio, 2018, s. 33.
[161] Luoto, 2022, s. 409.
[162] Nuutila, 1997, s. 371.

lisäksi kuvitteellisessa esimerkkitapauksessa arvioitavana voisivat kuitenkin olla myös yksityisoikeudelliset vahingonkorvausvaatimukset molempien asianomistajien toimesta.

4.4 Datavahingonteko

Datavahingonteko on määritelty rikoslain 35 luvun 3 a §:ssä. Datavahingonteon edellytyksenä on

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

Myös datavahingonteosta on määriteltynä rikoslaissa lievä ja törkeä tekomuoto. Törkeä datavahingonteko on määritelty rikoslain 35 luvun 3 b §:ssä. Datavahingonteko kvalifioituu rikoslain 35 luvun 3 b §:n 1 momentin mukaan törkeäksi

> ”Jos datavahingonteossa
>
> 1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa,
>
> 2) rikos tehdään osana 6 luvun 5 §:n 2 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa,
>
> 3) rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään tietojärjestelmiä käyttäen 34 luvun 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa tai
>
> 4) rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon
>
> ja datavahingonteko on kokonaisuutena arvostellen törkeä…”

Törkeän datavahingonteon vähimmäisrangaistus on vähintään neljän kuukauden vankeusrangaistus ja enimmäisrangaistus viiden vuoden vankeusrangaistus. Rikoslain 35 luvun 3 b §:n 3 momentin mukaan törkeän datavahingonteon yritys on rangaistava.

Lievän datavahingonteon määritelmä sijaitsee rikoslain 35 luvun 3 c §:ssä. Jos datavahingonteko on huomioiden vahingon vähäisyys tai muut rikokseen liittyvät seikat kokonaisuutena arvostellen vähäinen, tuomitaan henkilö lievästä datavahingonteosta sakkorangaistukseen. Datavahingonteon tekotapojen kriminalisoidessa millä eri tavoin dataa voidaan muuttaa oikeudettomasti sen alkuperäisestä muodosta, suojeluintressi on samankaltainen kuin tietomurrossa, omaisuudensuoja ja tiedon eheyden säilyttäminen. Rangaistavuuden edellytyksenä on vahingoittamistarkoitus ja sen tapahtuminen oikeudettomasti.[163] Datavahingonteon arvioinnin kannalta tallennetun datan muodolla ei ole merkitystä. Tunnusmerkistön perusteella kaikki tietojärjestelmässä oleva data kuuluu rikossäännöksen piiriin. Datalla täytyy kuitenkin olla arvoa, jotta vahingoittamistarkoitus voi täyttyä ja sitä voidaan arvioida.[164]

Datavahingonteko on etusijalla tietomurtoon nähden vertaillessa tietomurtoa ja datavahingontekoa yleisten lainkonkurrenssisääntöjen kannalta. Datavahingonteon rangaistusasteikko on kovempi verrattuna tietomurron rangaistusasteikkoon, jolloin tietomurron toissijaisuussäännöksen perusteella asia tulee tutkia ja rangaistus määrittää datavahingonteon perusteella. Myös suojelukohde on arvioitavissa samansuuntaiseksi molempien rikossäännösten osalta. Toisaalta lainkonkurrenssia vastaan puhuu rikossäännösten tunnusmerkistöjen erilaisuus. Tietomurrossa tunkeudutaan oikeudettomasti järjestelmään tai otetaan selkoa siellä olevasta datasta, datavahingonteko edellyttää selkeästi järjestelmässä olevaan dataan vaikuttamista negatiivisesti.

Tietomurto voi näyttäytyä valmisteluluonteisena tekona suhteessa datavahingontekoon. Datavahingonteon edellytyksenä voi olla ensimmäisenä pääsy kohteena olevaan tietojärjestelmään, mikä edellyttää tietomurtoa, oikeudetonta tunkeutumista itse tietojärjestelmään. Oikeuskirjallisuudessa on tarkasteltu lainkonkurrenssitilanteiden ratkaisun kannalta myös tekokokonaisuuden yhtenäisyyttä. Mitä yhtenäisemmästä kokonaisuudesta on kyse rikoksen tekotavan, ajan ja paikan kannalta, sitä perustellumpaa on tarkastella sitä yhtyneenä rikoksena.[165] Samanaikaisesti

[163] Lappi-Seppälä, ym., 2022.
[164] Frände, ym., 2018, s. 547.
[165] Luoto, 2022, s. 415.

merkitystä on tekijän tahtotilalla. Jos tekijän menettely perustuu yhteen ja samaan tahtotilaan, pidetään rikosten yhtymistä perusteltuna.[166]

Mikäli datavahingonteon rikostunnusmerkistön täyttävä toiminta tapahtuu välittömästi oikeudettoman tietojärjestelmään tunkeutumisen jälkeen, on koko tapahtumaketjua perusteltua tarkastella datavahingonteon tunnusmerkistön perusteella. Samalla olisi mahdollista arvioida sitä, onko tekijän tavoitteena ollut yleisesti aiheuttaa vahinkoa tietojärjestelmässä. Tämä puhuisi rikosten yhtymisen puolesta. Vastavuoroisesti lainkonkurrenssin arviointi on haastavampaa kuvitteellisessa tilanteessa, missä oikeudeton tietojärjestelmään tunkeutuminen on tapahtunut huomattavan kauan aikaa sitten, minkä jälkeen tekijä palaa vertauskuvainnollisesti rikospaikalle vahingoittamaan tietojärjestelmässä olevaa dataa. Tapahtumapaikka on sama, tietojärjestelmä, johon on hankittu oikeudeton pääsy, mutta tapahtumien ajallinen etäisyys asettaa lainkonkurrenssin edellytykset arvioitavaksi. Kuvatussa tilanteessa olisi tärkeää myös arvioida onko tekijän tahtotilana alun perin ollut vain järjestelmään tunkeutuminen, vai onko kyse ajallisesti hajautetusta datavahingonteosta.

Tietomurron törkeän tekomuodon yhtenä vaihtoehtoisena edellytyksenä on erityinen suunnitelmallisuus, minkä on mahdollista ilmetä poikkeuksellisina valmistelutoimenpiteinä tai erityisinä kiinnijäämistä estävinä toimenpiteinä.[167] Lainkonkurrenssin kannalta mielenkiintoinen arvioinnin kohde olisi tilanne, jossa henkilön olisi katsottu syyllistyneen törkeään tietomurtoon ja normaaliksi kvalifioitavaan datavahingontekoon. Lähtökohtaisesti törkeä tekomuoto sisältää alemman asteisen tekomuodon vääryyden ja oikeudenloukkaukset. Ryöstö sisältää lähtökohtaisesti pahoinpitelyn, mutta ei törkeää pahoinpitelyä.[168] Jos tapahtumaketjussa valmisteluteoksi katsottavissa oleva rikos on katsottavissa törkeäksi, mutta varsinaisen pääteon kohdalla noudatetaan tavallista rikossäännöstä, lainkonkurrenssin arviointi ja toteutuminen on haastavampaa. Erityisesti datavahingonteon toteutumisen kohdalla voi olla tarpeen arvioida tietojärjestelmään tunkeutumisen suunnitelmallisuutta.

[166] Luoto, 2022, s. 414.
[167] Lappi-Seppälä, ym., 2022.
[168] Luoto, 2022, s. 413.

5 Tietomurtorikosten tutkintaan liittyviä haasteita

5.1 Esitutkinnan vaatimuksista

Koska tietomurron kohdalla rikospaikka sijaitsee fyysisen ympäristön sijasta sähköisessä ympäristössä, todistusaineiston keräämiseen ja rikoksentekovälineisiin liittyy omia erikoisuuksiaan. Aloitettaessa esitutkinta digitaalisen rikospaikan tutkimus eroaa tavanomaisesta esitutkinnasta toimintaympäristönsä vuoksi. Voi olla mahdollista, että rikokselle ei ole määriteltävissä selkeästi epäiltyä. Sähköisessä toimintaympäristössä myös todisteiden tuhoamiseen tai peittelyyn on enemmän mahdollisuuksia tavanomaiseen tilanteeseen verrattuna. Kun murtautuja on jo oikeudettomasti järjestelmässä, hänellä on yleensä mahdollisuus myös modifioida järjestelmän tietoja peitelläkseen omia jälkiään. Tietojärjestelmiin liittyvä tutkinta aloitetaan yleisesti murron kohteena olevasta järjestelmästä, mutta tietomurtoon liittyvää dataa hankitaan myös muista lähteistä, kuten avoimesta verkosta ja kolmannelta osapuolelta, kuten internet-yhteyden palveluntarjoajalta.[169] Tietojärjestelmän lokitiedoista on yleisesti yksilöitävissä, mistä IP-osoitteista tietojärjestelmään on otettu yhteyttä. Vastaavasti tietoliikennepalveluntarjoajalla on mahdollisuus yksilöidä IP-osoitteen käyttäjä omassa järjestelmässään, jonka perusteella on mahdollista selvittää IP-osoitteen käyttäjä.

