Verkkoavusteisten petosten sääntely ja torjunta talousrikosoikeudellisesta näkökulmasta

Lapin yliopisto
Oikeustieteiden tiedekunta
Maisteritutkielma
Mikko Piira
Talousrikosoikeus
Kesä 2022

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Verkkoavusteisten petosten sääntely ja torjunta talousrikosoikeudellisesta näkökulmasta
Tekijä: Mikko Piira
Oppiaine: Maisteritutkielma, Talousrikosoikeus
Työn laji: Tutkielma
Sivumäärä: XVIII + 71 s.
Vuosi: 2022

Tiivistelmä:

Verkkoavusteiset petokset ovat eniten tehty petosrikosten muoto niin kansallisesti kuin kansainvälisestikin, ja niiden määrä nousee vuosi vuodelta. Verkkoavusteiset petokset kohdistuvat niin kansalaisiin, yrityksiin kuin valtiollisiinkin instituutioihin. Verkkoavusteisia petoksia tekeville rikollisille menetetään vuosittain niin valtavat summat rahaa, että ilmiöstä voidaan puhua merkittävänä yhteiskunnallisena uhkana. Jatkuva teknologinen kehitys, kryptovaluuttojen käyttö ja mahdollisuus kohdistaa rikolliset toimet toisen valtion toimijoihin rikoksille sääntelyllisesti hedelmällisestä maasta ovat haasteita, joihin lainsäädännön ja rikostentorjunnan on haastavaa puuttua.

Verkkoavusteiset petokset voidaan lukea talousrikoksi niiden suuren määrän ja taloudellisten kokonaisvaikutusten vuoksi, sillä useat yksittäiset verkkopetokset saman tahon toimesta ovat yksiköitävissä yhdeksi suuremmaksi rikoskokonaisuudeksi. Verkkopetosten tarkasteleminen talousrikoksina tarjoaa kriminaalipoliittisen työkalun verkkopetosten rikostorjunnan parantamiseksi poliisin resurssien lisäämisellä ja rajat ylittävän viranomaisyhteistyön tukemisella. Verkkopetosten eri muodot vaihtelevat runsaasti, mutta ovat jäsennettävissä kahdeksaan eri luokkaan niiden ominaispiirteiden ja yhteiskunnallisten vaikutusten perusteella. Sähköisten todisteiden keräämistä tulee helpottaa muuttamalla kansallista sähköisen viestinnän palveluista annettua lakia sen 157 §:n sääntelemien tietojensäilytysaikojen suhteen. Rikostutkijoiden tulee jatkossa pystyä hankkimaan metatietoja rikostutkintaa varten vähintään kahden vuoden ajalta. Tältä osin myös pakkokeinolain 10 luvun 6 § tulee uudistaa tietojensaannin mahdollistamiseksi myös lievien verkkoavusteisten petosten osalta.

Avainsanat: Talousrikos, rikosoikeus, petos, verkkopetos, verkkoavusteinen petos, tietosuoja, sähköinen todistelu, tietoverkko, rikostorjunta, kriminaalipolitiikka

Sisällys

LÄHTEET

Kirjallisuus ja artikkelit

Aarnio, Aulis: Laintulkinnan teoria: yleisen oikeustieteen oppikirja. Werner Söderström Osakeyhtiö 1989.

Alvesalo, Anne: The Phenomenon Called Economic Crime. Teoksessa: *Alvesalo, Anne* – L*aitinen, Ahti*: Perspectives on Economic Crime. University of Turku. Publications of the Faculty of Law. Criminal Law and Judicial Procedure, Series A:20. Turku 1994, s. 67–111.

Axberger, Hans-Gunnar: Eko-brott, Eko-lagar och Eko-domstolar - En rättspolitisk utvärdering av lagstiftningen mot ekonomisk brottslighet. Brå forskning 1988:3. Tukholma 1988.

Biddle, Peter – England, Paul – Peinado, Marcus – Willman, Bryan: The Darknet and the Future of Content Distribution. Teoksessa: *Feigenbaum, Joan* (toim.): Digital Rights Management. ACM CCS-9 Workshop, DRM 2002. Washington DC, USA, November 1, 2002. Revised Papers. Springer 2003, s. 155–176.

Chertoff, Michael − Simon, Tobby: The Impact of the Dark Web on Internet Governance and Cyber Security. Global Commission on Internet Governance. Paper series 6/2015.

Christakis, Theodore: Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR? Teoksessa: Milch, Randal − Benthall, Sebastian (eds.): Cybersecurity and Privacy in a Globalized World - Building Common Approaches. New York University School of Law 2019, s. 1–17.

Danielsson, Petri – Näsi, Matti: Suomalaiset väkivallan ja omaisuusrikosten kohteena 2019 - Kansallisen rikosuhritutkimuksen tuloksia. Helsingin yliopisto, Kriminologian ja oikeuspolitiikan instituutti 2020.

Danielsson, Petri (Toim.): Rikollisuustilanne 2019. Helsingin yliopisto, Kriminologian ja oikeuspolitiikan instituutti 2020.

Delem, Mathieu: Economic Crisis and Crime. Emerald 2011.

Dupont, C. − Cilli, V. − Omersa, E. et al.: Study on the retention of electronic communications non-content data for law enforcement purposes − Final report. European Commission, Directorate-General for Migration and Home Affairs. Publications Office, 2020.

Ekfeldt, Jonas: Om informationstekniskt bevis. Stockholms universitet 2016.

Friedrichs, David O.: Trusted Criminals. White Collar Crime in Contemporary Society. Belmont, California: Wadsworth Publishing Company 1996.

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

Frände, Dan: Yleinen rikosoikeus. Suomentanut ja seuraamusosan päivittänyt Markus Wahlberg. Edita 2012, Porvoo.

Gillespie, Alisdair: Cybercrime, key issues and debates. Routledge 2016.

Haasio, Ari: Verkkorikokset. Avain 2017, Vantaa.

Hasham, Salim − Joshi, Shoan – Mikkelsen, Daniel: Financial crime and fraud in the age of cybersecurity. McKinsey & Company article 2019. Saatavissa: [https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity].

Helin, Markku: Monet on metodit. Oikeus 1998/3, s. 310–314.

Jareborg, Nils: Allmän kriminalrätt. Iustus 2001.

Kargl, Walter: Die Tathandlung beim Betrug, s. 613−633. Teoksessa: *Prittwitz, Cornelius – Baurmann, Michael – Günther, Klaus – Kuhlhen, Lothar − Merkel, Reinhard − Nestler, Cornelius – Schulz, Lorenz* (Hrsg.): Festschrift für Klaus Lüderssen. Zum 70. Geburtstag am 2. Mai 2002. Baden-Baden 2002.

Keinänen, Anssi – Väätänen, Ulla: Empiirinen oikeustutkimus – mitä ja milloin? Edilex 2015/7.

Kimpimäki, Minna: Kansainvälinen rikosoikeus. Kauppakamari 2015.

Kindhäuser, Urs: § 263. Teoksessa: *Kindhäuser, Urs – Neumann, Ulfrid* – Paeffgen Hans-Ullrich (Hrsg.): Nomoskommentar. Strafgesetzbuch. Band 2. 2. Auflage. Baden-Baden 2005.

Kindhäuser, Urs: Täuschung und Wahrheitsanspuruch beim Betrug. ZStW 1991, s. 398–424.

Kolehmainen, Antti: Tutkimusongelma ja metodi lainopillisessa työssä, s. 106–127. Teoksessa: Tarmo Miettinen (toim.): Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edita Publishing Oy 2016. (https://www.edilex.fi/kirjat/16170, avattu 10.2.2021).

Koponen, Pekka: Yksi vai useita rikoksia – rikosten yhtymisestä. Defensor Legis 4/2015, s. 609–625.

Korsell, Lars Emanuelsson: Ekobrott, liksom! Svensk Juristtidning 10/2000, s. 932–965.

Kukkonen, Reima: Rikoshyödyn menettäminen, osa I – Yleiset edellytykset, määrittely ja määrä. Defensor Legis 5/2016, s. 721–740.

Länsineva, Pekka: Perusoikeudet ja varallisuussuhteet. Vammala 2002.

Määttä, Kalle – Hirvonen, Markku: Viranomaisten tietojenvaihtosäännösten kehitys harmaan talouden torjunnassa. Edilex, 18/2018.

Paukku, Eelis: Tilintarkastaja ja taloudellinen rikollisuus tarkastuskohteessa. Liikejuridiikka 3/2021, s. 25–52.

Pawlik, Michael: Das unerlaubte Verhalten beim Betrug. Köln-Berlin-Bonn-München 1999.

Peltomäki, Juha − Norppa, Kati: Rikos meni verkkoon: näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Talentum 2015, Helsinki.

Pihlajamäki, Antti: Tietojenkäsittelyrauhan rikosoikeudellinen suoja. Datarikoksia koskeva sääntely Suomen rikoslaissa. Suomalainen lakimiesyhdistys 2004, Vammala.

Pirjatanniemi, Elina: Ympäristörikokset talouden rikoksina. Teoksessa: *Nuutila*, *Ari-Matti – Pirjatanniemi, Elina* (toim.): Rikos, rangaistus ja prosessi. Turun yliopisto, Oikeustieteellinen tiedekunta 2005, s. 261–282.

Puppe, Ingeborg: Die Erfolgszurechnung im Strafrecht: dargestellt an Beispielsfällen aus der höchstrichterlichen Rechtsprechung. Baden-Baden 2000.

Riekkinen, Juhana: Verkkopetoksista ja todistelusta. Lakimies 1/2018 s. 75–102.

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

Ripatti, Janne: Kilpailumanipulaatioteko petoksena. Urheilu ja oikeus 2020, s. 150–232.

Salmivuori, Riku: Miljoonaperintö tarjolla: kuinka verkkopetos toimii. Myllylahti 2016. Espoo.

Schafer, Burkhard – Mason, Stephen: The characteristics of electronic evidence in digital format. Teoksessa: *Mason, Stephen* (ed): Electronic Evidence. Third Edition. LexisNexis Butterworths 2012, s. 23–69.

Siltala, Raimo: Oikeustieteen tieteenteoria. Suomalaisen lakimiesyhdistyksen julkaisuja. Vammalan kirjapaino 2003.

Snyder, J. M.: Online auction fraud: Are the auction houses doing all they should or could to stop online fraud? Federal Communications Law Journal 52/2000, s. 453−472.

Stabek, Amber− Watters, Paul – Layton, Robert: The Seven Scam Types: Mapping the Terrain of Cybercrime. Second Cybercrime and Trustworthy Computing Workshop 2010, s. 41–51.

Ståhlberg, Kaarlo: Petoksesta, erityisesti pitäen silmällä erehdyksen aikaan saamista ja vireillä pitämistä sekä tavaran tai rahan tappiota: rikosoikeudellinen tutkimus. Suomalainen lakimiesyhdistys, Vammala 1964.

Sunde, Inger Marie: Databevis. Teoksessa: *Aarli, Ragna – Hedlund, Mary-Ann – Jebens, Sverre Erik* (red.): Bevis i straffesaker. Utvalgte em-ner. Gyldendal Juridisk 2015, s. 599–633.

Sutela, Mika: Pysyykö oikeustiede mukana modernin yhteiskunnan murroksessa? Oikeutta kohtuudella – The blog of UEF law school, 2019. Saatavissa: [https://blogs.uef.fi/oikeuttakohtuudella/tag/empiirinen-tutkimus/] (Avattu 4.5.2022, päivitetty 23.8.2019)

Sutherland Edwin H.: White Collar Crime. The Uncut Version. With an Introduction by Gilbert Geis and Colin Goff. New Haven and London: Yale University Press 1983.

Tapani, Jussi: Miten asianomistajien selonottovelvollisuus määrittää petoksen rangaistavuuden alaa? Teoksessa: *Paloranta, Paula − Hoppu, Kari − Hemmo, Mika − Mansala, Marja-Leena – Pönkä, Ville*: Keskuskauppakamarin liiketapalautakunta 80 vuotta. Alma Talent. Helsinki 2017, s. 309–318.

Tapani, Jussi: Petos liikesuhteessa. Talousrikosoikeudellinen tutkimus. Suomalainen lakimiesyhdistys, Helsinki 2004.

Tolvanen, Matti: Johdatus kriminaalipolitiikan teoriaan. Joensuun yliopisto, Joensuu 2005.

Träskman, Pers-Ole: Taloudellinen rikollisuus ja yhteiskunta. Taloudellisen rikollisuuden käsite, yleisyys ja vaikutukset. Teoksessa: Taloudellinen rikollisuus. Lakimiesliiton koulutuskeskuksen julkaisusarja N:o 32. Helsinki: Suomen Lakimiesliiton Kustannus Oy. Vammala 1981, s. 13–30.

Träskman, Pers-Ole: Taloudellinen rikollisuus tutkimuksen haasteena. Oikeus 2/1987, s. 122–133.