Kansallisessa lainsäädännössä poliisilain (872/2011) 4 luvun 3 §:n perusteella poliisilla on oikeus pyytää teleyritykseltä tietoja poliisille kuuluvan tehtävän, kuten rikoksen selvittämisen, toimittamiseksi. Teleyritykseltä, toisin sanoen tietoliikennepalveluntarjoajalta, pyydettäviä tietoja voivat olla esimerkiksi teleosoitteeseen liittyvät yhteystiedot tai teleosoitteen tai päätelaitteen yksilöivät tiedot. Tiedot voivat kohdistua siis esimerkiksi IP-osoitteen käyttäjän yksilöiviin tietoihin tai palveluntarjoajaan yhteydessä olevien laitteiden tietoihin. Poliisilain 4 luvun 3 §:n 2 momentissa on määritelty poliisille valtuus saada yksittäistapauksessa teleyritykseltä tai yhteisötilaajalta tietoja teleosoitteesta, jos tiedot ovat tarpeen poliisille kuuluvan tehtävän suorittamiseksi. Oikeuskirjallisuudessa on katsottu, että minkä tahansa rikoksen tutkinta on tehtävä, joka oikeuttaa poliisia saamaan edellä mainittuja tietoja.[170] Käsitteitä ei myöskään ole yksilöity

[169] Riekkinen, 2019, s. 210.
[170] Riekkinen, 2018, s. 88.

poliisilaissa, joten tiedonsaantioikeus on tulkittu verrattain laajaksi.[171] Yhteystiedon, eli esimerkiksi osoitteen perusteella on mahdollisuus toteuttaa pakkokeinolain (806/2011) mukainen paikkaan kohdistuva etsintä, johon sisältyy myös laite-etsintä. Etsintää sääntelee pakkokeinolain 8 luku.

Poliisilain lisäksi pakkokeinolain 10 luvun 25 §:ssä esitutkintaviranomaiselle on määritelty mahdollisuus hankkia teleosoitteen tai telepäätelaitteen yksilöintitietoja. Yksilöintitietoja on mahdollista hankkia, jos epäillyn rikoksen säädetty ankarin rangaistus on vähintään vuosi vankeutta, mikä täyttyy sekä tietomurron että törkeän tietomurron kohdalla. Erona poliisilain ja pakkokeinolain välillä on se, että pakkokeinolaissa esitutkintaviranomainen itse käyttää laitetta, joka suorittaa teleosoitteen, yleensä IP-osoitteen ja telepäätelaitteen yksilöimisen ja laite antaa tiedot esitutkintaviranomaiselle, eikä esimerkiksi teleyritys.

Teleyritykselle on määritelty säilyttämisvelvollisuus tunnistetietoihin määritellyksi ajaksi. Teleyrityksen tunnistamistietojen säilyttämisvelvollisuus perustuu Euroopan parlamentin ja neuvoston direktiiviin 2006/24/EY yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä. Direktiivissä tunnistetiedoilla katsotaan olevan olennainen merkitys rikosten selvittämisessä.[172] Ajallisesti säilyttämisvelvollisuuden vaatimuksen tulee olla riittävä rikostutkinnan ja syyteharkinnan kannalta. Direktiivin 6 artikla määrittelee säilytysajan kuuden kuukauden ja kahden vuoden välille. Kansallisesti säilyttämisvelvollisuudesta säädetään sähköisen viestinnän palveluista annetun lain 157 §:ssä. Säilyttämisvelvoitteen aikamääre on säädetty Suomessa 12 kuukauteen, minkä katsottiin lain valmistelussa riittävän direktiivin oikeamukaiseen toteutumiseen suhteessa säilyttämisestä aiheutuviin kustannuksiin.[173]

Yleensä ensimmäinen todiste tietoverkkoa hyödyntäen toteutetuissa rikoksissa on IP-osoite ja palveluntarjoajalta hankitut osoitteeseen liittyvät asiakastiedot.[174] Todistustaakan kannalta pelkkä tietokoneen omistaminen, josta rikos on mahdollisesti tehty, ei riitä rikosoikeudelliseen vastuuseen, vaan rikoksentekijä tulee yksilöidä paremmin näyttökynnyksen saavuttamiseksi.[175] Oikeudenkäynnin kannalta syytetylle voi kuitenkin muodostua asiakastietojen perusteella

[171] Riekkinen, 2018, s, 89.
[172] 2006/24/EY, lausunnon 7 kohta.
[173] Innanen, ym., 2012, s. 212.
[174] Riekkinen, 2020, s. 1007.
[175] Riekkinen, 2019, s. 188.

selitysvelvollisuus tietoverkkorikosten yhteydessä.[176] Rikosasian vastaaja ei voi pelkästään kiistää vastapuolen esittämiä väitteitä, jos vastapuolella on esittää asiakastietojen perusteella yksilöitävään IP-osoitteeseen yhdistettävää verkkoliikennettä, esimerkiksi tietomurtotapauksessa yhteydenottoja murron kohteena olevaan tietojärjestelmään.

Selitysvelvollisuus ja IP-osoitteeseen liittyvä todistelu ei kuitenkaan ole käytännössä yksiselitteistä. Helsingin hovioikeuden tapauksessa 16.07.2021, R 20/523 vastaajaa oli epäilty tietomurrosta nuorena henkilönä. Syyte tietomurrosta oli hylätty ensimmäisenä oikeusasteena toimineessa Helsingin käräjäoikeudessa teknisen todistusaineiston perusteella. Käräjäoikeuden tuomiolauselmassa henkilön syyllisyyden oli katsottu jäävän epäselväksi. Tietomurtopäivänä oikeudettoman tunkeutumisen kohteena olleelle sosiaalisen median käyttäjätilille oli kirjauduttu historiatietojen mukaan neljästä eri IP-osoitteesta. IP-osoitteiden haltijatiedot olivat jääneet selvittämättä, jolloin käräjäoikeus katsoi asiassa esitetyltä näytöltä puuttuvan riittävän varmuuden ja epäselvä asia ratkaistiin vastaajan eduksi. Käräjäoikeuden käsittelyssä huomionarvoista on se, että asiassa syytetyn hallussa oli todettu olleen uhrin yksityisyyttä loukkaavaa materiaalia, jota oli ladattu tapahtuneen tietomurron jälkeen sosiaalisen median palveluun.[177] Tämän oli katsottu asiassa puhuvan sen puolesta, että epäilty olisi tehnyt myös tarkastelun kohteena olleen tietomurron. Yksityisyyttä loukkaavan materiaalin lataaminen rangaistiin tapauksessa omana tekonaan yksityiselämää loukkaavan tiedon levittämisenä.

Tapauksessa syyttäjä valitti asiasta Helsingin hovioikeuteen. Valitus perustui väitteeseen käräjäoikeuden väärin toimittamasta näytön arvioinnista. Hovioikeus tarkasteli kokonaisuutena asiassa esiteltyä teknistä todistusaineistoa ja muuta todistusaineistoa, kuten todistajalausuntoa ja todisteena ollutta syytetyn ja uhrin välistä viestittelyä. IP-osoitteeseen liittyvästä todistelussa hovioikeus lausui, että asiassa IP-osoitteesta annettu selvitys ei puhunut vastaajan syyllisyyden puolesta tai sitä vastaan,[178] joten tuomio perustui muuhun asiassa esitettyyn, kuin yksinomaan tekniseen todistusaineistoon. Hovioikeus katsoi, ettei asiassa esitetyn aineiston perusteella syytetyn syyllisyydestä jäänyt järkevää epäilystä ja tuomitsi syytetyn tietomurrosta. Esitetyn perusteella on katsottavissa, että asiassa esitettävä tekninenkin todistusaineisto tulee olla yhdistettävissä rikoksentekijään huomattavalla varmuudella.

[176] Riekkinen, 2020, s. 1001.
[177] Helsingin KO, R 19/609, s. 5.
[178] Helsingin HO, R 20/523, s. 6.