Vogel, Joachim: Betrug durch konkludente Täuschung: ¨Recht auf Wahrheit¨ oder kommunikative Vehrkehrssicherungspflichten? Teoksessa: Gedächtnisschrift für Rolf Keller. Tübingen 2003 s. 313–324.

Waaben, Knud: Strafferettens specielle del. 5. reviderede udgave. København 1999.

Wilhelmsson, Thomas: Sosiaalisen siviilioikeuden metodiset lähtökohdat. Teoksessa: *Häyhä, Juha* (toim.): Minun metodini. WSOY Porvoo 1997, s. 339–358.

Wood, Jessica: The Darknet - A Digital Copyright Revolution. Richmond Journal of Law and Technology 16(4) 2010, s. 1–60.

Virallisjulkaisut

Hallituksen esitykset ja valiokuntien mietinnöt

Hallituksen esitys HE 1988/66 vp.

Hallituksen esitys HE 102/2005 vp.

Hallituksen esitys HE 52/2021 vp.

Liikenne- ja viestintävaliokunnan mietintö LiVM 10/2014 vp.

Perustuslakivaliokunnan lausunto PeVL 18/2014 vp.

Valiokunnan lausunto HaVL 23/2021 vp.

Muut virallisjulkaisut

Euroopan komissio: Trans-Atlantic Data Privacy Framework. Saatavissa: [file:///C:/Users/mipii/Downloads/Trans-Atlantic_Data_Privacy_Framework.pdf.pdf] (Avattu 4.9.2022, päivitetty maaliskuussa 2022.)

Euroopan petoksentorjuntavirasto (OLAF): Kansallisia petostentorjuntastrategioita koskevat suuntaviivat. Laadittu jäsenvaltioiden asiantuntijoiden työryhmässä Euroopan petostentorjuntaviraston (OLAF) petostentorjunta-, raportointi- ja analyysiyksikön ohjauksen ja koordinoinnin alaisena. OLAF 2016.

Information Commissioner's Office: Data sharing between the public and private sector to prevent fraud. ICO Review 2015.

Kyberturvallisuuskeskus: Rikostorjunnan haasteet globaalissa verkkoympäristössä. Salo Cyber Talks 2021. Kyberrikostorjuntakeskus 2020. Saatavissa: [https://salo.fi/wp-content/uploads/2021/01/SaloCyberTalks_20210126_Mikko-Rauhamaa.pdf] (Avattu 2.2.2022, muokattu 3.1.2020).

Oikeusministeriö: Arviomuistio rikoslain viimeaikaisesta kehityksestä ja tulevista kehitystarpeista. Mietintöjä ja lausuntoja 7/2018.

Privacy International: Kansalliset tietojen säilyttämistä koskevat lait Euroopan unionin tuomioistuimen Tele-2/Watson-tuomion jälkeen. Privacy International 2017.

Sisäministeriö: Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14/2017.

Tilastokeskus: Rikos- ja pakkokeinotilasto. Helsinki: Tilastokeskus. 2020a. Saatavissa: [https://stat.fi/til/rpk/] (Avattu 11.8.2022).

Tilastokeskus: Väestörakenne. Helsinki: Tilastokeskus. 2020b. Saatavissa: [https://www.stat.fi/til/vaerak/] (Avattu 11.8.2022).

Turvallisuuskomitea: Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 2019.

United Nations Office on Drug and Crime (UNODC): Comprehensive Study on Cybercrime. United Nations 2013.

Euroopan komission ehdotukset ja julkaisut

Euroopan komissio: Komission ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yleisten sähköisten viestintäpalvelujen tarjoamisen yhteydessä käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, COM(2005) 438 final, 21.9.2005.

Euroopan komissio: Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, verkkoalustat ja digitaaliset sisämarkkinat: Euroopan mahdollisuudet ja haasteet COM(2016) 288 final.

Euroopan komissio: Komission tiedonanto Euroopan parlamentille, Eurooppaneuvostolle ja neuvostolle. Kahdeksas raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia (COM(2017) 354 final, 29.6.2017). (Euroopan Komissio 2017b).

Euroopan komissio: Komission tiedonanto Euroopan parlamentille, Eurooppaneuvostolle ja neuvostolle. Yhdestoista raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia (COM(2017) 608 final, 18.10.2017). (Euroopan Komissio 2017a).

Euroopan komissio: Komission tiedonanto Euroopan parlamentille, Eurooppaneuvostolle ja neuvostolle. Yhdestoista raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia (COM(2017) 608 final, 18.10.2017).

Euroopan komissio: Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS sähköistä todistusaineistoa rikosoikeudellisissa asioissa koskevista eurooppalaisista esittämis- ja säilyttämismääräyksistä. COM/2018/225 final - 2018/0108 (COD).

Euroopan komissio: Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI yhdenmukaisista säännöistä laillisten edustajien nimeämiseksi todistusaineiston keräämistä varten rikosoikeudellisissa menettelyissä COM/2018/226 final - 2018/0107 (COD).

Euroopan komissio: SWD(2018) 118 final.

Internet-aineisto

Australian Federal Police: Australian Federal Police, Internet fraud. Saatavissa: [https://www.police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf] (Avattu 20.2.2022).

EU:n Muuttoliike- ja sisäasioiden pääosasto: Cybercrime. Saatavissa: [https://home-affairs.ec.europa.eu/cybercrime_fi] (Avattu 1.6.2022).

Eurojust: Takedown of infrastructure of call centres involved in online investment fraud responsible for losses of at least EUR 20 million. Saatavissa: [https://www.eurojust.europa.eu/news/take-down-infrastructure-call-centres-involved-online-investment-fraud-responsible-losses] (Avattu 6.6.2018, muokattu 21.4.2022).

Helsingin sanomat: Sijoituspetokset ovat yksi nopeimmin kasvavista rikollisista uhkista Euroopassa, arvioi Europol-johtaja – niiden tutkintaa ei kuitenkaan priorisoida. Saatavissa: [https://www.hs.fi/talous/art-2000006428641.html] (Avattu 15.8.2022, muokattu 5.3.2020).

Lehtinen, Viivi: Tietoverkkorikollisuus poliisin silmin 2020-2021. KRP Kyberrikostorjuntakeskus 2021. Saatavissa: [https://poliisi.fi/blogi/-/blogs/tietoverkkorikollisuus-poliisin-silmin-2020-2021] (Avattu 1.8.2022, muokattu 5.10.2021).

PwC: PwC's Global Economic Crime and Fraud Survey 2020. Saatavissa: [http://www.global-screeningsolutions.com/industries/global-economic-crime-and-fraud-survey-2020-1.pdf] (Avattu 28.1.2022).

PwC: PwC's Global Economic Crime and Fraud Survey 2020. Saatavissa: [https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html] (Avattu: 28.1.2022).

Yle Uutiset: Espanja pidätti etsityn kyberrikollisen – hakkeriliiga varasti maailman pankeilta yli miljardi euroa. Yle Uutiset 2018b. Saatavissa: [https://yle.fi/uutiset/3-10134557] (Avattu 14.8.2022, muokattu 26.3.2018).

Yle Uutiset: Loma-aika on toimitusjohtajahuijausten kulta-aikaa: "Onnistuvat yllättävän hyvin". Saatavissa: [https://yle.fi/ uutiset/3-9695948] (Avattu 1.4.2022, muokattu 29.6.2017).

Yle Uutiset: Nyt iskevät valetoimitusjohtajat – KRP kertoo pörssiyhtiöiden menettäneen miljoonia. Saatavissa: [https://yle.fi/uutiset/3-8625155] (Avattu 1.4.2022, muokattu 26.1.2016).

Yle Uutiset: Poliisi tutkii valtavaa tietomurtoa helsinkiläisessä yhdistyksessä – 130 000:n tiedot päätyneet vääriin käsiin. Yle Uutiset 2018a. Saatavissa: [https://yle.fi/uutiset/3-10148210] (Avattu 14.8.2022, muokattu 6.4.2018).

Oikeuskäytäntö

Korkein oikeus

KKO 1995:23

KKO 1995:24

KKO 1995:25

KKO 2008:38

KKO 2003:88

KKO 2009:109

KKO 2011:84

Hovioikeudet

HelHo 29.01.2016, R 15/631

HelHO 30.05.2016, R 16/807

HelHo 26.03.2018 R 17/362

HelHO 24.05.2018 R 17/1965

HelHO 31.05.2017 R 16/2646

HelHO 09.02.2018, R 17/336

THO 2019:15

Käräjäoikeudet

Keski-Suomen käräjäoikeus 14.6.2017, R 17/460

Euroopan unionin tuomioistuin

C-293/12 ja C-594/12 Digital Rights Ireland ja Seitlinger ym.

C-203/15 ja C-698/15 Tele2 Sverige AB ja Watson ym.

C 207/16 Ministerio Fiscal.

C-623/17 Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others.

C-511/18 ja C-512/18 Ranskan dataverkko, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet assosiatiivit v Premier ministre, Garde des Sceaux, Ministre de la Justice.

C-140/20 Commissioner of the Garda Síochána ym.

Liitteet

Liite 1. Poliisin talousrikostorjuntayksikön haastattelu.

Lapin yliopisto,
oikeustieteellinen tiedekunta

Helsingin poliisilaitos
Rikostutkintayksikkö, talous- ja petosrikokset

Vastaukset ON Mikko Piiran pro gradu -tutkielmaa varten

1. *Millä tasolla taloudellisesti motivoituneiden ja verkkoa hyväksi käyttävien petosrikosten torjunta ja selvittäminen on? Onko tällaisilla rikoksilla jotain erityisiä ongelmakohtia?*

Yleisesti totean tietoverkkoa hyväksi käyttävien petosrikosten torjunnan olevan tyydyttävällä tasolla, joskin tässä on havaintojeni mukaan paljonkin poliisilaitoskohtaisia eroja. Niissä poliisilaitoksissa ja valtakunnallisissa poliisiyksiköissä, joissa tietoverkkoavusteisia (TVA) petoksia selvitetään omassa rikosalaan erikoistuneessa tutkintaryhmässä sekä osaaminen että esitutkintaan käytettävät resurssit ovat parempia, kuin poliisilaitoksissa, joissa tva-petoksia tutkitaan niin sanotuissa yleisryhmissä, joiden toimenkuvaan kuuluu kaikkien rikoslakirikosten esitutkinta.

Luokiteltavien "nettipetosten" osalta rikosten lukumäärä kasvaa jatkuvasti. Vuonna 2020 poliisissa on valtakunnallisesti tutkittu 20 603 tva-petosta ja vuonna 2021 näitä tekoja oli jo 26 696. Oletan, että vuonna 2022 rikoksia on edelleen edeltävää vuotta enemmän. Erityisseurattavien tva-petosten rikoshyöty Suomessa on poliisin tietojen mukaan vuonna 2021 ollut noin 33 miljoonaa euroa, joten näiden rikosten osalta voidaan jo puhua yhteiskunnallisestikin merkittävästä vahingosta, etenkin kun vahinko kohdistuu suuressa määrin yksittäisiin kansalaisiin tai pienyrityksiin.

Keskeistä tva-petosrikosten torjunnassa on poliisilla käytettävissä olevien pakkokeinojen ja poliisilain mukaisten tiedonsaantioikeuksien hallinta. Pakkokeinolain ja poliisilain soveltamiseksi tehokkaasti tulee lisäksi olla osaamista eri tietojärjestelmien käytöstä ja avointen lähteiden tarjoamista mahdollisuuksista esitutkinnan ja rikostiedustelun välineenä. Torjunnan kannalta merkityksellistä on myös seurata ja ymmärtää erilaisia ilmiöitä, joita tva-petosrikoksiin liittyy. Oman näkemykseni mukaan poliisissa ja etenkin Helsingin poliisilaitoksessa on hyvät edellytykset suorittaa esitutkintaa tva-petoksiin liittyen. Tutkijat, joiden toimenkuvaan näiden rikosten esitutkinta kuuluu, osaavat käyttää eri tietojärjestelmiä hyvinkin monipuolisesti sekä soveltaa rikosten tutkintaan liittyvää lainsäädäntöä. Helsingin poliisilaitoksessa työskentelevillä tutkijoilla on myös erittäin hyvät valmiudet analysoida sidosryhmien tuottamaa aineistoa ja selvittää rikoksia aineiston avulla. Tämän mahdollistaa käytännössä se, että tutkijoiden ei tarvitse tutkia muita rikoslakirikoksia.

Yleisesti voidaan todeta, että uudet ilmiöt ja tekotavat tulevat poliisin tietoon ilmoitettujen rikosten kautta, jonka jälkeen poliisin tutkintatoimenpiteitä kehitetään vastaamaan mahdollisesti uuteen tekotapaan. Tva-petosrikosten torjunta edellyttää tiivistä yhteistyötä muun muassa teleoperaattoreiden ja pankkien sekä rahoitusyhtiöiden kanssa. Kaiken tva-petosrikollisuuden ennalta estäminen on käytännössä mahdotonta niin kauan, kun ihmisillä on vapaa pääsy tietoverkkoihin ja

mahdollisuus hoitaa esimerkiksi omia pankkiasiointejaan sähköisesti, mutta muun muassa EU:n toisen maksupalveludirektiivin (PSD2) myötä tietyt tva-petosrikokset ovat romahtaneet. Rikolliset onnistuvat kuitenkin kehittämään jatkuvasti uusia tapoja tehdä tva-petoksia ja hyödyntämään tietoverkkoihin liittyviä haavoittuvuuksia.

Tietoturvallisuus yleisesti on keskeisin ongelma, mikä tva-petoksiin liittyy. Tässä yhteydessä vakavin tietoturvallisuuteen liittyvä aukko on loppukäyttäjissä eli yleensä rikosten asianomistajissa, jotka eivät suojaa omaa toimintaansa tietoverkoissa riittävästi tai sitten itse aktiivisesti omalla toiminnallaan mahdollistavat rikosten tekemisen.

Toisena ongelmakohtana koko tietoverkkorikollisuuteen liittyen on tietoverkkojen globaalius ja mahdollisuus tehdä rikoksia kansainvälisesti. Ulkomaille siirtyvien varojen seuranta on, jos ei mahdotonta, niin hyvin vaikeaa, ja näitä saadaan hyvin harvoin palautettua rikoksen asianomistajille, vaikka rikoksella saatuja varoja pystyttäisiinkin seuraamaan tiettyyn pisteeseen saakka.

Kolmantena ongelmakohtana näen henkilökohtaisesti virtuaalivaluuttojen kehittymisen sekä niillä suoritettavien siirtojen yleistymisen. Virtuaalivaluuttoihin liittyen osaaminen poliisissa on rajattua ja virtuaalivaluuttoihin kohdennettavien pakkokeinojen osalta vieläkin rajatumpaa.

2. *Pitäisikö lainsäädäntöä kehittää vastaamaan rikostorjunnan ja rikosten selvittämisen tarpeita verkkopetosten suhteen? Jos pitäisi, niin miten?*

Lainsäädäntöä on uudistettu ja esimerkiksi valmisteilla olevan pakkokeinolain uudistusten myötä poliisin mahdollisuudet puuttua rikollisuuteen ylipäätään ovat hyvällä tasolla. Pakkokeinojen käyttämiseen liittyvän kohtuusperiaatteen mukaisesti pakkokeinoja tulee käyttää ensisijaisesti vakavammissa rikoksissa ja lievemmissä tekomuodoissa pakkokeinojen käyttäminen laajalti ei yleensä ole mahdollista.

Tva-petosrikoksiin keskeisesti liittyvää lainsäädäntöä on pakkokeinolain 10 luvun 6 § televalvonta ja sen edellytykset. Pakkokeinolaki mahdollistaa televalvonnan käyttämisen petosrikoksissa lieviä tekomuotoja lukuun ottamatta silloin kun teko on tehty teleosoitetta tai telepäätelaitetta käyttäen. Tätä soveltamisalaa ei ole mielestäni tarpeen laajentaa koskemaan lieviä tekomuotoja, vaikka se tarkoittaakin sitä, että lievissä tva-petoksissa tekijää ei aina saada selvitettyä. Poliisilla ei tällä hetkellä ole myöskään riittäviä resursseja televalvonnan suorittamiseksi lievien rikosten osalta, vaikka lainsäädäntö sen mahdollistaisi.

Toinen keskeisesti tva-petosrikosten selvittämiseen liittyvä lainsäädäntö löytyy laista sähköisen viestinnän palveluista (2014/917), jonka 19 luvussa säädetään viranomaistoimintaan liittyvistä tiedoista ja 157 § säädetään teleyritysten tietojen säilytysvelvollisuudesta. Tällä hetkellä lainsäädäntö edellyttää teleyrityksiä säilyttämään muun muassa internetyhteyspalveluun liittyviä IP-tietoja 9 kuukautta viestintätapahtuman ajankohdasta lukien. Näitä tietoja poliisi saa käyttöönsä niissä rikoksissa, joissa on PKL 10:6 mukaiset edellytykset. Kun ottaa huomioon sen, miten tva-petosrikokset tulevat poliisin tietoon, niin säädetty 9 kk:n säilytysvelvollisuus ei

aina riitä. Usein asianomistajat tulevat tietoiseksi heihin kohdistuneesta rikoksesta pitkänkin ajan kuluttua teon tapahtuma-ajankohdasta esimerkiksi perintäyhtiöiden lähettämien perintäkirjeiden kautta ja ilmoittavat vasta tällöin rikoksesta poliisille. Kun teosta on kulunut aikaa, ei poliisilla välttämättä ole enää mahdollisuutta saada tarvittavaa näyttöä rikoksesta ja syytteen tueksi teoissa, joista on jo ilmoitushetkellä kulunut yli 9 kk. Lievemmissä tekomuodoissa poliisilla on mahdollisuus saada teleyrityksiltä IP-tietoja 1 - 3 kk:n ajalta teleyrityksestä riippuen. Käytännössä tämä tarkoittaa sitä, että lievemmissä tekomuodoissa poliisilla ei ole edellytyksiä suorittaa esitutkintaa saatavilla olevan lisäselvityksen puutteen vuoksi ja esitutkinnat on tästä syystä keskeytettävä. Mikäli lainsäädäntöä tarkastellaan teleyritysten säilytysvelvollisuuden osalta, niin tämä tva-petosrikosten selvittämiseen liittyvä seikka tulisi huomioida lainvalmistelun yhteydessä.

Helsinki 12.8.2022

Teemu Haapala
rikoskomisario
Helsingin poliisilaitos

LYHENTEET

BEC	Businness email compromise
EJCN	Euroopan kyberrikollisuusverkosto
ENISA	Euroopan unionin verkko- ja tietoturvaviraston
ETL	Esitutkintalaki (805/2011)
EU	Euroopan Unioni
FRA	Euroopan unionin perusoikeusviraston
HelHO	Helsingin hovioikeus
IOCTA	Europol Internet Organised Crime Threat Assessment
KKO	Korkein oikeus
OLAF	Euroopan petostentorjuntavirasto (European Anti-Fraud Office)
PKL	Pakkokeinolaki (806/2011)
PL	Perustuslaki (731/1999)
PolL	Poliisilaki (872/2011)
RL	Rikoslaki (39/1889)
SEUT	Euroopan unionin toiminnasta tehty sopimus
StGB	Strafgesetzbuch
SVPL	Sähköisen viestinnän palveluista annettu laki (917/2014)
THO	Turun hovioikeus
UNODC	YK:n huumeiden ja rikollisuuden torjunnasta vastaavan toimisto
VL	Valiokunta
YK	Yhdistyneet kansakunnat

KUVIOT JA TAULUKOT

1 Johdanto

1.1 Aihe ja kysymyksenasettelu

Tutkimuksen aiheena on verkkoavusteisten petosten sääntely ja torjunta. Tutkimustehtävänä on selvittää verkkoavusteisten talousrikosten sääntelyn haasteita erityisesti petosrikosten näkökulmasta. Aihe on ajankohtainen, sillä eri tahojen tuottamien kyselyiden ja poliisin tietoon tulleiden rikosten perusteella nähdään tietoverkkojen toimivan jatkuvasti kasvavissa määrin taloudellisten rikosten näyttämönä.[1] Uusi teknologia ja tietoverkkojen kansainvälinen luonne luovat haasteita erilaisten tietoverkkojen välityksellä tapahtuvien rikosten torjunnassa sekä sääntelyssä.

Tutkimuksen tarkoituksena on vastata kysymykseen, miten tietoverkot vaikuttavat petosrikosten sääntelyn kehitystarpeisiin. Tähän kysymykseen vastaamiseksi tulee myös käsitellä seuraavia apukysymyksiä:

1. Millaisia erilaisia verkkopetoksia on olemassa?
2. Mikä on tietoverkkojen merkitys modernissa rikosoikeudessa?
3. Millä tasolla taloudellisten verkkopetosrikosten torjunta on?

Näihin kysymyksiin vastaamalla on tarkoituksena muodostaa kattava kuva verkossa tapahtuvista taloudellisista rikoksista rikosoikeudellisena ilmiönä sekä niiden merkityksestä yhteiskunnassa ja globaaleilla markkinoilla. Tällöin voidaan vastata myös tutkimuksen pääkysymykseen. Näin saavutetusta vastauksesta riippuen pyritään myös muodostamaan suositus petossääntelyn kehityksestä ja tulkinnasta tutkimuksen lopputulemana.

1.2 Tutkimuksen tausta

Tietotekniikan ja erityisesti tietoverkkojen hyvin nopea kehitys 2000-luvulla ovat muuttaneet perustavanlaatuisesti yhteiskuntaa ja arkipäiväistä elämää. Kansainvälisen digitalisaation seurauksena tietotekniikan ja tietoverkkojen käyttö on yleistynyt ja jopa muuttunut pakolliseksi monilla talouden ja yhteiskunnan sektoreilla. Monet yhteiskunnalliset instituutiot ovat riippuvaisia erilaisiin tietojärjestelmiin varastoidusta tiedosta ja näiden tietojärjestelmien toimivuudesta sekä luotettavuudesta. Tämä nopea kehityskulku ja riippuvaisuus

[1] Ks. esim PwC 2020 sekä kyberturvallisuuskeskus 2021.

tietoverkkojen turvallisuudesta sekä luotettavuudesta on aiheuttanut myös haasteita rikosoikeudelle. Erilaiset tietomurrot ja tietojen kalastelu ovat tulleet jäädäkseen.[2]

Esimerkiksi vuonna 2014 kyberrikollisuuden on arvioitu aiheuttaneen maailmantaloudelle yli 400 miljardin euron tappiot.[3] Tämän jälkeen rikosten volyymi on vain kiihtynyt suurien voittojen ja pienen kiinnijäämisriskin seurauksena. Vastaamoon tehty tietomurto on silmät avaava esimerkki 2020-luvun yhteiskunnallisista ja poliisin kohtaamista haasteista. Pelkästään noin 30 000 tuhannen asianomistajan rikosilmoituksen kirjaaminen on ollut mittava toimenpidekokonaisuus viranomaisille. Tietoverkkorikosten kansainvälisen toimintakentän ja anonymiteetin seurauksena kansallisilla viranomaisilla on haasteita saada tietoverkkojen välitykselle toimivat rikolliset rikosoikeudelliseen vastuuseen. Rikostutkinnan kohtaamat modernit haasteet liittyvät yhä enemmän suurten datamassojen[4] hallintaan ja tutkimiseen. Lisäksi rikollisten ja laittoman toiminnan siirtyessä yhä enenevissä määrin tietoverkkoihin syntyy näiden uudenlaisten, entistä kansainvälisempien rikosten sekä lainsäädännön välille kitkaa sääntelyn rakentuessa ajatukselle reaalimaailman perinteisistä rakenteista. Uudenlaiset salausmenetelmät tietoteknisissä laitteissa, sovelluksissa, käyttöjärjestelmissä ja verkkoliikenteessä lisääntyvät jatkuvasti edellyttäen poliisin omien menetelmien, laitteistojen ja osaamisen jatkuvaa kehittämistä.[5]

Verkkoavusteiset petokset eivät kohdistu vain yksityishenkilöihin tavanomaisten verkkohuijausten kautta, vaan myös suuriin kansainvälisiin organisaatioihin. Verkkoavusteiset petokset ovatkin nousseet yhdeksi yleisimmäksi petos- ja talousrikostyypiksi viimeisten vuosien aikana. Petoksien seurauksena yrityksille ja valtiollisillekin toimijoille on koitunut yhä suurempia taloudellisia vahinkoja. Esimerkiksi Europolin arvion mukaan pelkästään petoksilla saatu rikoshyöty Euroopan Unionissa (EU) on vuosittain noin 10 miljardia euroa, kun valmistevero- ja arvonlisäveropetoksia ei lueta mukaan.[6]

Tietoverkoilla tarkoitetaan tässä tutkimuksessa laitteiden välisten tietoliikenneyhteyksien välille muodostuvaa järjestelmää, joka mahdollistaa datan välittämisen. Tietoverkon käsitteen alle lukeutuu internet, joka voidaan karkeasti jakaa näkyvyyden mukaan normaaliin

[2] HaVL 23/2021 vp.
[3] Peltomäki – Norppa 2015, s. 6.
[4] Datan oikeudellisista määritelmistä ks. tietoverkkorikollisuutta koskevan yleissopimuksen (2001, ETS 185) 1(b) artikla, yleissopimuksen selitysmuistion kohta 25 ja pakkokeinolain (806/2011, PKL) 7:1.2.
[5] HaVL 23/2021 vp.
[6] Helsingin sanomat 2020.

internetiin,[7] syvään internetiin[8] ja pimeään internetiin.[9] Internetin avoimet palvelut, kuten useimmat sosiaalisen media palvelut, lukeutuvat normaaliin internetiin. Keskimmäiseen liittyvät erilaiset verkkopankit ja valtiolliset tietokannat sekä maksumuurin takana olevat sivustot. Viimeisen joukon muodostavat erilaiset piilossa olevat palvelut, joihin pääsemiseksi tarvitaan lähtökohtaisesti erillinen ohjelmisto.[10]

Tämä tutkimus tarkastelee tietoverkkoa hyödyntävien petosrikosten aiheuttamaa rikosoikeudellista ja rikostorjunnalle aiheutuvaa problematiikkaa talousrikosoikeudellisesta näkökulmasta. Tutkimuksessa käsitellään erilaisia verkkopetostyyppejä, mutta päähuomio tulee olemaan organisaatioihin kohdistuvissa tai muutoin taloudellisesti merkittävissä tietoverkkoa hyödyntävissä petosrikoksissa.