Pakkokeinolain 8 luvun 20 §:n mukaan tietokoneessa tai muussa vastaavassa teknisessä laitteessa tapahtuva etsintä on laite-etsintää. Laite-etsinnän edellytyksenä on pakkokeinolain 8 luvun 21 §:n 1 momentin perusteella, että epäillystä rikoksesta on säädetty ankarimpana rangaistuksena vähintään kuusi kuukautta vankeutta. Tietomurrosta säädetty ankarin rangaistus on rikoslain 38 luvun 8 §:n mukaan kaksi vuotta vankeutta. Törkeän tietomurron rangaistusmaksimi rikoslain 38 luvun 8a §:n perusteella on kolme vuotta, joten laite-etsintä voidaan kohdistaa tietomurron tai törkeän tietomurron epäilyyn. Laite-etsintä voidaan ulottaa myös alle 18-vuotiaan tekemään tietomurtoon tai tietomurron yritykseen.

Laite-etsinnän kannalta ongelmaksi voi kuitenkin muodostua takavarikoidun digitaalisessa muodossa olevan aineiston salaus. Esimerkiksi matkapuhelimen salaus numeroyhdistelmällä tai sormenjäljellä on nykyisin mahdollista ja yleistä. Pakkokeinolain 8 luvun 23 §:ssä tietojärjestelmän haltijalle on määrätty tietojenantovelvollisuus tarpeellisten salasanojen ja vastaavien tietojen toimittamiseen laite-etsinnän suorittamista varten. Suomessa epäillyllä on kuitenkin itsekriminointisuoja, joten häntä ei voida velvoittaa luovuttamaan salasanaa tai purkamaan jonkun tietolaitteen salausta.

Toisaalta mikäli salaus on purettavissa biometrisellä tunnisteella, kuten esimerkiksi sormenjäljellä, pakkokeinolain 9 luvun 3 §:n mukainen henkilötuntomerkkien ottaminen on oikeuskäytännössä hyväksytty ulottumaan myös biometrisen tunnisteen käyttämiseen salauksen purkamiseksi.[179] Pakkokeinolain kannalta on merkittävää huomioida myös pakkokeinolain 1 luvun 2 §:ssä määritelty suhteellisuusperiaate. Pakkokeinoa ei saa käyttää, jos sitä ei voi pitää puolustettavana rikoksen selvittämisen kannalta, ottaen huomioon rikoksen törkeysaste ja pakkokeinosta eri osapuolille aiheutuvat mahdolliset oikeudenloukkaukset. Laite-etsinnällä ei saa myöskään kiertää muiden pakkokeinojen, kuten televalvonnan ja teknisen tarkkailun korkeampia vaatimuksia.[180] Toisaalta tekninen tutkinta on vaikeaa ilman laite-etsintää ja takavarikkoa, kun kyseessä on digitaaliseen ympäristöön liitännäinen tietomurtorikos.

Perinteisen salauksen, jonka purkaminen perustuu esimerkiksi salasanaan, tutkintaan ja purkamiseen liittyvää määräystä ei ole sisällytetty suoraan pakkokeinolakiin. Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus käsittelee asiaa sopimuksen 19 artiklassa. Artiklan 1 kappaleen mukaan sopimuspuolen asiassa toimivaltaisella viranomaisella on oltava joko

[179] Riekkinen, 2019, s. 280.
[180] Fredman, ym., 2020, s. 1039.

etsinnällä tai muulla vastaavalla tavalla valtuudet hankkia pääsy tietojärjestelmään ja sen osaan, dataan ja tietovälineeseen.

Laite-etsinnän lisäksi esitutkinnan aikana voidaan määrätä takavarikosta tutkinnan toimittamiseksi. Pakkokeinolain 7 luku sisältää takavarikkoa koskevia säännöksiä. Pakkokeinolain 7 luvun 1 §:n mukaan esine, omaisuus tai asiakirja voidaan takavarikoida, jos voidaan olettaa, että sitä voidaan käyttää todisteena rikosasiassa. Pykälän 2 momentti määrää myös, että asiakirjan takavarikosta säädettyä voidaan soveltaa myös teknisellä laitteella tai vastaavassa tietojärjestelmässä olevaan tietoon. Pykälän 3 momentti määrää, että esineestä voidaan myös irrottaa osa takavarikoitavaksi todisteena käyttämistä varten. Tämän myötä erilaiset tallennusmediat, kuten kiintolevyt ovat takavarikoitavissa kokonaisen tietokoneen sijasta.

Oikeuskirjallisuudessa on todettu, että esitutkinnassa on teknisestä tallenteesta mahdollista valmistaa kopio, jolloin takavarikko kohdistuu kopioon, eikä alkuperäiseen materiaaliin, johon kopio rinnastuu.[181] Kopion tutkinnasta aiheutuu lähtökohtaisesti vähemmän haittaa, kuin alkuperäisen kappaleen takavarikoinnista esitutkinnan suorittamiseksi. Suhteellisuusperiaatteen nojalla takavarikon tulisi olla järkevässä suhteessa sen aiheuttamiin haittoihin. Tietokonelaitteistoon kohdistuvien takavarikkojen on kuitenkin kritisoitu kohdentuvan myös sellaisiin osiin tietokonelaitteistoa, josta ei ole hyötyä todistelussa.[182] Poliisin tutkittavaksi on haettu vähintään täysi tietokoneen keskusyksikkö, mutta muutkin lisälaitteet, joista ei lähtökohtaisesti ole hyötyä rikoksen tutkinnassa.

5.2 Salaisista pakkokeinoista

Pakkokeinolain 10 luku määrittelee rikosten tutkinnassa käytettävät salaiset pakkokeinot. Pakkokeinolain 10 luvun 1 § luettelee salaiset pakkokeinot, joihin kuuluvat esimerkiksi telekuuntelu, peitelty tiedonhankinta, teleosoitteen yksilöintitietojen hankinta ja peitetoiminta. Salaisten pakkokeinojen osalta voidaan ensimmäisenä todeta, että tietomurto tai törkeä tietomurto eivät kuulu rikoksiin, joiden perusteella esitutkintaviranomaiselle voidaan antaa pakkokeinolain 10 luvun 3 §:n perusteella lupa telekuunteluun. Telekuuntelu tunkeutuu salaisten pakkokeinojen joukosta kaikista suurimmalla painolla henkilön yksityiselämän suojan alueelle, joka on

[181] Helminen, ym., 2014, s. 970.
[182] Oksanen, ym., 2008, s. 220.

määritelty kansallisella tasolla perustuslain 10 §:ssä sekä kansainvälisesti esimerkiksi Euroopan unionin perusoikeuskirjan 7 artiklassa. Tämän myötä telekuuntelun käyttö on rajattu määriteltyihin rikoksiin.

Perustuslakivaliokunta arvioi televalvonnan edellytyksiä tietojenkäsittelyjärjestelmään kohdistuvien rikosten kannalta pakkokeinolain kokonaisuudistusta käsittelevässä lausunnossa. Valiokunta katsoi lausunnossaan, että vaikka tällaisia rikoksia ei pystytä useinkaan selvittämään ilman televalvontaa, eivät kaikki tietojenkäsittelyjärjestelmään kohdistuvat rikokset, kuten esimerkiksi tietomurto, ole yksilön tai yhteiskunnan turvallisuutta tai kotirauhaa vaarantavia rikoksia. Rikoksen tulee vähintään vaarantaa yksilön tai yhteiskunnan turvallisuutta tai kotirauhaa, jotta edellytykset käyttää telekuuntelua ovat olemassa.[183] Oikeustieteen tohtori *Tuomas Metsäranta* esittää väitöskirjassaan ”Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja”, että tietojärjestelmiin liittyvät rikokset voivat olla jopa yhteiskunnan turvallisuutta vaarantavia rikoksia ja että tietojenkäsittelyjärjestelmiin kohdistuvat rikokset tulisi jotenkin ottaa huomioon televalvonnan kannalta.[184]

Törkeä datavahingonteko on määritelty pakkokeinolain 10 luvun 3 §:ssä rikokseksi, jonka perusteella esitutkintaviranomaiselle voidaan antaa lupa telekuunteluun. Verrattaessa tietomurtoa tai törkeää tietomurtoa törkeään datavahingontekoon, voidaan perustuslakivaliokunnan näkökulma katsoa perustelluksi. Tietomurtoa koskevalla rikossääntelyllä kyllä suojataan kotirauhaan verrattavissa olevaa tietojenkäsittelyrauhaa, mutta tietomurto eri vakavuusasteineen ei ole katsottavissa yksilön tai yhteiskunnan turvallisuutta vaarantavaksi rikokseksi. Kyseessä on järjestelmään luvaton tunkeutuminen, jonka soveltamisalaan ei kuulu järjestelmässä käsiteltävien tietojen tarkastelu, tuhoaminen tai muu tiedon vaarantuminen eheyden kannalta, jolla voi olla yksilöön tai yhteiskuntaan vaikutuksia.