1.3 Aiheen rajaus

Yleisenä rikosnimikkeenä petokset pitävät sisällään laajan kirjon erilaisia rikoksia. Petoksista puhuttaessa voidaan tarkoittaa esimerkiksi veropetoksia, maanpetoksia tai erilaisia maksuvälinepetoksia. Petosten yhteydessä tai niiden tunnusmerkistön täyttymistä pohdittaessa voidaan puhua myös muun muassa kavalluksesta ja korruptiosta. Talousrikosoikeudellisesta näkökulmasta erityisesti velallisen petokset ja veropetokset ovat merkittävässä asemassa.

Näin ollen tutkimuksen johdonmukaisuuden vuoksi on syytä rajata tutkimuksen ala koskemaan rikostunnusmerkistöjen osalta nimenomaisesti lievää petosta, petosta ja törkeää petosta. Vaikka maksuvälinepetokset ja veropetokset tapahtuvatkin nykyään usein tietoverkkoja hyväksikäyttäen, eivät ne ole tutkimuksen kohteen, tietoverkkojen petosrikoksille aiheuttamien sääntelyllisten vaikutusten, kannalta erityisen merkittäviä rikoksia. Veropetokset eivät toimi samalla logiikalla kuin verkkoavusteiset petokset, ja maksuvälipetoksista on olemassa jo paljon kattavaa sääntelyä. Lisäksi maksuvälinepetosten arvioiminen verkkopetosten näkökulmasta tekisi tutkimuksen aiheesta liian laajan. Sähköisiä todisteita käsitellään vain niiden suorien vaikutusten osalta, eikä esimerkiksi rikosprosessioikeudellisia kysymyksiä käsitellä. Sähköiset todisteet ovat sinällään oleellinen osa verkkopetosten oikeudellista viitekehystä, mutta tutkielmassa käsitellään tätä ilmiötä vain siltä osin, kuin se

[7] Eng. clearnet.
[8] Eng. deepweb.
[9] Eng. darknet.
[10] Ks. internetin datan näkyvyyden tasoista tarkemmin Chertoff – Simon 2015, s. 1–7.

liittyy rikostorjunnan haasteisiin ja tarpeisiin. Syvempi prosessioikeudellinen katsanto sähköisestä todistelusta tekisi tutkimuksesta liian laajan. Samasta syystä tutkimuksessa käsitellään vain välttämättömin osin perinteisiä, yksityishenkilöihin kohdistuvia ja tunnettuja verkkopetoksia, kuten tietojenkalastelua ja ennakkomaksupetoksia. Tutkimuksen tarkka rajaaminen rikoslain (39/1889) 36:1–3 §:iin tietoverkkojen viitekehyksessä mahdollistaa aiheen syväluotaavan käsittelyn, jonka avulla tutkimuskysymyksiin pystytään antamaan kattava sekä tieteellisesti perusteltu vastaus.

1.4 Tutkimuksen metodi

Oikeustieteellisessä tutkimuksessa metodi on sekä tieteenteoreettisesti että käytännön kirjoittamisen kannalta monitulkintainen asia. Yhtä ainoaa oikeata metodia ei oikeustieteessä ole. Siinä hyödynnetään monenlaisia menetelmiä, jotka määrittyvät paljolti tutkimusongelman mukaan. Tarjolla ei siis ole valmista metodipakettia, joka olisi aina käyttökelpoinen tutkijan käytettäväksi. Metodi liittyy kuitenkin saumattomasti tutkimuskysymykseen ja siihen liittyvien ongelmien ratkaisuun. Valitun menetelmän tulee olla sellainen, että sen avulla tutkimuskohteesta saadaan esiin jotain merkittävää ja mielenkiintoista.[11]

Tutkimukseen sopivia metodeja ovat oikeusdogmatiikka, oikeusvertailu ja *de lege ferenda*. Oikeusdogmatiikan keinoin tarkastellaan kansallisen sääntelyn tilaa ja oikeusvertailun avulla puolestaan voidaan tutkia muiden maiden lainsäädännöllisiä ratkaisuja globaalin kyberrikollisuuden torjunnassa. Tutkimuskysymykseen vastaamisen ja tutkimuksen tarkoituksen kannalta *de lege ferendan* mukainen tavoite-keino -analyysi tarjoaa myös toimivan mallin tutkielman rakentamiselle.

Kansallisen näkökulman korostamiseksi ja tutkimuksen sisäisen logiikan ylläpitämiseksi tutkimuksessa pitäydytään kuitenkin pääosin oikeusdogmaattisen eli lainopillisen metodin käytössä. Oikeusvertailun painottaminen ei ole myöskään tutkimuksen tehokkaan rajaamisen vuoksi mielekästä. Oikeusvertailua voidaan kuitenkin hyödyntää rajoitetusti haettaessa johtoa ongelman ratkaisuun ulkomaisista säännöksellisistä ja yhteiskunnallisista sovelluksista. Samoin *de lege ferenda* metodia voidaan käyttää rajoitetusti tutkimuksen loppupuolella lainsäädännöllisen ehdotuksen muodostamisessa, mikäli tälle on tarvetta.

[11] Kolehmainen 2015, s. 112.

Tämän tutkielman tutkimusmetodina toimii siis pääsääntöisesti lainoppi. Lainopin tiedonintressinä on tuottaa voimassa olevaa oikeutta koskevia perusteltuja tulkinta-, punninta- ja systematisointikannanottoja.[12] Tutkielman lopputulosten perusteella voidaan mahdollisesti tuottaa tulkintakannanotto sääntelyn nykytilaa koskien. Tämän mahdollisuuden vuoksi lainopillinen tutkimusmetodi on tutkimuskysymysten kannalta soveltuva. Lainopin tehtävänä on perinteisesti pidetty oikeussääntöjen sisällön selvittämistä eli tulkintaa, oikeusperiaatteiden punnintaa eli yksittäisen oikeusperiaatteen ratkaisuarvon määrittämistä sekä oikeussäännösten systematisointia.[13] Käsillä olevassa tutkielmassa käytetään aineistona perinteisiä oikeuslähteitä kuten oikeussäännöksiä, oikeuskirjallisuutta, viranomaisasiakirjoja ja oikeuskäytäntöä. Lisäksi tutkimuksessa hyödynnetään asiantuntijoiden lausuntoa haastattelututkimuksen avulla.[14] Lainopillisen metodin mukaisesti näitä lähteitä tulkitsemalla ja systematisoimalla pyritään löytämään vastaus tutkimuskysymykseen. Metodin hyödyntämistä vaativat perustelut ovat keskeisessä asemassa koko tutkimuksen läpäisevästi. Hyvän lainopillisen tutkielman perustana on tietenkin onnistunut kysymyksenasettelu sekä se, että tutkimustehtävään haetaan vastausta asianmukaisen metodin avulla. Toisaalta vasta tutkimuksen loppupuolella huomataan, oliko metodi asianmukainen – voihan olla, että valittu tutkimustapa ei kykenekään enää vastaamaan alkuperäiseen tutkimuskysymykseen, kun tutkimus on elänyt ja muovautunut tutkimusprosessin aikana. Tämän lopputuleman välttämiseksi tutkimusmetodia on syytä arvioida huolellisesti jo tutkimuksen alussa.

Oikeustieteen tiedonintressi koskee sitä, mitä tai millaista tietoa tutkimuksella tavoitellaan. Tiedonintressi voi olla esimerkiksi laintulkinnallinen, systematisoiva, sääntelyn vaikutuksia arvioiva tai sääntelyä kehittävä.[15] Lainopin tiedonintressinä on tuottaa voimassa olevaa oikeutta koskevia perusteltuja tulkinta-, punninta- ja systematisointikannanottoja. Tavanomaisesti tällaiset kannanotot koskevat sitä, mikä on voimassa olevan oikeuden tietyn hetkinen sisältö vallitsevan lainopin mukaisesti. Huomio kohdistetaan tällöin siihen, miten oikeus on tosiasiallisesti aiemmin toteutunut, sekä siihen, miten oikeus tulee tulevaisuudessakin toteutumaan. Oikeusdogmatiikan vallalla oleva doktriini kiinnittää oikeudellisen tulkinnan, arvioinnin ja systematisoinnin tuomareiden ja muiden lakia soveltavien viran-

[12] Kolehmainen 2015, s. 107.
[13] Kolehmainen 2015, s. 113.
[14] Ks. Liite 1.
[15] Oikeustieteen tiedonintressistä tarkemmin ks. Kolehmainen 2015 s. 107 ja Siltala 2003, s. 135–137.

omaisten yhteistuumaisesti hyväksymään tuomarinideologiaan, eli niin kutsuttuun vallitsevaa tuomarinideologiaan. Näin ollen tiedonintressinä on se, mitä oikeus on.[16]

Lainoppia voidaan näin ollen luonnehtia luonteeltaan käytännönläheiseksi. Se ei kuitenkaan voi toimia vailla teorian tuottamia yleisiä oppeja tai periaatteita. Aarnio kuvailee teorian tekevän lainopista todellisen tieteen, joka syntyy teorian ja käytännön välisestä kognitiivisestä resonanssista.[17] Lainopillisella tutkimuksella on Aarnion mukaan ”tieteellinen asenne”, joka tarkoittaa sitä, että lainopissa sitoudutaan tieteelliseen paradigmaan. Tässä paradigmassa lainoppi suorittaa sen tehtävää hallitusti perustellen ja muodostaen objektiivisia sekä sisällöllisesti yhtenäisiä oikeudellisia argumentteja. Näin ollen oikeustieteilijän ja tavallisen maallikkoon välinen ero on se, että oikeustieteilijä kykenee tuottamaan lainopin avulla kontrolloituja hypoteeseja lain merkityksestä, tai systematisoida lakia yleisten oppien perusteella.[18]

Summaten todettakoon, että lainopillisen tutkimuksen keskeisinä tehtävinä pidetään oikeussäännösten tulkintaa ja systematisointia, oikeusperiaatteiden punnintaa sekä voimassa olevan oikeuden selvittämistä. Lainopillisessa tutkimuksessa tarkasteltavaa tapausta lähestytään tulevia lainsoveltamistilanteita ajatellen normatiivisesta näkökulmasta ja vallitsevan oikeuden lähtökohdista. Huomiota kiinnitetään erityisesti myös siihen, kuinka oikeus on tosiasiallisesti toteutunut ja kuina se tulee myös tulevaisuudessa todennäköisesti toteutumaan. Lainopin tutkijan tehtävänä on perustelluilla tulkintasuosituksillaan auttaa lainsoveltajia heidän työssään sekä osaltaan vaikuttaa siihen, että viranomaiset ja tuomioistuimet tekevät lainmukaisia ja hyvin perusteltuja päätöksiä toteuttaen oikeutta niin kuin on lainsäädännössä tarkoitettu.

Ennen metodin lopullista lukkoon lyömistä on vielä täsmennettävä tutkimuksen metodologista logiikkaa. Koska tutkimuksessa tarkastellaan tietoverkkojen aikaansaamisia vaikutuksia petosrikosten suhteen kokonaisvaltaisena ilmiönä pelkästään normatiivisen lähestymistavan sijaan, ei puhdas lainoppi ole riittävä keino tutkimuskysymykseen vastaamiseksi. Vaihtoehtoinen lainoppi sen sijaan tarjoaa tähän vaihtoehdon. Kolehmaisen mukaan vaihtoehtoisessa lainopissa ei haeta niinkään tietoa siitä, mitä on voimassa olevan oikeuden sisältö, vaan mitä sen pitäisi olla. Siinä vallitsevasta tuomarinideologiasta ollaan valmiita luopumaan, jos se ei johda tutkijan sisäistämän ideologian kannalta toivottuun lopputulok-

[16] Kolehmainen 2015, s. 107.
[17] Aarnio 1989, s. 304.
[18] Aarnio 1989, s. 304.

seen.[19] Näin ollen vaihtoehtoinen lainoppi nostaa esille oikeuden sisäisiä ristiriitoja ja jännitteitä. Nimenomaisesti näiden ristiriitojen ja jännitteiden avulla voidaan perustella se, mitä oikeuden pitäisi olla.[20] Parhaita mahdollisia laintulkinnallisia ratkaisuja perustelemalla oikeus hahmotetaan yhteiskunnallisena mahdollisuutena eikä vain toteutuneena tai toteutettavissa olevana tosiasiana.[21]

Hieman samalla tavoin oikeuden hahmottaa oikeuspoliittinen eli *de lege ferenda* -tutkimus, joka yhdistyy vaihtoehtoiseen lainoppiin siten, että uutta lainsäädäntöä koskeva ratkaisuehdotus muodostuu tulkintaan ja systematisointiin pyrkivän lainopin eräänlaisena oheistuotteena. *De lege ferenda* -tutkimuksen osalta tulee ymmärtää sen arvioivan erilaisia lainsäädännöllisiä ratkaisumalleja, joihin tuleva lainsäädäntö voisi perustua. Metodin käyttäjän on kuitenkin tunnistettava laintulkinnan asettamat absoluuttiset rajat ja tiedettävä, mitä hän on tekemässä. Erityisesti lukijalle on tehtävä selväksi, antaako tutkimuksen tekijä tulkintasuosituksia *de lege lata* vai *de lege ferenda*, sillä näiden metodien edellyttämät perustelut poikkeavat selkeästi tosistaan. *De lege lata* tulkintasuositukset ovat oikeuslähdeoppiperusteisia, kun taas *de lege ferenda* arviointi voidaan tehdä vapaammin esimerkiksi yhteiskunnallisen tarkoituksenmukaisuusharkinnan pohjalta.

Yhteiskunnallisen tarkoituksenmukaisuusharkinnan pohjalta herää myös ajatus käsillä olevan tutkimuksen tarkoituksesta. Koska tietoverkkojen käytön yleistyminen ja rikollisuus kumpikin ovat koko yhteiskunnan läpäiseviä ilmiöitä ja koska tutkimuksen aihe ei ole puhtaan normatiivinen, tullaan tutkimuksessa väistämättä törmäämään yhteiskunnallisiin näkökohtiin vähintään kriminaalipolitiikan muodossa. Tällöin ei todennäköisesti voida välttyä ottamasta kantaa näihin näkökohtiin, eikä toisaalta tutkimustulosten saavuttamisen vuoksi tällaista kannanottoa pitäisikään vältellä. Näin ollen tutkimuksessa voidaan käyttää johtopäätösten osalta *de lege ferenda* -metodia, vaikka tutkimuksen yleisote onkin vaihtoehtoislainopillinen. Rikollisuuden ja tietoverkkojen tarkastelussa yhteiskunnallisina ilmiöinä ei voida myöskään välttyä empiiristen lähteiden hyödyntämiseltä vaarantamatta tutkimuksen tuloksia.

---

[19] Siltala 2003, s. 525.
[20] Wilhelmsson 1997, s. 343–352. Toisaalta vaihtoehtoista lainoppia kohtaan voidaan esittää myös perusteltua kritiikkiä, sillä opissa oikeuden pääsäännöt muuttuvat poikkeussäännöiksi ja päinvastoin. Tämän voidaan katsoa olevan metodin heikko kohta, sillä tälle vaihtelulle ei ole kyetty esittämään kattavia metodologisia perusteita. Kysymys on siis siitä, mikä oikeuttaa korottamaan oikeuteen jollain lailla päässeen poikkeussäännön pääsäännöksi. Ks. Helin 1998, s. 311–312.
[21] Wilhelmsson 1997, s. 347–353 ja Siltala 2003, s. 62 ja 544.

Empiirinen oikeustutkimus kohdistaa huomion oikeuteen sellaisena kuin se tosiasiallisesti tulee sovelletuksi ja ymmärretyksi lainsoveltajien eli tuomioistuimien, viranomaisten kansalaisten ja yrityksien keskuudessa. Empiirisen oikeustieteen kysymyksenasettelut tarkastelevat empiiristä kysymystä määrällisten tai laadullisten menetelmien avulla. Tarkastelunäkökulmana voi olla tällöin vaikkapa se, miten lainsäätäjä tai lainsoveltaja on toiminut sen sijaan, miten näiden olisi voimassa olevan oikeuden valossa pitänyt toimia. Empiiristen menetelmien avulla voidaan kuvailla vallitsevaa oikeudellisesta tilaa ja sen yhteiskunnallista merkitystä. Tällä on merkitystä etenkin oikeusjärjestyksen kehittämisen ja lainvalmistelun näkökulmasta. Oikeuden empiirinen tutkimus vaatii tavanomaisesti eri tutkimusperinteiden teoreettisten ja metodologisten lähtökohtien kekseliästä yhdistämistä. Erilaisia tutkimusmetodeja yhdistämällä voidaan oikeudellisesta ilmiöstä saada monipuolisempi ja kokonaisvaltaisempi käsitys.[22] Oikeudellisen tutkimuksen tiedonintresseissä on nykyään entistä useammin tuottaa empiiristä tietoa oikeuden ja yhteiskunnan välisistä ilmiöistä.[23]

Näin ollen tässä tutkimuksessa hyödynnetään lainopin ohella myös empiiristä lähestymistapaa. Yksi tutkittavaa ilmiötä esittelevä taulukko ei kuitenkaan vielä tee tutkimuksesta empiiristä.[24] Samalla tutkimuksessa tiedostetaan, ettei haastattelun tuottaminen tai muut vastaavat toimet vielä itsessään tee tutkimuksesta empiiristä. Tutkimuksen tutkimuskysymyksiä lähestytäänkin lähtökohtaisesti perinteisin ja vaihtoehtoisin oikeusdogmaattisin keinoin systematisointia ja tulkintaa pääasiallisina työkaluina käyttäen.[25] Näiden työkalujen käyttöön ei kuitenkaan lukkiuduta, vaan tarvittaessa tuodaan esille ja käsitellään myös empiirisiä ja oikeuspoliittisia näkökohtia. Näin tutkimuksen kohteesta voidaan muodostaa niin selkeä ja kokonaisvaltainen kuva kuin mahdollista, mikä auttaa ymmärtämään tutkimuskysymykseen vastaamiseksi vaadittavat seikat.

[22] Sutela 2019.
[23] Keinänen – Väätänen 2015.
[24] Sutela 2019.
[25] On pidettävä mielessä, että eri tiedonintressejä sisältävien erilaisten lainopin tulkintatapoja yhdistelemisessä on kiinnitettävä huomiota siihen, että näin toimiessa ei vaaranneta työn tieteellistä johdonmukaisuutta. Kolehmainen 2015, s. 108.

2 Petos modernissa rikosoikeudessa

2.1 Petoksen määritelmä

Suomen rikoslaissa (1889/39) on useita erilaisia petosrikosten tunnusmerkistöjä. Verkkopetoksia ei ole erikseen kriminalisoitu, vaan tavanomaisesti verkkoa hyväksikäyttäviä petoksia tarkastellaan yleisen petosrikostunnusmerkistön kautta. Näin ollen verkkopetosten käsittelyssä tulee lähteä liikkeelle yleisluontoisen petoksen ymmärtämisestä. Petos määritellään Suomen rikoslain 36 luvun 1 §:ssä ja törkeä tekomuoto saman luvun 2 §:ssä. Rikoslain (RL) 36:1:n mukaan petoksesta rangaistaan sitä, joka hankkiakseen itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä.

Pykälän toisessa momentissa on huomioitu erityisesti tietoverkot petosten alustana. Niin sanotusta tietojenkäsittelypetoksesta rangaistaan sitä, joka 1 momentissa mainitussa tarkoituksessa dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan tietojenkäsittelyn lopputuloksen vääristymisen ja siten aiheuttaa toiselle taloudellista vahinkoa. Myös tällaisen petoksen yritys on rangaistava. Huomionarvoista on, että tietojenkäsittelypetoksessa ketään ihmistä ei suoranaisesti erehdytetä, vaan kohteena on automaattinen tietojenkäsittely, jonka seurauksena hankitaan oikeudetonta taloudellista hyötyä tai aiheutetaan taloudellista vahinkoa toiselle taholle. Tällaista tietojärjestelmään kohdistuvaa erehdyttämistä on muun muassa maksullisen verkkopalvelun virheen hyödyntäminen sellaisella tavalla, että palvelu on mahdollista saada ilmaiseksi. On kuitenkin huomioitava, että esimerkiksi verkkokaupan itse tekemän hinnoitteluvirheen hyödyntäminen ei ole rangaistavaa.[26]

Tunnusmerkistöstä nähdään, että petoksen rangaistavuudella on seitsemän kriteeriä: taloudellisen hyödyn tavoittelu, hyödyn oikeudettomuus, erehdyttäminen tai erehdyksen hyväksikäyttäminen, erehdyttämisestä aiheutuva erehdys, erehdyksen vallassa tehty määräämistoimi, määräämistoimesta aiheutuva taloudellinen vahinko sekä tahallisuus. Petoksen rangaistavuus edellyttää siten tekijän välittävän virheellistä, puutteellista tai harhaanjohtavaa,

[26] Rikoslain 36 luvun 1 §:n 2 momentissa tarkoitettu tietojenkäsittelypetos liittyy Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen 8 artiklan kansalliseen täytäntöönpanoon. Ks. tarkemmin HE 2/2003 vp; HE 153/2006 vp, s. 20–21 ja Pihlajamäki 2004, s. 191–204.

informaatiota, jonka vuoksi toinen osapuoli eli asianomistaja erehtyy. Edelleen petoksen rangaistuus vaatii asianomistajan tekevän virheellisen, muutoin puutteellisen tai tosiasioiden kanssa ristiriitaisen tiedon perusteella määräämistoimen aiheuttaen tällä menettelyllä seurauksen, joka voidaan katsoa taloudelliseksi vahingoksi.[27] Jo tappion syntymisen välitön vaarakin saattaa merkitä sellaista taloudellisen aseman todellista heikentymistä, että sitä voidaan pitää tunnusmerkistössä tarkoitettuna taloudellisena vahinkona, vaikka lopullinen tappio ei vielä olisikaan syntynyt.[28] Taloudelliseen vahinkoon johtavan määräystoimen osalta on puolestaan oikeuskirjallisuudessa todettu, että petoksen määräämistoimi on yleensä oikeustoimi, kuten kauppasopimuksen solmiminen tai luoton myöntämistä koskeva sitoumus.[29] Tunnusmerkistössä on kuitenkin tarkoituksellisesti vältetty käyttämästä käsitettä oikeustoimi, koska määräämistoimi voi olla pelkkää tosiasiallista toimintaa eli tekemättä jättämistä. Lain esitöissä on esitetty esimerkkinä tilanne, jossa velkoja erehdytetään luopumaan saatavan perimisestä, jonka seurauksena saatava vanhentuu.[30]

Erehdyttäminen ja erehdyksen käsite ovat petossäännöksen rangaistavuuden keskiössä. Itse säännökseen sisältyy kaksi eri tekomuotoa. Avainasemassa ovat erehdyttäminen ja erehdyksen hyväksikäyttäminen. Erehdyttäminen on edelleen mahdollista jakaa aktiiviseen ja konkludenttiseen erehdyttämiseen. Aktiivisen erehdyttämisen ollessa kyseessä toiselle osapuolelle välitetään virheellistä informaatiota, joka on tälle osapuolelle annettavan selityksen eksplisiittinen osa.[31] Tapani käyttää esimerkkinä tilannetta, jossa A tilaa X Oy:n nimissä tuotteita kertoen X Oy:n olevan maksukykyinen, vaikka tosiasiassa X Oy on maksukyvytön. Tällainen virheellinen informaatio voidaan välittää kirjallisesti, sanallisesti, sähköisesti tai elekielellä.