Mikäli järjestelmä tunkeutumisen jälkeen joutuukin muiden rikosten kohteeksi, asia arvioidaan kyseisten rikostunnusmerkistöjen kannalta uudelleen. Rajanveto salaisten pakkokeinojen käytölle on määriteltävissä yhteiskunnan intressin avulla. Intressi selvittää rikoksia ei voi olla niin vahva, että salaisia pakkokeinoja tulisi käyttää tavanomaisten ja sitä vähäisempien rikosten

[183] PeVL 32/2013 vp., s. 4.
[184] Metsäranta, 2015, s. 96.

tutkintaan,[185] erityisesti ottaen huomioon tason, jolla tutkintakeino ulottuu henkilön yksityisyydensuojan ja luottamuksellisen viestin suojan alueelle.

Poikkeuksena asiasta on kuitenkin pakkokeinolain 10 luvun 7 §, jonka perusteella televalvontaa suoritetaan teleosoitteen tai telepäätelaitteen haltijan suostumuksella. Esitutkintaviranomainen saa kohdistaa televalvontaa rikoksesta epäillyn, asianomistajan, todistajan tai muun henkilön suostumuksella tämän hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen, mikäli yksi määrätyistä kriteereistä täyttyy. Ensimmäinen kriteeri koskee rikosta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Vaatimus täyttyy sekä tietomurron että törkeän tietomurron rikossäännösten kohdalla. Pakkokeino voisi olla relevantti esimerkiksi tilanteessa, jossa tietojärjestelmän haltijan suostumuksella pyritään aiempien lokitietojen lisäksi selvittämään mahdollisesti vielä käynnissä olevaa tietojärjestelmään tunkeutumista.

Asiassa tulee kuitenkin huomioida, että telekuuntelu ja -valvonta ovat vain kaksi pakkokeinolain määrittelemistä yli kymmenestä salaisesta pakkokeinosta. Tietomurtorikosten tutkinnan kannalta yksi relevantti salainen pakkokeino on pakkokeinolain 10 luvun 25 §:n määrittelemä teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, jonka kriteerinä on rikosepäily, josta säädetty ankarin rangaistus on vähintään vuosi vankeutta. Rangaistusvaatimus täyttyy sekä tietomurron että törkeän tietomurron rikossäännösten kohdalla.

Poliisille on annettu pakkokeinolain 10 luvun 27 §:n 4 momentin perusteella oikeus suorittaa peitetoimintaa tietoverkossa, jos henkilöä epäillään rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Peitetoiminnassa henkilöön tai hänen toimintaansa kohdistetaan suunnitelmallista tiedonhankintaa käyttämällä keinona soluttautumista. Tiedonhankinnan paljastumisen estämiseksi pakkokeinolain 10 luvun 27 §:n 1 momentti määrittelee soluttautumisessa mahdolliseksi käyttää vääriä, harhauttavia tai peiteltyjä tietoja. Fyysisessä ympäristössä tapahtuvan peitetoiminnan kriteerit ovat korkeammat, sen rajoittuessa ainoastaan tiettyihin ennalta määriteltyihin rikoksiin. Mikäli peitetoimintaa on tarpeen tehdä sekä fyysisessä että digitaalisessa ympäristössä, tulee fyysisessä ympäristössä tapahtuvan peitetoiminnan kriteerien täyttyä.[186]

[185] Metsäranta, 2015, s. 111.
[186] Fredman, ym., 2020, s. 1132.

Peitetoiminnassa poliisi tai muu viranomainen ei tuo ilmi omaa asemaansa viranomaisena. Peitetoiminnan kohdalla on kuitenkin havainnoitava pakkokeinolain 10 luvun 28 §:n mukainen rikoksentekokielto, poliisi ei saa tehdä itse rikoksia eikä tehdä aloitetta rikoksen tekemiseen. Tämä huomioiden verkossa tapahtuva peitetoiminta on mahdollista tietomurtorikosten kohdalla. Pakkokeinolaki on kuitenkin säädetty lähtökohtaisesti reaalimaailman toimivaltuudet ja toiminta huomioiden, mikä voi aiheuttaa ongelmia toimittaessa tietoverkossa. Fyysisessä ympäristössä menestyksekkään peitetoiminnan edellytykset ovat vähäisemmät. Pelkkä henkilön tavanomaisesta poikkeava pukeutuminen voi olla toimivan peitetoiminnan ainoa edellytys.[187]

Tietoverkossa toimiminen vaatii yleensä käyttäjätilin, olipa keskustelualustana sosiaalisen median palvelu tai keskustelufoorumi. Pakkokeinolain 10 luvun 47 §:n 2 momentin perusteella väärien, harhauttavien tai peiteltyjen tietojen käyttö on kuitenkin sallittua silloin, kun se on välttämätöntä jo toteutetun, käynnissä olevan tai tulevaisuudessa toteutettavan salaisen pakkokeinon käytön suojaamiseksi. Lainsäädäntö ei anna perusteita tulevaisuudessa toteutettavan salaisen pakkokeinon suojaamiselle, joten on epäselvää, missä määrin poliisi tai muu peitetoiminnassa toimivaltainen viranomainen voi valmistella pätevää peitetoimintaidentiteettiä tietoverkoissa, jos siihen käytettävää rikosta ei ole yksilöitävissä tai sitä ei ole vielä tapahtunutkaan. Erityisesti sosiaalisessa mediassa uskottavan käyttäjäprofiilin rakentaminen vie aikaa.[188]

Rikoksen selvittämisen kannalta on merkittävää lokitietojen saavutettavuus ja mahdollinen IP-osoitteen perusteella suoritettava yksilöinti, yhdistettynä teleoperaattoreilta saataviin tietoihin poliisilain tiedonsaantioikeuden turvin. Nykyisin internetin käyttäjän on mahdollista hankkia itselleen käyttöön VPN-palvelu, jonka tarkoituksena on häivyttää IP-osoitteen seurantatiedot kierrättämällä käyttäjän internetliikenne useamman välityspalvelimen kautta. VPN on lyhenne englanninkielisestä käsitteestä ”Virtual private network”. Lopputuloksena kohteena oleva tietojärjestelmä ei tiedä järjestelmän tai verkkosivun käyttäjän oikeaa identiteettiä. VPN-palvelun käyttö ei ole kriminalisoitua, mutta sitä käyttämällä on mahdollista häivyttää tietoverkossa tapahtuvan rikoksen jälkiä.

VPN-palvelun toteuttama anonymisointi on haasteellista rikosten selvittämisen kannalta. Tämän myötä esitutkintaviranomaisella voi olla intressi murtaa VPN-palvelun anonymiteetti. VPN-palvelun ylläpitäjä pystyy asiakas- ja välitystietoja yhdistelemällä selvittämään

[187] Forss, ym., 2017, s. 22.
[188] Forss, ym., 2017, s. 23.

anonymisoidun käyttäjän identiteetin. Suomessa asiaa on käsitelty korkeimmassa oikeudessa tapauksessa KKO 2022:23. Tapauksessa keskusrikospoliisi oli takavarikoinut vieraan valtion oikeusapupyyntöön liittyen suomalaiselta VPN-palveluntarjoajalta lokitietoja pakkokeinolain nojalla. Lokitietojen perusteella rikoksesta epäillyn henkilöllisyys oli mahdollista selvittää. Korkeimman oikeuden kysymyksenasettelussa oli kyse siitä, olivatko VPN-palveluntarjoajan lokitiedot sellaisia tietoja, jotka olivat takavarikoitavissa pakkokeinolain 7 luvun säännösten nojalla ja oliko niitä mahdollista käyttää rikoksen selvittämiseen. Kysymyksenasettelu poikkesi siis teleyrityksen asiakastietojen käsitteestä ja pakkokeinolain 10 luvun 25 §:n poliisin oikeudesta hankkia teleosoitteen tai telepäätelaitteen yksilöintitietoja, kun takavarikon kohteena oleva taho ei ollut suoraan viestinnän palveluntarjoaja.

Korkein oikeus katsoi ratkaisusta ilmenevillä perusteilla, että pakkokeinolain 7 luvun 4 §:n telekuunteluun ja televalvontaan liittyvä teleyrityksen ja yhteisötilaajan takavarikoimis- ja jäljentämiskielto koski myös viestinnän välittäjiä. VPN-palveluntarjoaja oli tapauksessa viestinnän välittäjä. Korkein oikeus katsoi pakkokeinolain kieltosäännöksen koskevan myös muita kuin nimenomaisesti laissa säänneltyjä tahoja, mikä esti tapauksessa takavarikon käyttämisen telepakkokeinojen korkeiden vaatimusten kiertämiseen. Varsinaisen takavarikkokiellon lisäksi korkein oikeus otti kantaa VPN-palveluntarjoajan lokitietojen asemaan. Takavarikoiduissa lokitiedoissa oli kyse IP-osoitteista, jotka olivat yhdistettävissä internetliittymän haltijaan, joten VPN-palveluntarjoajalta takavarikoidut lokitiedot olivat pakkokeinolain tarkoittamia tunnistetietoja. Myös tällä perusteella lokitietojen takavarikointi katsottiin kielletyksi pakkokeinolain 7 luvun 4 §:n 1 momentin nojalla.