Konkludenttinen eli ns. hiljainen erehdyttäminen kuvaa tilannetta, jossa toisen annetaan ymmärtää tai olettaa virheellistä tietoa. Tapani käyttää esimerkkinä tilannetta, jossa asiakas menee ravintolaan ja tilaa jotakin. Tällaisessa tilanteessa asiakkaan ei ole erikseen ilmoitettava maksukyvyttömyydestään, sillä sitä ei odoteta tavanomaisessa kanssakäymisessä ja tämä herättäisi jopa epäilyjä asiakkaan tarkoituksista tai saisi aikaan ylimääräistä vaivannäköä. Tahdonilmaisuun liittyy myös vastapuolen odotus tietynlaisesta aikomuksesta. Näin

[27] Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 629.
[28] Ks. KKO 2003:88.
[29] Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 643.
[30] HE 66/1988 vp. sivu 132.
[31] Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 630.

ollen esimerkiksi sopimusta solmittaessa kumpikin osapuoli antaa ymmärtää voivansa ja haluavansa täyttää sopimusvelvoitteet.[32]

Kuten edellä on todettu, erehdyttämisen käsite on avainasemassa petoksen tunnusmerkistön käsittämiseksi. Tästä huolimatta petoksen tunnusmerkistön täyttymistä arvioitaessa on huomioitava myös informaationvaihdon toisen osapuolen johtopäätöksiin tekijän käyttäytymisestä sekä tästä syntyvistä perustelluista odotuksista, jotka vaikuttavat kommunikaation toisen osapuolen päätöksentekoon. Toisin sanoen petoksen arviointi ei saa kohdistua ainoastaan tekijän yksipuoliseen toimintaan kuten harhaanjohtavan, puutteellisen tai virheellisen tiedon levittämiseen.[33] Oikeuskirjallisuudessa tätä arviointinäkökulmaa on kutsuttu sosiaalisen oletusmallin loukkaukseksi.[34]

Erehdyttämisen lisäksi petoksen tunnusmerkistön täyttymisen kannalta itse erehdys on oleellinen käsite. Erehdys voidaan määritellä virheelliseksi ja todellisuutta vastaamattomaksi mielikuvaksi sellaisesta asiasta, joka on omiaan vaikuttamaan henkilön toimintaan tai päätöksentekoon.[35] Erehdyttäminen johtaa erehdykseen psyykkisen vaikuttamisen kautta.[36] Kyse ei ole suorasta kausaliteetista, mutta erehdyttämisen katsotaan yleensä jotenkin oleellisesti vaikuttavan erehdytetyn henkilön tahdonmuodostukseen. Syy-yhteyden arviointia ja merkitystä kuvaa esimerkiksi tapaus KKO 2004:109, jossa linjattiin, ettei asianomistajan erehdys johtunut vastaajan toiminnasta, koska tämän laiminlyöntiä ei tullut katsoa erehdyttämiseksi.[37] Erehdyksen aiheutuminen ei siten aina ole syy-yhteydessä erehdyttämiseen.[38] Syy-yhteyden lisäksi on kiinnitettävä huomiota myös siihen, kuka tai mikä taho on erehtynyt. Yleisesti ottaen petoksessa erehdyttämisen kohde, erehtynyt taho tai vahingon kärsijä on tapauksessa asianomistaja. Petoksissa, jotka kohdistuvat yrityksiin tai mui-

[32] Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 630. Ks. myös Kindhäuser 2005, s. 109–110 ja 147.
[33] Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 630.
[34] Ks. tarkemmin Kargl 2002 s. 628–629.
[35] Ståhlberg 1964, s. 15. Ks. myös Waaben 1999, s. 121.
[36] Tapani 2004, s. 137–138. Ks. lisäksi Tapani – Tolvanen 2013, s. 166–167 ja Frände 2012, s. 79.
[37] Tapauksessa KKO 2009:109 A oli valmistanut videokasetteja, joista olisi tullut suorittaa tekijänoikeuslain 26 a §:ssä tarkoitettu maksu, mutta laiminlyönyt tekijänoikeuslain 26 d §:ssä säädetyn velvollisuuden antaa Säveltäjien Tekijänoikeustoimisto Teosto ry:lle maksun perinnässä tarvittavat tiedot. Syyttäjän mukaan A:n laiminlyönti oli erehdyttänyt Teoston jättämään maksun perimättä. Koska Teosto ei ollut ollut tietoinen A:n toiminnasta, maksut olivat jääneet perimättä. Korkeimman oikeuden mukaan Teostolle ei ollut syntynyt laiminlyönnin vuoksi todellisuutta vastaamatonta mielikuvaa. A:n ei siten katsottu menettelyllään syyllistyneen petokseen. Tapaus oli äänestysratkaisu.
[38] Erehdyttämisen ja erehdyksen syy-yhteydestä tarkemmin ks. Jareborg 2001, s. 161; Puppe 2000, s. 59 sekä Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 636–638.

hin oikeushenkilöihin, erehdytetään luonnollista henkilöä, joka voi tehdä oikeushenkilöä sitovia toimia.[39]

Toinen mahdollinen tapa tehdä petos on tunnusmerkistön mukaan erehdyksen hyväksikäyttäminen. Tällöin tekijä aiheuttaa taloudellista vahinkoa tai hyötyy oikeudettomasti toisen kustannuksella siten, että jättää korjaamatta havaitsemansa toisen tahon erehdyksen. Lain esitöissä korostetaan tätä oikeudellista velvollisuutta korjata toisen erehdys. Käytännössä oikeudeton hyötyminen voi ilmetä hallituksen esityksen mukaan esimerkiksi siten, ettei tekijällä ole alun perinkään aikomusta täyttää velvoitteitaan, vaan hän pyrkii ainoastaan hyötymään vastapuolen suorituksista tämän kustannuksella.[40]

Lopulta on tarkasteltava vielä asianomistajan myötävaikutuksen arviointia. Lähtökohtana on asianomistajien oma ja normatiivinen vastuu hankkimastaan informaatiosta ja sen perusteella tapahtuvasta toiminnasta. Asianomistajien on siis noudatettava tiettyä huolellisuutta taloudellisten ja muiden varallisuuden kannalta merkityksellisten asioidensa hoidossa saadakseen rikosoikeudellista suojaa osakseen.[41] Myötävaikuttamisen arviointiin vaikuttaa informaation hankinnan huolellisuus, taloudellisen toiminnan ja samalla mahdollisten vahinkojen laajuus sekä epäilyksen herättävät seikat informaation todenperäisyydestä. Selonottovelvollisuuden arviointi on yleisimmin relevanttia liike-elämän taloudellisissa suhteissa.[42]

Petossäännöksen tarkoituksena on ensisijaisesti varallisuuden suojaaminen. Tämä tarkoitus perustuu perustuslain (PL) 15 §:n ja Euroopan ihmisoikeussopimuksen (EIS) ensimmäisen lisäpöytäkirjan 1 artiklaan.[43] Varallisuuden suojaaminen puolestaan turvaa yksilöiden taloudellista toimintavapautta vahvistamalla kaupanteon ja vaihdannan vaatimaa luottamusta. Taloudellisia sopimussuhteita solmittaessa ja niistä neuvoteltaessa sopimusosapuolten sekä muiden vastaavien toimijoiden tulee voida luottaa toisen osapuolen toimivan rehellisesti. Oikeuskirjallisuudessa tätä suhdetta on pyritty jäsentämään oikeus totuuteen -

[39] Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 637.
[40] HE 1988/66 vp, s. 131–133.
[41] Tarkemmin selonottovelvollisuudesta petoksen suhteen ks. Tapani 2004, s. 175–196 ja Tapani 2017, s. 309–318. Ks. lisäksi KKO 1995:23; KKO 1995:24; KKO 1995:25 sekä KKO 2011:84.
[42] Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 642.
[43] Tapani 2004, s. 82. Tarkemmin omaisuudensuojasäännöksistä ks. Länsineva 2002, s. 191–204.

käsitteen avulla.[44] Ihmisten erehdyttäminen evää heiltä mahdollisuuden tämän vapauden hyödyntämiseen.[45]

2.2 Petos taloudellisena rikoksena

Petoksen rikostunnusmerkistön määrittelyn jälkeen on syytä laajentaa näkökulmaa petoksen tarkastelun suhteen. Verkkopetokset ovat laaja ilmiö, jotka maksavat valtioille, yrityksille sekä yksityisille erittäin suuria summia rahaa. Rahassa mitattuna ja ilmiön laajuuden huomioiden voidaan puhua verkkopetoksista talousrikollisuutena. Käytännössä tämä käsitteellinen luokittelu merkitsee hieman erilaista lähestymistapaa ilmiön suhteen. Verkkopetosten luokittelu talousrikoksiksi tarjoaa myös perustellun kriminaalipoliittisen näkökulman aiheeseen.[46]

Talousrikokselle ei ole yksiselitteisesti hyväksyttyä määritelmää kansainvälisesti.[47] Termin määritelmä ei ole täysin vakiintunut myöskään Suomessa.[48] Rajanveto tavanomaisen omaisuus- ja varallisuusrikoksen välillä ei ole aina selkeää.[49] Määritelminä on käytetty toisaalta kaikkeen taloudelliseen hyötyyn tähtäävää toimintaa, mutta toisaalta vain tiettyjen rikoslain lukujen mukaisia rikoksia.[50] Verkkopetokset muistuttavat selkeästi talousrikoksia huomattavan hyödyn tavoittelun sekä suhteellisen pienen kiinnijäämisen riskin osalta – tietojenkalasteluviestin lähettäminen tuhansille tahoille on kiinnijäämis- ja sanktioriskiltään vähäinen, mutta teolla tavoiteltu taloudellinen hyöty voi olla hyvinkin suurta. Talousrikosten ydinosasta puhuttaessa viitataan yleensä sellaisiin rikoksiin, joita tehdään lähtökohtaisesti ansaitsemistarkoituksessa ja tavoitellaan suoraa taloudellista hyötyä, kuten esimerkiksi rikoslain veroihin liittyvät rikokset, velallisen epärehellisyydestä johtuvat rikokset, elinkeinoelämän rikokset, sekä arvopaperimarkkinarikokset.[51] Oikeuskirjallisuuden perusteella

[44] Kindhäuser 1991, s. 398 ja Pawlik 1999, s. 82–83.
[45] Frände – Matikkala – Tapani – Tolvanen – Viljanen – Wahlberg 2018, s. 630. Ks. myös Vogel 2003. s. 318–322 ja KKO 2008:38.
[46] Ks. Pirjatanniemi 2005, s. 269–274. Kriminaalipolitiikalla tarkoitetaan rikollisuuden hallitsemiseen tähtäävää yhteiskunnallista päätöksentekoa, joka kohdistuu rikollisuuteen ja rikosoikeuteen. Määritelmä voidaan käsittää suppeasti tai laajasti. Suppean käsityksen mukaan kriminaalipolitiikka jäsennetään kriminalisointiteoriaksi eli päätöksenteoksi tekojen rangaistavuuden rajoista. Laajan käsityksen mukaan kriminaalipolitiikka sisältää puolestaan varsinaisen rikosoikeuspolitiikan lisäksi koulutuspolitiikan, sosiaalipolitiikan sekä rikostorjunnan kokonaisuudessaan. Tolvanen 2005, s. 126.
[47] Delem 2011, s. 61.
[48] Pirjatanniemi 2005, s. 268–269.
[49] Ks. Träskman 1981, s. 13.
[50] Määttä – Hirvonen 2018, s. 249–250.
[51] Paukku 2021, s. 29.

määrittelyä voidaan lähestyä myös arvioinnin huomion kiinnittämisellä teosta ulkoisesti pääteltäviin ominaisuuksiin. Esimerkiksi Axbergerin mukaan talousrikoksen on oltava tietyin tavoin kehittynyt, suunniteltu sekä harkittu teko, jonka on pohjimmiltaan perustuttava talousjärjestelmän sääntöjen väärinkäyttöön.[52] Eräs tapa jaotella talousrikollisuutta on myös tarkastella ovatko rikokset tehty kokonaan laittomassa toiminnassa vai laillisen toiminnan yhteydessä.[53] RL 36:1 §:n petos on joissain yhteyksissä jätetty kokonaan talousrikosten ydinryhmän ulkopuolelle.[54] Toisissa yhteyksissä petoksen on taas argumentoitu olevan osa talousrikoksia, jotka tulisi muutoinkin ymmärtää laajasti.[55]

Mikäli petos katsotaan taloudelliseksi rikokseksi, olisi petostunnusmerkistöön sisältyvät verkkopetokset katsottava luonnollisesti myös talousrikoksiksi. Ymmärrettävästi voi olla kuitenkin hankalaa samaistaa perinteinen, monimutkainen ja vuosia jatkunut valkokaulusrikos,[56] kuten pankin toiminnassa tapahtuva arvopaperimarkkinarikoksiin lukeutuva sisäpiirin tiedon väärinkäyttö, tyypilliseen verkkohuijaukseen, jossa yksityinen henkilö myy toiselle 50 euron arvoisen videopelin internetissä toimivan kauppa-alustapalvelun välityksellä jättäen pelin kuitenkin toimittamatta maksun saatuaan. Jälkimmäisen kuvauksen mukainen teko voidaan helposti mieltää tavanomaiseksi ja suhteellisen merkityksettömäksi massarikokseksi, johon eivät täsmää talousrikosten tavanomaiset tunnusmerkit. Verkkopetokset tulee kuitenkin asettaa oikeaan kontekstiin, jotta niiden luonnetta ja olemusta voidaan todella ymmärtää.