Korkeimman oikeuden tuomion perusteella, mikäli internetin käyttäjä on suojannut tietonsa VPN-palvelulla, poliisin tiedonsaantioikeudet kaventuvat huomattavasti. VPN-palveluntarjoaja on sähköisen viestinnän välittäjä, eikä viestinnän osapuoli, toisin kuin teleyritys tai yhteisötilaaja. Korkeimman oikeuden tuomio laajentaa pakkokeinolain 7 luvun 4 §:n soveltamisalaa teleyrityksistä ja yhteisötilaajista viestinnän välittäjiin. Lisäksi päätöksen perusteella viestinnän välittäjän lokitiedot kuuluvat pakkokeinolain 7 luvun 4 §:n tarkoittamiin tunnistamistietoihin. Tietoverkossa tapahtuvia tai tietoverkkoliitännäisiä rikoksia selvittävän tahon kannalta päätös on negatiivinen, toisaalta yksilötasolla korkeimman oikeuden päätöksen on katsottavissa lisäävän henkilön yksityisyyden suojaa, olipa kyse sitten luvallisesta tai luvattomasta toiminnasta tietoverkossa.

5.3 Kansainvälinen liityntä tietomurtorikoksissa

Kansallisen tietoverkkorikollisuuden lisäksi on huomioitava tietomurtorikosten kansainvälinen näkökulma tietomurtojen tutkinnan ja tuomitsemisen kannalta. Digitaalisen ympäristön myötä rikoksen tekijä voi sijaita toisella puolella maapalloa, jolloin tarkastelun kohteena voi olla myös rikoksesta epäillyn henkilön luovuttaminen toiseen maahan. Merkitystä on myös digitaalisen aineiston fyysisen sijainnin määrittelyllä. Suvereniteettiperiaatteen perusteella jokaisen valtion toimintavalta rajoittuu lähtökohtaisesti oman valtion sisälle, myös suoritettaessa rikostutkintaa.[189] Nykyisin tarjolla olevat digitaaliset palvelut voivat olla pilvipalveluja, joissa palveluntarjoaja ja tietojen fyysinen sijainti on yhdessä valtiossa, mutta palveluja voidaan tarjota saman palveluntarjoajan toimesta useassa eri maassa. Miten esitutkintaviranomainen voi lainsäädännön kannalta kestävällä tavalla ja oikeudenmukaisesti suorittaa rikoksen tutkintaa, jos tutkinnan kohteena olevan henkilön käyttäjätili tai tallentamat tiedot sijaitsevat toisessa maassa. Merkitystä on myös sillä, mikä on palveluntarjoajan kotipaikka.

Euroopan unionin rikosoikeudellisen yhteistyön oikeusperusta on sopimuksessa Euroopan unionin toiminnasta, jossa määritellään päätavoitteiksi aineellisen rikoslainsäädännön lähentäminen ja vastavuoroinen tunnustaminen. Aineellisen rikoslainsäädännön lähentämisen voidaan Suomen näkökulmasta katsoa tarkoittavan muutoksia tulevaisuudessa rikosoikeuden erityisen osaan.[190] Aineellisen rikoslainsäädännön lähentämisen oikeusperusta on SEU 83 artiklassa. Sen mukaan lähentäminen koskee sopimuksessa määriteltyjä erityisen vakavan rikollisuuden aloja, joilla on rajat ylittävä aspekti tai mikäli niiden torjuminen on erityisen tarpeellista. Tietokonerikollisuus on määritelty sopimuksessa rikosalaksi, jossa unionitason lähentäminen on tarpeellista. Lähentäminen on ilmentynyt yllä mainittuina puitepäätöksinä ja direktiiveinä. SEU 82 artikla määrittelee vastavuoroisen tunnustamisen periaatteen, jolla Euroopan unionissa tuomioistuinten tuomiot ja oikeusviranomaisen päätökset tunnustetaan vastavuoroisesti. Vastavuoroisessa tunnustamisessa lähtökohtana on suoraviivaisempi yhteydenpito asioita kansallisella tasolla käsittelevien viranomaisten välillä, kun perinteisesti luovuttamispyynnöt käsitellään hallinnollisten keskusviranomaisten kautta.[191]

[189] Oerlemans, 2015, s. 295.
[190] Melander, 2015, s. 79.
[191] Kimpimäki, 2017, s. 143.

Vastavuoroinen tunnustaminen ei ole kuitenkaan varauksetonta Euroopan unionin jäsenvaltioiden kesken, vaan täytäntöönpanosta kieltäytymisestä on jätetty varaumia puitepäätöksessä eurooppalaisesta pidätysmääräyksestä ja jäsenmaiden välisestä luovuttamismenettelystä.[192] Yhtenä vastavuoroisen tunnustamisen kriteerinä on kaksoisrangaistavuuden tutkimus, teko tulee olla rangaistava sekä luovutusta pyytävässä että pyynnön vastaanottaneessa maassa. Puitepäätöksessä 2002/584/YOS kuitenkin määritellään 2 artiklan 2 kohdassa rikoksia, joissa kaksoisrangaistavuutta ei tarvitse tutkia, mikäli pidätysmääräyksen antaneessa valtiossa asiasta voi seurata vapaudenmenetyksen käsittävä rangaistus, jonka enimmäisrangaistus on vähintään kolme vuotta. 2 artiklan 2 kohdan määrittelemiin rikoksiin kuuluu tietoverkkorikollisuus. Kansallisella tasolla unionimaiden välisestä luovutuksesta on säädetty laissa rikoksen johdosta tapahtuvasta luovuttamisesta Suomen ja muiden Euroopan unionin jäsenvaltioiden välillä (1286/2003).

Kyberrikosten kansainvälisen aspektin kannalta merkittävä sopimus on Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (ETS 185), johon viitataan myös Budapestin sopimuksena tai kyberrikollisuutta koskevana sopimuksena. Tietoverkkorikollisuutta koskeva yleissopimus sisältää III luvussa artiklat 27–35, jotka määrittelevät sopimusosapuolet velvolliseksi antamaan toisilleen keskinäistä oikeusapua erilaisissa tilanteissa.

Nimenomaisesti tietoverkkorikollisuutta koskevan yleissopimuksen lisäksi erityisesti Euroopan unionin jäsenmaiden ja Euroopan neuvoston maiden kesken on sopimuksin määriteltyä yhteistyömenettelyä oikeusavusta yleisesti rikosasioissa. Kansallisen lain tasolla asiaa on määritelty kansainvälisestä oikeusavusta rikosasioissa annetun lain perusteella (4/1994). Lain kannalta on havaittava, että se ei voi määritellä minkälaista apua toinen valtio voi antaa Suomelle rikosasiassa, vaan sääntelyn kohteena ovat Suomen toimet annettaessa oikeusapua, sisältäen menettelyllisiä säännöksiä oikeusavun pyytämisestä toiselta valtiolta. Kohdemaan lainsäädäntö määrittelee oman lainsäädäntönsä puitteissa, millaista apua vastapuolella olevalle valtiolle annetaan.

Mikäli valtio ei ole esimerkiksi hyväksynyt tai ratifioinut Budapestin sopimusta, ei sopimuksessa määritellyillä keinoilla oikeusavusta ole merkitystä. Sopimus edesauttaa rajat ylittävien tietomurtotapausten tutkintaa vain sopimuksen ratifioineiden tai hyväksyneiden maiden välillä. Koska esimerkiksi Kiina tai Venäjä eivät ole Budapestin sopimuksen sopimusosapuolia,[193] käytännössä tietoverkkorikosten tutkintaan liittyvän kansainvälisen yhteistyön onnistuminen on

[192] Kimpimäki, 2017, s. 142.
[193] Clough, 2014, s. 727.

hyvin riippuvaista kohdemaasta, eikä läheskään kaikkia rajat ylittäviä tietomurtoepäilyjä ole mahdollista selvittää nykyisten sopimukseen liittyneiden maiden kesken.

Tietomurtorikosten tutkintaa vaikeuttaa ensisijaisesti se, ettei tietoverkkoja ole mahdollista säännellä eikä hallita keskitetysti. Myös digitaalinen toimintaympäristö asettaa omat erityisyytensä rikospaikkatutkinnalle. Fyysisessä ympäristössä valtioiden rajat ovat selkeästi määriteltyjä. Internet on rajat ylittävä ympäristö, jota ei kuitenkaan hallinnoi mikään yksittäinen taho. Internetin ja muiden tietoverkkojen laitteisto on sijoittuneena johonkin maahan ja sen lainsäädännön alaisuuteen. Murtautuja voi sijaita laitteiston näkökulmasta tarkasteltuna toisella puolella maapalloa ja eri valtion lainsäädännön ja toimivallan alueella. Tämän seurauksena rikostutkinnassa voi tulla kyseeseen rajat ylittävä aspekti, joka tekee tutkinnasta haastavampaa. Valtion suvereniteetti on yleinen kansainvälinen oikeusperiaate, joka sisältyy esimerkiksi Yhdistyneiden Kansakuntien peruskirjaan.[194]

Perinteisesti lainsäädännössä tuomiovalta on määriteltävissä maan rajojen perusteella. Alueperiaatteen nojalla valtiolla on toimivalta sen alueella tehtyihin rikoksiin. Myös maan yläpuolella sijaitseva ilmatila on määritelty oikeuskirjallisuudessa maanomistajan ja valtion määräysvallan alaisuuteen.[195] Valtion lainsäädäntö- ja lainkäyttövalta ovat vahvasti toisiinsa liitännäisiä tarkastellessa rikosasioita. Valtion tuomioistuin soveltaa lähtökohtaisesti oman maansa oikeutta, lisäksi oikeuden täytäntöönpanotoimet tapahtuvat oletusarvoisesti vain valtion omalla alueella.[196] Rikoslain 1 luvun 1 §:n perusteella Suomessa tehtyyn rikokseen sovelletaan Suomen lakia. Poikkeus rikoslain 1 luvun 1 §:n suvereniteettiin on määriteltynä rikoslain 1 luvun 15 §:ssä. Velvoittavista kansainvälisistä sopimuksista ja muista säädöksistä johtuvia rajoituksia, jotka rajoittavat Suomen rikosoikeuden soveltamisalaa, tulee noudattaa.

Alueperiaate ei ole kuitenkaan ainoa toimivaltaperuste, jonka perusteella valtion tuomiovalta on nykyisin määriteltävissä. Muita kansainvälisiä valtion rikosoikeudellisen toimivallan periaatteita ovat lippuperiaate, aktiivinen ja passiivinen persoonallisuusperiaate, reaaliperiaate, sijaislainkäytön periaate ja universaaliperiaate.[197] Periaatteissa on kyse valtion tuomiovallan laajentamisesta rikoksiin, joita on tarpeen käsitellä kyseisen maan tuomioistuimessa, vaikka niillä

[194] Yhdistyneiden Kansakuntien peruskirja, 1/1956, 2 artikla.
[195] Li, 2008, s. 110.
[196] Frände, 2012, s. 291.
[197] Kimpimäki, 2015, s. 539.

olisi heikko liityntä tai ei ollenkaan liityntää kyseisen valtioon.[198] Persoonallisuusperiaatteissa on kyse siitä, että rikoksen on tehnyt maan kansalainen tai rikos on kohdistunut kyseisen maan kansalaiseen. Reaaliperiaatteessa katsotaan valtion olevan oikeutettu suojelemaan itseään ja intressejään,[199] universaaliperiaatteessa on kyse kansainvälisistä, erikseen sopimuksin määritellyistä kansainvälisistä rikoksista, kuten joukkotuhonnasta tai aluksen kaappauksesta, joiden tuomitseminen on mahdollista myös muualla kuin tekopaikan valtiossa siihen kuuluvan kansainvälisen intressin myötä.[200] Tietomurtorikokset eivät kuulu universaaliperiaatteen soveltamisalaan.

Lippuperiaate määritellään rikoslain 1 luvun 2 §:ssä. Suomalaisessa aluksessa tai ilma-aluksessa tehtyihin rikoksiin sovelletaan Suomen lakia. Toisin sanoen valtion tuomiovalta ulottuu sen rekistereihin merkittyihin aluksiin, jos ne ovat muiden valtioiden toimivaltaan kuulumattomalla alueella.[201] Sijaislainkäytön periaatteessa on kyse tilanteesta, missä valtio ei voi itse käyttää tuomiovaltaansa ja pyytää toista valtiota käsittelemään rikostapauksen, vaikka valtiolla ei olisi lainkaan intressiä asiassa.[202]

Fyysisessä ympäristössä tapahtuvassa rikollisuudessa rajat ylittävän liitynnän voidaan katsoa rajoittuvan yleensä kahden valtion alueelle. Digitaalisessa rikosympäristössä rikoksen tekijä ja uhri voivat sijaita eri valtioissa, lisäksi myös tietojärjestelmän sisältävä palvelin tai muu vastaava tietolaite voi sijaita osapuoliin nähden kolmannessa valtiossa. Ubikviteettiteorian perusteella teon tunnusmerkistön mukainen tekopaikka voi olla siellä, missä tekoon ryhdyttiin, tai samanaikaisesti siellä, missä seuraus ilmenee.[203] Tietomurtorikosten osalta ubikviteettiteorian mukainen tilanne voi olla hyvin mahdollinen, rajat ylittävä luonne huomioiden. Kansallisessa lainsäädännössä rikoslain 1 luvun 10 §:n perusteella rikos katsotaan tehdyksi yhtäaikaisesti siellä, missä rikollinen teko on suoritettu, että myös siellä, missä tunnusmerkistön mukainen seuraus on ilmennyt. Lähtökohtaisesti tietomurtorikos olisi siis mahdollista tuomita joko hakkerin sijaintipaikan tai kohteena olevan tietojärjestelmän sijainnin mukaisesti, jolloin toimivalta rikoksen selvittämiseen ja tuomitsemiseen voi olla useammalla valtiolla.

[198] Kimpimäki, 2015, s. 540.
[199] Kimpimäki, 2015, s. 556.
[200] Frände, 2012, s. 296.
[201] Frände, 2012, s. 294.
[202] Kimpimäki, 2015, s. 566.
[203] Kimpimäki, 2015, s. 542.

Asialla on merkitystä *ne bis in idem* -periaatteen kannalta. Periaatteen mukaan ketään ei saa tutkia ja rangaista useampaan kertaan rikoksesta, josta hänet on jo tuomittu syylliseksi tai vapautettu. Osaltaan periaate ilmenee kansallisessa lainsäädännössä perustuslain 21 §:n vaatimuksesta oikeudenmukaisesta oikeudenkäynnistä. Euroopan ihmisoikeussopimuksen seitsemännen lisäpöytäkirjan neljäs artikla[204] sisältää *ne bis in idem* -vaatimuksen suoraan todettuna vaatimuksena, joskin vaatimus koskee vain saman valtion tuomiovaltaa. Euroopan unionin sisällä on kuitenkin tavoitteita sitoutua valtioiden välisten rikosoikeudellisten toimivaltojen tunnustamiseen ja yhteensovittamiseen. Euroopan unionin puitepäätös 2009/948/YOS pyrkii ratkaisemaan toimivaltaristiriitoja jäsenvaltioiden kesken rikosoikeudellisissa tapauksissa. Sen mukaan, jos jäsenvaltiolle käy ilmi, että toisessa jäsenvaltiossa on käynnissä rinnakkainen menettely samasta asiasta, valtioiden viranomaisten tulisi käynnistää neuvottelut asiasta. Puitepäätös ei kuitenkaan velvoita toista valtiota luopumaan lainkäyttövallasta neuvotteluista ja niiden lopputuloksesta riippumatta.[205]

Rikoslain 1 luvun 13 § määrää, ettei Suomessa saa nostaa syytettä teosta, josta on jo tekopaikan valtiossa tai toisessa Euroopan unionin jäsenvaltiossa annettu lainvoimainen tuomio. Säännös ei ole sellaisenaan tyhjentävä, vaan lainsäätäjä on jättänyt valtakunnansyyttäjälle mahdollisuuden määrätä syytteen tiettyjen rikosten kohdalla määrättyjen kriteerien täyttyessä. Rikoksen tulee kohdistua Suomeen, sen tulee olla virka- tai sotilasrikos tai kansainvälinen rikos. Rikos voidaan myös katsoa tehdyksi Suomessa. Rikoksen katsotaan rikoslain 1 luvun 3 §:n perusteella kohdistuvan Suomeen, jos se on maan- tai valtionpetosrikos, kohdistuu Suomen viranomaiseen tai teolla muutoin vakavasti loukataan Suomen valtiollisia, sotilaallisia tai taloudellisia oikeuksia tai etuuksia. Tietomurtorikollisuuden kannalta tilanne voi todennäköisimmin tulla tarkasteltavaksi ainoastaan, mikäli tietomurto kohdistuu Suomen viranomaiseen tai jos rikos katsotaan tehdyksi Suomessa. Viitaten perustuslakivaliokunnan lausunnon tarkasteluun salaisten pakkokeinojen soveltamisesta tietomurtorikoksiin, tietomurto ei ole katsottavissa yhteiskunnan turvallisuutta merkittävästi vaarantavaksi rikokseksi.[206]

On siis arvioitavissa, että kansainvälisestä näkökulmasta tarkasteltuna valtioilla ei ole suoraan sitovaa velvoitetta noudattaa *ne bis in idem* -periaatetta rajat ylittävässä tietomurtorikoksessa, mikäli ne eivät itse halua sitä noudattaa. Rajoituksia tälle valinnanvapaudelle Suomen

[204] SopS 63/1999.
[205] Kimpimäki, 2015, s. 575.
[206] PeVL 66/2010 vp., s. 7.

näkökulmasta tulee Euroopan unionin sääntelystä. Toisaalta Suomen rikoslaki sisältää sääntelyn tilanteisiin, joissa samaa asiaa on käsitelty jo rikoksen tekopaikan valtiossa tai toisessa unionijäsenen tuomioistuimessa.