Verkkopetoksia tehdään määrällisesti hyvin paljon, usein saman tekijän toimesta. Kun edellä kuvatun kaltainen myyntipetos toteutetaan saman tahon toimesta satoja tai tuhansia kertoja ja mahdollisesti monen eri valtion alueella, voidaan yksittäiset rikolliset teot nähdä

---

[52] Esimerkkeinä Axberger on esittänyt vero- ja tullirikokset, lahjonnan sekä sisäpiirintiedon väärinkäytön. Ks. Axberger 1988, s. 18−20.
[53] Pirjatanniemi 2005 s. 262–263.
[54] Esimerkiksi rikoslaissa petokset ovat jätetty talousrikos-otsakkeen ulkopuolelle. Sen sijaan useita muita petoksen lajeja kuten veropetoksia ja velallisen petosta pidetään vakiintuneesti talousrikollisuuden alaan kuuluvina tekoina. Lisäksi maksuvälinepetokset liittyvät usein saumattomasti rahanpesuun, jota pidetään myös useimmiten talousrikoksena.
[55] Ks. esimerkiksi Tapani 2004, jonka koko tutkimuksen lähtökohtana toimii petosrikosten lukeminen talousrikoksiksi.
[56] Termillä valkokaulusrikos viitataan usein talousrikoksiin, mutta käsitteitä ei voida pitää kaikilta osin yhtenevinä. Ks. tarkemmin Friedrichs 1996, s. 5–11. Talousrikostutkimuksen uranuurtajana ja jopa oppi-isänä pidetty Edwin H. Sutherland teki käsitteen tunnetuksi kriminologian perusteoksiin lukeutuvassa tutkimuksessaan White Collar Crime. Sutherlandin mukaan valkokaulusrikoksilla tarkoitetaan rikoslajeja, joihin korkean yhteiskunnallisen aseman omaavat ja arvossa pidetyt henkilöt tyypillisesti syyllistyvät ammattiasemansa kautta, kuten esimerkiksi kartellit, kilpailunrajoitukset ja rahoituspetokset. Pirjatanniemi 2005, s. 262. Tarkemmin valkokaulusrikollisuuden määritelmästä Ks. Sutherland 1983, s. 63–197.

samana kokonaisuutena. Tästä näkökulmasta rikollinen toiminta on systemaattista, laajaa ja mahdollisesti pitkäaikaista. Samalla useista pieniä summia koskevista petoksista voi kertyä tekijälle yhteenlaskettuna merkittäväksi katsottavaa taloudellista hyötyä. Oikeuskäytännössä on esitetty tätä näkökulmaa tukevia kannanottoja. Esimerkiksi Helsingin hovioikeuden (HelHO) 24.05.2018 antamassa ratkaisussa R 17/1965 todettiin useista verkkopetoksista koostuvan rikoskokonaisuuden suhteen, että jokaisen petollisen myyntiilmoituksen julkaiseminen vaatii erillisen päätöksen rikokseen ryhtymisestä.[57] Varsinkin pidemmällä aikavälillä tällainen toiminta merkitsee väistämättä rikoksentekijän suunnitelmallisuutta ja määrätietoisuutta. Suunnitelmallinen toiminta on taas ominaista esimerkiksi organisoiduille ja ammattimaisille rikollisille. Tällaiset tahot ovatkin hyvin usein verkkoa hyödyntävien petosten suunnittelun sekä toteutuksen takana.[58] Huomionarvoista on, että järjestäytynyt rikollisuus luetaan usein talousrikollisuuden alaan kuuluvaksi rikollisuuden muodoksi.[59] Lopuksi verkkopetokset tulee asettaa niiden omaan viitekehykseen.

Tarkasteltaessa verkkopetoksia niiden omassa kontekstissa, eli rikollisilta mahdollisuuksiltaan runsaassa ja samalla rikostekojen määrää nostavassa rajat ylittävässä tietoverkkotoimintaympäristössä, huomataan suhteellisen yksinkertaisiinkin verkkopetoksiin liittyvän erittäin monia talousrikoksille tunnusomaisina pidettyjä piirteitä, kuten suunnitelmallisuus, tekojen mahdollinen pitkällä aikavälillä tapahtuminen sekä matala kiinnijäämisen riski suhteessa merkittävän taloudellisen hyödyn tavoitteluun. Samalla laajoissa ja monimutkaisissa, ammattirikollisten toteuttamissa isoihin taloudellisiin toimijoihin kuten pankkeihin kohdistuvissa verkkopetoksissa yhteydet talousrikoksiin huomataan selvemmin ilman kontekstuaalisten perusteluiden tarvetta. Tässä valossa verkkopetosten lukeminen talousrikoksiksi vaikuttaa perustellulta.

---

[57] Ratkaisussa HelHo R 17/1965 yli sadassa eri syytekohdassa syytettynä ollut X oli syyllistynyt kahden vuoden aikana huomattavaan määrään verkkokauppoihin kohdistuvia petoksia tilaamalla toistuvasti väärennettyjen tai luvattomasti hankittujen henkilötietojen avulla tuotteita ilman aikomusta maksaa niistä. Tuomioistuimen perusteluissa katsottiin jokaisen tilauksen edellyttävän erillistä rikoksentekopäätöstä. Tämän puolestaan katsottiin merkitsevän yhdessä rikosten tekemisen pitkäaikaisuuden kanssa, että menettely osoitti jatkuvaa pyrkimystä laittoman hyödyn saamiseen ja tällaisen pyrkimyksen laittoman hyödyn saamiseen vaativan erityistä päättäväisyyttä ja järjestelmällisyyttä. Näiden perusteluiden pohjalta tuomioistuin totesi rikostekojen olevan yhteydessä toisiinsa, mikä merkitsi menettelyn vaativan merkittävää suunnitelmallisuutta ja siten rangaistuksen ankaroittamista.

[58] Haasio 2017, s. 75 ja Kyberrikostorjuntakeskus 2020, s. 4.

[59] Esim Träskmanin luoman jaottelun mukaan talousrikollisuus voidaan jakaa niihin rikoksiin, jotka tehdään sinänsä laillisen toiminnan puitteissa sekä sellaisiin rikoksiin, jotka ovat *de facto* itsessään laitonta toimintaa. Ensimmäistä ryhmää kutsutaan talouselämän rikollisuudeksi, kun taas jälkimmäistä organisoituneeksi taloudelliseksi rikollisuudeksi. Träskman 1981, s. 15–18. Organisoidun rikollisuuden mahdollisuudesta lukeutua talousrikokseksi ks. Alvesalo 1994, s. 71–75 sekä Tapani 2004, s. 97–98.

Tämä rinnastus vaatii toimiakseen kuitenkin sen, että verkkopetokset tosiaan tehdään laajoina kokonaisuuksina ja suunnitelmallisesti. Yksittäisen verkkopetoksen tekevän henkilön, jonka teko jää ainoaksi tai lukeutuu muutamiin epäsäännöllisiin kertoihin, ei voida lähtökohtaisesti nähdä toimivan suunnitelmallisesti, määrätietoisesti tai osana ammattirikollisuutta. Yksittäiset epäsäännölliset teot eivät siten muodosta sellaista aiemmin kuvailtua rikoskokonaisuutta, joka perustelee verkkopetoksien rinnastuvan talousrikoksiin. Tällöin ainoa yhdistävä jäljelle jäävä tekijä on taloudellisen hyödyn tavoittelu. Tutkimuksen näkökulman riittävän kattavuuden vuoksi verkkopetoksia on tarkasteltava siis tästä lähtökohdasta. Vain lukumääriltään suuriin petoskokonaisuuksiin keskittyminen johtaisi yksittäisten, mutta laajuudeltaan ja tavoitelluilta taloudellisilta hyödyiltään merkittävien verkkopetosten arvioinnin laiminlyöntiin. Samalla vain taloudellisesti merkittävien ja yleensä yrityksiin kohdistuvien verkkopetosten painottaminen jättäisi tunnustamatta suurimman osan tilastoiduista petoksista, jolloin huomiota ei voitaisi riittävästi kiinnittää useiden pienempien petosten muodostamiin kokonaisuuksiin.

Näin ollen tutkimuksessa verkkopetoksia ei tarkastella talousrikoksina tiukan tulkintatavan mukaan kategorisesti rikosnimikkeen tai tekotavan perusteella, vaan laajemmasta näkökulmasta teon vaikuttimien perusteella. Termiä ”talousrikos” käytetään siis sellaisista rikoksista, joiden tarkoituksena on saavuttaa taloudellista hyötyä. Lavea määritelmä jättää sijaa taloudellisina rikoksina hyvin vähämerkityksisillekin verkkopetostyypeille, mutta tällaisten tekojen käsittely voidaan tutkimuksen näkökulman perusteella jättää vähäiseksi.

2.3 Talousrikoksen käsite kriminaalipolitiikan välineenä

Käsitteen määrittelyn tarve voidaan kuitenkin kyseenalaistaa. Mitä konkreettista hyötyä verkkoavusteisten petosten määrittelystä talousrikokseksi on? Tulkitsemalla taloudellisen rikollisuuden käsite laveasti annetaan kriminaalipoliittisille päätöksentekijöille selkeä signaali, jonka mukaan he voivat vapaasti kohdentaa rikoksentorjunnan tavoitteet ja suuret linjat haluamaansa suuntaan. Tosin sanoen taloudellisen rikollisuuden käsitettä koskevassa dilemmassa ovat aina mukana erimielisyydet kriminaalipolitiikan suunnasta.

Käsitteiden sisällön määrittelemisen oleellisuus on ymmärretty jo pitkään. Esimerkiksi Hans-Gunnar Axberger on kiteyttänyt määritelmien tärkeyden hyvin - valtiollisessa kriminaalipolitiikassa talousrikostermiä ei ole käytetty niinkään ilmiön kuvaamiseksi taikka selityksenä, vaan enemmänkin kriminaalipoliittisen ongelman paikantamisen keinona: ”*Dess*

[definitionens] syfte är också – och kanske primärt – att fixera den måltavla mot vilken vissa rättspolitiska åtgärder skall riktas. Det är skillnad mellan en politiskt neutral beskrivning av en viss typ av brottslighet (ekonomisk brottslighet) och en politisk bestämning av utgångspunkten och målet för vissa politiska åtgärder (”EKO-brott”).”[60] Pelkästään velallisen rikoksiset ja verorikokset tunnustava talousrikosmääritelmä vie lainkäyttäjän toisenlaisiin painotuksiin kuin esimerkiksi verkkopetos-, kuluttaja- sekä ympäristörikokset kattava käsite. Siten kulloinkin yleisesti vallalla oleva ja omaksuttu talousrikoksen määritelmä ei ole ainoastaan informatiivinen, vaan sen lisäksi se on myös ohjaava.[61]

3 Verkkoavusteiset petosrikokset

3.1 Verkkopetoksista yleisesti

Taloudellisella petosrikollisuudella on äärimmäisen monia esiintymismuotoja. Vaikka verkkoavusteisista petoksista annetaan Suomessa tietoa ja varoituksia median sekä viranomaisten toimesta, tämä ei ole hillinnyt petosmäärien jatkuvaa kasvua.[62] Vuonna 2020 nettipetoksia koskevia rikosilmoituksia rekisteröitiin poliisissa noin 20 600.[63] RL 36 luvun 1–3 §:ien mukaisia petosrikoksia tuli poliisin tietoon samana vuonna yli 30 000, eli merkittävä osa petosrikoksista oli nettipetoksia.[64]

Verkkopetosten suurta ja vuosi vuodelta kasvavaa määrää selittää verkkopetosten tekemisen vaivattomuus sekä toisaalta verkkoon pääsyn yleistyminen. Koko yhteiskunta rakentuu nykyään tietoverkkojen toimivuuden varaan ja merkittävä osa kaikesta ihmisten sekä yritysten keskisestä tietojenvaihdosta tapahtuu internetin välityksellä. Luonnollisesti myös petosrikokset ovat siirtyneet verkkoon muiden palvelujen ja yhteiskunnallisten toimintojen tavoin. Internet voidaankin hahmottaa uutena foorumina rikoksentekijöille. Jos 1990-luvulla tilasi puhelinluettelosta postitse tuotteen ilman aikomustakaan maksaa tuotetta, täyttyi mitä todennäköisimmin petoksen tunnusmerkistö. Samaten olemattoman tuotteen myyminen ilmoitustaulun ilmoituksen välityksellä tai torilla katsotaan petokseksi. Rikos on petoksen tunnusmerkistön osalta sinänsä tismalleen sama, jos tuote tilataan 2020-luvulla