Unioniliitännäisyyden osalta on myös arvioitavissa, ettei Iso-Britannian ero Euroopan unionista omalta osaltaan helpota kyberrikollisuuden tutkintaa tulevaisuudessa tilanteissa, joissa Iso-Britannia on yhtenä osapuolena. Huolimatta siitä, että Euroopan neuvoston kyberrikollisuutta koskeva yleissopimus on unionioikeudesta erillinen instrumentti, johon Iso-Britannia on toistaiseksi sitoutunut, on unionin rikostorjunnassa instrumentteja, joissa maa ei ole jatkossa mukana Brexitin myötä.

6 Lopuksi

Tutkielman tutkimuskysymyksenä oli selvittää mitä haasteita rikoslaissa määritellyn tietomurtorikoksen ja törkeän tietomurtorikoksen määrittelyyn, tutkintaan ja tuomitsemiseen liittyy. Tarkoituksena oli selvittää, mitä tietomurtorikokset ovat, mihin niiden sääntely perustuu, miten rikoslain yleiset opit tulee huomioida käsiteltäessä tietomurtorikoksia, miten tietomurron rikossäännökset ovat lainkonkurrenssissa muun lainsäädännön suhteen ja mitä haasteita tietomurtorikosten tutkintaan liittyy.

Perusväitteenä on esitettävissä, että tietomurtorikoksia koskeva rikossäännös on pysynyt teknisen kehityksen mukana. Tietomurron tekniikkaneutraali rikossäännös on sovellettavissa tapauksiin, joita ei ollut vielä mahdollista yksilöidä alkuperäisen rikossäännöksen kirjoitushetkellä. Tietomurtona on tuomittavissa tapaus, joka perustuu hyvin seikkaperäiseen teknisin apuvälinein suoritettavaan tietojärjestelmään tunkeutumiseen, tai vastaavasti käyttäjän heikkouksiin perustuviin tietomurtoihin.

Tietomurtorikoksissa asianosaisten piiri voi olla tietojärjestelmän ominaisuuksista riippuen laaja. Asianosaisiin kuuluvat oikeudettoman tunkeutumisen kohteeksi joutuneen tietojärjestelmän omistajan tai hallinnoijan lisäksi myös yksittäiset henkilöt, joiden käyttäjätileille tietomurroissa on tunkeuduttu. Mikäli tietomurron kohteeksi joutunut tietojärjestelmä on laaja, yksittäinen tietomurtorikoksen uhri voi joutua valvomaan itsenäisesti omaa rikosasiaansa. Koska tietomurto on määritelty asianomistajarikokseksi, rikoksen uhrilla on korostunut asema rikosprosessin etenemisen kannalta.

Tuomioiden perusteella on myös määriteltävissä tietomurtorikollisuuden kehittyminen käsitteestä 1.0 laajempaan someaikakauden 2.0 käsitteeseen. Hovi- ja käräjäoikeuksien materiaalin perusteella tietomurroissa, joista on annettu tuomio, ei ole nykypäivänä kyse niinkään pelkästään tietojärjestelmän oikeudettomasta käytöstä murtamalla turvajärjestely teknisesti hakkeroimalla, vaan tietojärjestelmää käytetään oikeudetta ennalta tiedossa olevan käyttäjätunnuksen ja salasanan avulla, tai vaihtamalla käyttäjätietoja. Saman tyyppiseen toimintaan voidaan katsoa kuuluvan myös käyttäjätietojen arvaaminen. Käsiteltävien tapausten perusteella rikoksen uhri on usein myös ennalta tekijän tiedossa. Rikosten tuomitsemisen kannalta merkittävää on

oikeuskäytännön tietojärjestelmän käsitteen ulottaminen sosiaalisen median tileihin. Lopulta sosiaalisessa mediassa käsiteltävä aineisto on pakkokeinolain määritelmän mukaista sähköiselle alustalle tallennettua dataa. Datan laadulla ei ole merkitystä tietomurron tunnusmerkistön kannalta.

Voidaan pohtia, onko oikeudeton tunkeutuminen sosiaalisen median tileille tietomurtorikollisuutta, joka on havaittavissa ja selvitettävissä kohtuullisella vaivannäöllä, suhteessa muun tyyppisiin tietojärjestelmään tunkeutumisiin. Sosiaalisen median palveluilla on myös omia turvajärjestelyitä, jotka reagoivat herkästi mahdollisiin tietomurron yrityksiin. Tällaisia ovat esimerkiksi palvelun lähettämät ilmoitukset käyttäjätilille kirjautumisesta uudesta laitteesta tai sijainnista,[207] jolloin myös rikoksen uhrin on mahdollista havaita tietomurto tai sen yritys nopeasti. Tietomurto sosiaalisen median palveluun on myös mahdollista havaita muuten kuin lokitietoja tarkkailemalla, mikäli rikoksen tekijä käyttää murrettua käyttäjätiliä ja tekee esimerkiksi tilapäivityksiä esiintymällä uhrina palvelussa. Huomionarvoista on, että käyttäjätilin käyttäminen tietomurron jälkeen voi synnyttää rikosvastuun muustakin kuin pelkästä tietomurrosta.

Rangaistavan tietomurron yrityksen edellytykset on määritelty oikeuskäytännössä alhaiseksi, ottaen huomioon, että itse rikoksen täyttymisen edellytyksenä on oikeudeton sisäänpääsy tai oikeudeton selon ottaminen järjestelmässä olevasta datasta. Teknisestä näkökulmasta vähäiseksi katsottava toimi, porttiskannaus, oli katsottu tapauksessa KKO 2003:36 rangaistavaksi tietomurron yritykseksi. Tarkastellessa avunantoa, vaatimus yhteisymmärryksessä toimimisesta ja avunantajan kyky arvioida päätekijän tulevaisuuden toimia ovat merkityksellisiä myös tietomurtorikosten kohdalla. Määrättäessä tietomurtorikoksesta rangaistusta, erityisesti suunnitelmallisuuden käyttämistä rangaistuksen koventamisperusteena tulee käyttää harkiten. Tietomurtorikokset edellyttävät yleisesti tarkasteltuna jo suunnitelmallisuutta onnistuakseen. Tutkielmassa tarkasteltujen tuomioiden perusteella tietomurrosta määrättävä rangaistus on useimmiten sakkorangaistus.

Konfiskaation käyttäminen turvaamistoimenpiteenä tietomurtorikoksissa ei vaikuta sellaisenaan tarkoituksenmukaiselta. Konfiskaatiolla ei ole suoranaista rikoksen uusimista estävää vaikutusta, kun rikoksessa käytettävä laite, kuten tietokone, on mahdollista hankkia uudelleen vähäisellä vaivannäöllä ja on kaksikäyttöisenä käytettävissä myös lailliseen toimintaan.

[207] Pohjanmaan käräjäoikeus R 18/1062, s. 8.

Välinekonfiskaation osalta tuleekin tarkastella määriteltyä mahdollisuutta käyttää konfiskaatiota tietokoneohjelmiin, ei pelkästään fyysisiin laitteisiin. Tarkastelun kohteina olleissa tapauksissa tietomurtorikoksista ei ole tuomittu konfiskaatiota. Tilanne voi olla erilainen, jos tietomurtoon käytettäisiin jotain erityislaitteistoa, jolle ei olisi määriteltävissä laillista käyttötarkoitusta.

Lainkonkurrenssin käsittely keskittyi pääasiassa erilaisten lainkonkurrenssitilanteiden tarkasteluun abstraktien tapahtumainkulkujen kautta. Tarkastellessa lainkonkurrenssia, tietomurron rikossäännöksessä lainkonkurrenssi on lähtökohtaisesti ratkaistu subsidiariteetilla, toisin sanoen kirjaamalla toissijaisuuslauseke rikossäännökseen. Pelkkä toissijaisuuslausekkeen tarkastelu ei kuitenkaan ole riittävä toimi konkurrenssitilanteen ratkaisemiseksi. Tarkastelu tulee ulottaa ensimmäisenä päällekkäisten rikossäännösten suojeluintresseihin. Merkitystä on myös asianomistajilla ja rangaistuksen arvioinnilla. Tietomurto voi olla useaan rikokseen nähden esiteko. Lähtökohtaisesti esi- ja jälkiteot on huomioitu sovellettaessa yhtä rikossäännöstä. Tätä arvioidessa tulee kuitenkin huomioida tekokokonaisuuden ajan, paikan ja tekotavan yhtenäisyys.

Lisäksi on arvioitava, perustuuko tekijän menettely yhteen ja samaan tahtotilaan, jota voidaan käyttää perusteluna rikosten yhtymisen puolesta. Joka tapauksessa lainkonkurrenssitilanteet vaativat tapauskohtaisen tarkastelun ja ratkaisun, etukäteen on määriteltävissä vain ohjeita erilaisten konkurrenssitilanteiden ratkaisemiseen. Oikeuskirjallisuudessa on esitetty tapauksen konkreettisten tosiseikkojen olevan merkityksellisiä lainkonkurrenssin määrittelyn kannalta tilanteessa, jossa esiymmärrys on mahdollista saavuttaa abstrakteilla tunnusmerkistöillä.[208]

Tietomurtorikosten tutkintaan ja tuomitsemiseen liittyvät haasteet johtuvat useamman eri tekijän yhteisvaikutuksesta. Teknisen käsitteistön tuntemus ja määrittely on tärkeää rikoksen kunnollisen selvittämisen kannalta, vaikka itse rikossäännös onkin tekniikkaneutraali. Haasteen ratkaisu voisi perustua viranomaisen toimivaltuuksien laajentamiseen selvittäessä tietoverkkorikoksia.

Tietomurtorikosten selvittäminen edellyttää yhteistyötä vähintään telepalveluntarjoajien kanssa, mihin kansallinen lainsäädäntö määrää poliisille tiedonsaantioikeuksia. Yleensä ensimmäisenä johtolankana tietomurtorikoksissa on yksittäinen IP-osoite. Oikeuskäytännössä pelkkä

[208] Luoto, 2022, s. 406.

IP-osoitteeseen perustuva argumentointi epäillyn syyllisyyden tueksi on kuitenkin voinut jättää epäilyksen vastaajan syyllisyydestä tietomurtoon. Muita tietomurtorikosten selvittämiseksi mahdollisia pakkokeinolainsäädännön keinoja ovat esimerkiksi laite-etsintä ja takavarikko. Pakkokeinojen käytössä tulee kuitenkin muistaa suhteellisuusperiaate.

Pakkokeinolainsäädännön perusteella poliisilla on myös mahdollisuus suorittaa peitetoimintaa tietoverkossa tietoverkkorikoksien selvittämiseksi, mikä on kuitenkin nykylainsäädännön puitteissa hankalaa. Peitetoiminnassa vaadittavaan uskottavaan valeidentiteettiin edellytetään tietoverkossa pitkäkestoisempaa suunnitelmallista toimintaa, kuin fyysisessä ympäristössä, mutta lainsäädäntö ei anna toistaiseksi perusteita tulevaisuuden peitetoimintaan varautumiseen. Jatkossa oman haasteensa tietomurtorikostenkin tutkinnassa asettaa oikeuskäytännön näkemys siitä, että käyttäjän identiteetin salaavat VPN-palvelut eivät ole viestinnän palveluntarjoajia, vaan sähköisen viestinnän välittäjiä, mihin pakkokeinolainsäädäntö ei ole suoraan sovellettavissa samalla tavalla.

Tietomurtorikosten rajat ylittäviä ominaisuuksia ja niihin liittyviä haasteita on yritetty ratkaista kansainvälisellä yhteistyöllä ja sääntelyllä. Käytännössä ongelmallista on kuitenkin se, että kaikki valtiot eivät sitoudu tietoverkkorikoksia ja niiden selvittämistä koskevaan kansainväliseen sääntelyyn. Asiassa tuleekin ottaa huomioon myös muu valtioiden välistä rikosasioiden selvittämistä koskeva oikeudellinen sääntely ja toimivaltaperiaatteet.

Tulevan lainsäädäntötyön kannalta jatkossa tietomurtoja koskevan sääntelyn tulisi mahdollisuuksien mukaan olla mahdollisimman ajantasaista ja neutraalia teknisten yksityiskohtien osalta. Nykymuodossaan rikossäännöksen tekniikkaneutraalius on toteutunut kohtuudella. Tuomioistuimessa tietomurron rikossäännös on tutkimuksessa käsiteltyjen tuomioiden perusteella ollut sovellettavissa myös myöhempiin tietoteknisiin innovaatioihin, kuten sosiaalisen median palveluihin. Tietojärjestelmän käsite kuulostaa hyvin tekniseltä, mutta lopulta kyse on alustasta, jolla käsitellään tietoa. Tieto on lopulta digitaaliselle alustalle tallennettua tietoa, merkitystä ei anneta sille, kuinka informatiivista se on. Hahmoteltaessa sitä, miten tietomurtoja on mahdollista ennaltaehkäistä tulevaisuudessa, rikosten torjunnan periaatteiden perusteella[209] merkittävintä olisi lisätä tietomurtorikollisuuteen liittyviä riskejä, kuten kiinnijäämisen riskiä lisäämällä valvontaa.

[209] Lappi-Seppälä, 2006, s. 54.

Arvioitaessa tulevaisuuden kyberrikosten, kuten tietomurtojen, lainsäädäntökehitystä, painopiste rikostorjunnassa on palveluntarjoajan ennakkovarautumisen ja vastuiden lisäämisessä tulevaisuudessa. Euroopan unionin verkko- ja tietoturvadirektiivi, toisin sanoen kyberturvallisuusdirektiivi, (EU) 2016/1148 määritteli vuonna 2016 ensimmäisenä toimenpiteitä unionitasolla määrättyjen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi unionin tasolla. Vaikka direktiivi tarkastelee asiaa riskienhallinnan ja turvallisuuden kannalta, rikosoikeudellisesta näkökulmasta kyse on rikokselle suotuisien olosuhteiden heikentämisestä, mikä vähentää mahdollisuuksia toteuttaa rikos.

Kirjoitushetkellä Euroopan unionin käsittelyssä on tarkistettu kyberturvallisuusdirektiivi, joka tulee korvaamaan tulevaisuudessa nykyisen kyberturvallisuusdirektiivin.[210] Tarkistetussa direktiivissä soveltamisalaa laajennetaan, määrittelemällä entistä useampi sektori ja toimija kyberturvallisuusriskien hallintatoimien ja raportointivelvoitteiden alaiseksi. Myös riskienhallintatoimenpiteitä on päivitetty, mikä käytännössä tarkoittaa uusia varautumistoimenpiteitä. Näin ollen on arvioitavissa, että tietomurron toteuttamismahdollisuuksia pyritään heikentämään entisestään tulevaisuudessa, millä on ennakolta rikostorjunnallinen vaikutus jatkossakin.

Jatkotutkimuksen kannalta kiinnostavaa olisi kiinnostavaa pureutua tuomioistuinten antamien tuomioiden perusteella lainkonkurrenssiin. Pelkällä abstraktilla arviolla ei välttämättä saada riittävää kuvaa säännösten välisestä tosiasiallisesta rikosoikeudellisesta suhteesta.[211] Tietomurron rikossäännöksen sisältämän toissijaisuuslausekkeen perusteella tietomurto väistyy useassa tilanteessa suhteessa toiseen mahdolliseen sovellettavan rikossäännökseen. Yllä esiteltyjen tilanteiden perusteella asia ei kuitenkaan ole yksiselitteinen, jolloin käytännön tarkastelu on aiheellista. On todennäköistä, että digitalisoituneen yhteiskunnan myötä tietomurrot lisääntyvät ja voivat vaarantaa yhteiskunnan kriittisiä toimintoja, joten aiheeseen liittyvä tutkimustyö on ja tulee olemaan tärkeää myös tulevaisuudessa.

[210] Euroopan neuvosto, lehdistötiedote, 13. toukokuuta 2022.
[211] Piippo, 2022, s. 657.