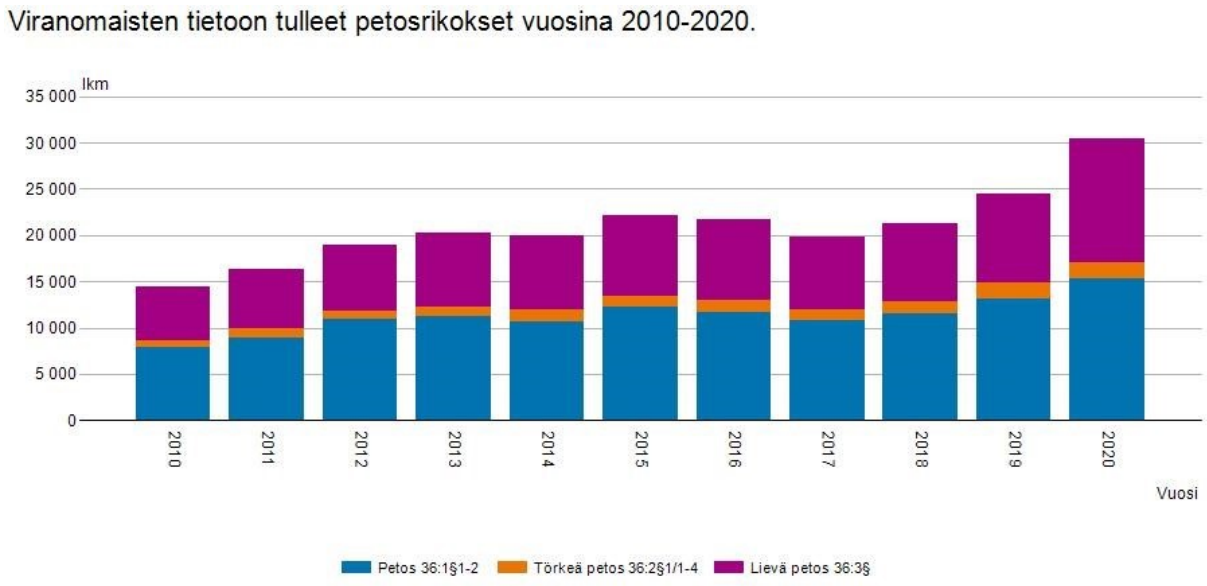
[60] Axberger 1988, s. 17.
[61] Pirjatanniemi 2005, s. 269. Ks. myös Träskman 1987, s. 124 ja Korsell 2000, s. 937.
[62] Ks. esim. tilastokeskus 2020a.
[63] Lehtinen 2021.
[64] Tilastokeskus 2020a. Nettipetoksiksi on poliisin tilastoissa luokiteltu petosrikokset, joiden tekopaikaksi on kirjattu internet. Näitä ovat petos ja maksuvälinepetos lievine ja törkeine tekomuotoineen, maksuvälinepetoksen valmistelu sekä petoksen ja törkeän petoksen yritykset. Ks. Riekkinen 2018, s. 75.

internetin välityksellä verkkokaupasta ilman aikomusta maksaa tuotteesta tai jos olemassa olematon tuote myydään verkossa yleisellä kauppasivustolla. Internet ei ole tästä näkökulmasta rikostunnusmerkistön kannalta tai muutoinkaan rikosoikeudellisesti kovin oleellinen tekijä – verkkoympäristö on vain rikoksentekopaikka, puhelinluettelon ja ilmoitustaulun seuraaja, samoin kuin tori.fi -sivusto on perinteisen torin seuraaja.

Verkkoympäristön vaikutus ei ole kuitenkaan näin yksioikoista. Petosten nousua rikostilastoissa selittää osaltaan juuri tämä uusi rikoksentekopaikka. Verkkopetosten tekeminen on huomattavasti nopeampaa ja vaivattomampaa kuin ansaintalogiikaltaan samanlaisten, mutta verkkoa hyödyntämättä jättävien petosten tekeminen. Tässä mielessä internet on toimintaympäristönä nostanut petosrikosten määrää valtavasti suhteutettuna tavanomaiseen rikollisuuden kehitykseen.[65] Esimerkiksi vuosien 2010–2020 välisenä aikana kavallus- ja petosrikokset, veropetokset poissulkien, ovat ainoa rikollisuuden muoto, jonka määrät lisääntyivät muiden rikollisuuslajien määrien pysyessä jokseenkin stabiileina tai vähentyessä.[66] Kohdistaessa tarkastelu yksinomaan RL 36 luvun 1–3 pykäliin kehityskulku on vielä helpommin hahmotettavissa.

[65] Ks. Tilastokeskus 2020a sekä tilastokeskus 2020b.

[66] Kaikkien rikostyyppien yhteenlaskettu kokonaismäärä on ollut pääsääntöisesti laskusuuntainen vuoden 1990 jälkeen. Vuonna 1990 rikosten määrä oli 1 150 rikosta väestön 10 000 asukasta kohti, kun taso vuonna 2019 oli enää vain 819. Rikostilastoja tulkittaessa on kuitenkin huomioitava eri rikoslajien kehityksen riippuvan rikollisuuden todellisen lisääntymisen ja vähenemisen ohella myös siitä, miten aktiivisesti rikosten uhriksi joutuneet ilmoittavat niistä poliisille. Poliisilta tilastoiden ulkopuolelle jäävien rikosten osuus on usein suurempi niin sanotuissa massarikoksissa, kun taas vakavammat rikokset tulevat huomattavasti useammin poliisin tietoon. Petokset voidaan yleisyytensä puolesta katsoa mainitunlaisiksi massarikoksiksi, mikä korostaa verkkopetosten merkittävyyttä rikollisena ilmiönä. Ilmi tulevien rikosten määrään vaikuttaa tietenkin myös viranomaisten valvonnan tehokkuus ja valvonnan suuntaamisen suuret linjat. Ks. tarkemmin Danielsson 2020, s. 5–7.



Kuvio 1. Viranomaisten tietoon tulleet petosrikokset vuosina 2010–2020. Lähde: Tilasto-keskus, rikos- ja pakkokeinotilasto (Tilastokeskus 2020a).

Kuviosta 1 on nähtävissä petosten tasainen ja huomattava nousu aina vuoteen 2020 asti, jolloin petosrikosten määrä nousi yli 24 % edellisvuoteen nähden. Kaikkiaan petosrikoksia tilastoitiin vuonna 2020 30 496 kappaletta, joista vajaat kuusi prosenttia oli tekomuodoltaan törkeitä, kun taas vuonna 2010 petosrikoksia tilastoitiin alle 15 000. Kymmenessä vuodessa petosrikosten määrä on kasvanut yli kaksinkertaiseksi.[67]

Verkkoympäristöllä on siten ensinnäkin petosten määrää lisäävä vaikutus. Tähän syynä on esimerkiksi verkkoasioinnin voimakkaasti laajentunut käyttö tuotteiden ostamisessa ja pankkiasioiden hoidossa.[68] Toinen verkkopetosten yleinen piirre potentiaalisten erehdyttämiskohteiden suuri määrä ja tietoverkkojen anonymiteetista johtuva matala kiinnijäämisen riski. Kolmas verkkoavusteisille petoksille tunnusomainen piirre on saman teon vaikutusten suuri varianssi. Yksittäisen tietojenkalastelupetoksen, jossa petoksentekijä esittää olevansa pankista ja pyytää vastaanottajan pankkitietoja, vaikutukset voivat petoksen uhrista riippuen vaihdella vain kymmenistä euroista miljooniin pankkitilillä olevista varoista tai tilin nostoasetuksista riippuen. Esimerkiksi vuonna 2013 tällainen petos aiheutti 1,1 miljoonan punnan taloudellisen menetyksen St. Aldhelmin akatemialle Dorsetissa petoksen

[67] Viranomaislähteiden lisäksi petosrikosten viime vuosien aikaista lisääntymistä indikoi viimeaikaiset kyselytutkimukset. Esimerkiksi vuoden 2019 kansallisessa rikosuhritutkimuksessa 5,2 prosenttia vastaajista kertoi palvelun tai tavaran hankintaan liittyneestä huijauksesta kuluneen vuoden aikana. Osuus oli noussut vuodesta 2014 noin kahdella prosenttiyksiköllä. Vastaavasti myös maksuvälinepetosten esiintyvyys oli samalla aikavälillä noussut 1,5 prosentista 3,1 prosenttiin. Ks. Danielsson − Näsi 2020, s. 22.
[68] Danielsson 2020, s. 101.

tekijän pyydettyä koululaitoksen taloudenhoitajaa vahvistamaan laitoksen tilitiedot.[69] Verkkopetosten vaikutukset ja taloudellisesti mitattu vakavuus vaihtelevat siis runsaasti petoksen kohteen hallitseman varallisuuden perusteella.

Yleisimmät tuomioistuimissa käsiteltävät verkkoa hyväksikäyttävät petokset ovat yksittäisten tekojen suhteen taloudellisilta vaikutuksiltaan pieniä, mutta suurissa määrin tehtyjä tilausrikoksia, joihin saattaa liittyä maksuvälinepetoksia (RL 37:8-11) tai identiteettivarkauksia (RL 38:9a), tai yksityishenkilöihin kohdistuvia myyntipetoksia, joissa myydään tavaroita ilman aikomusta lähettää niitä.[70] Isoimmat ja monimutkaisimmat verkkopetokset kohdistuvat kuitenkin yleensä pankkeihin tai muihin suuriin taloudellisiin toimijoihin. Tällaisissa tapauksissa myöskin petoksella anastettava varallisuus on yleensä huomattavan suurta. Verkkopetosten yleisen luonnon, yhteisien tekijöiden sekä erityispiirteiden ymmärtämiseksi tulee kuitenkin ensin käsitellä kaikki erilaiset verkkoa hyväksi käyttävän petosrikollisuuden muodot.

3.2 Verkkoavusteisten petosten eri muodot

Petoksien tekemiseen on lukuisia eri tapoja. Yksityisiä toimijoita ja yrityksien palveluksessa toimivia ihmisiä voidaan erehdyttää lukemattomin eri tavoin, ja toisten erehdyksiä käytetään hyväksi jatkuvasti. Jotkin petokseen tähtäävät tai sen aikaansaavat toimintatavat ovat toisia tehokkaampia ja toiset taas helpompia toteuttaa. Näin muodostuu tietynlaisia, toteutustapojensa perusteella määriteltäviä petostyyppejä, joilla on omat ominaispiirteensä. Tällaisten ominaispiirteiden olemassaolo voi vaikuttaa teon rikosoikeudelliseen arviointiin, vaikka arviointi tapahtuisikin aina saman rikostunnusmerkistön lähtökohdista. Näin ollen erilaisten petostapojen määrittäminen, analysoiminen ja lopulta ymmärtäminen on avain näiden petostapausten kokonaisvaltaiseen rikosoikeudelliseen arviointiin ja sitä kautta myös laajempien yhteiskunnallisten rikollisuuden parissa toimivien instituutioiden tukemiseen. Vaikka organisaatiolla olisi omat selkeät sisäiset käsitteensä, laajempi yhteistyö muiden organisaatioiden ja viranomaisten kanssa ongelmien ratkaisemiseksi on haastavaa. Rikollisuuden luokittelu paitsi kokonaisuudessaan, myös yksittäisen rikostunnusmerkistön sisäisesti tarjoaa siten tärkeän työkalun kriminaalipoliittisen päätöksenteon sekä rikostorjunnan tarpeisiin. Rikosten kategorisoimisen hyödyn perustelut vastaavatkin hieman ta-

[69] Gillespie 2016, s. 133.
[70] Ks. esim. HelHo 26.03.2018, R 17/362 sekä HelHo 24.05.2018, R 17/1965.

lousrikoksen käsitteen määrittelemisen tärkeyden yhteydessä kappaleessa 2.3 esitettyä argumentaatiota.[71]

Verkkoavusteiset petokset muodostavat itsessään oman lajinsa petoksen rikostunnusmerkistön sisällä. Kuten aiemmin on tuotu esille, tietoverkkojen käyttö petoksien tekemisessä värittää selkeästi tällaisten petosten toimintalogiikkaa ja tekotapaa asettaen ne erilleen muunlaisista petoksista. Jaottelu selkenee edelleen tarkastelemalla verkkoavusteisia petoksia taloudellisina rikoksina. Yksinkertaisimmat ja taloudelliselta arvoltaan pienimmätkin verkkopetokset toteutetaan yleensä määriltään niin moninaisina, että rikoksilla mahdollisesti saatu taloudellinen hyöty muodostuu huomattavan suureksi, ja että useiden rikollisten tekojen kokonaisuus voidaan katsoa systemaattiseksi ja järjestelmälliseksi toiminnaksi. Laaja-alaiset, systemaattiset ja huomattavaan taloudelliseen hyötyyn tähtäävät verkkopetokset voidaan edelleen jaotella niiden erilaisten toimintalogiikoiden mukaan siten, että omaksi verkkopetoslajikseen katsotaan keskenään saman tai samankaltaisen toimintalogiikan pohjalta toimivat yleisesti käytetyt, kansainvälisesti tunnetut tai useammin kuin yksittäisesti tehdyt petosrikokset.

Millaisia verkkopetoksia on sitten olemassa? Erilaisten määritelmien mukaan verkossa tapahtuvia petoksia on lukuisia. Yritystoiminnassa verkkoavusteisiksi petoksiksi katsotaan niiden liiketoiminnan näkökulmasta merkittäviä petoksia, kuten haittaohjelmien levittäminen, kampanja- sekä mainostoimintaan kohdistuvat napsautuspetokset,[72] tietomurrot ja käyttäjien manipuloiminen[73] yrityssähköpostien murtamiseksi. Julkisessa diskurssissa esille nousevat puolestaan yksityishenkilöihin kohdistuvat sangen tavanomaiset verkkopetokset. Tällaisista yleisistä petoksista luonnollisesti uutisoidaan enemmän, ja vastaavasti viranomaiset pyrkivät jakamaan tietoa petosten luonteesta niiden torjumista varten. Esimerkiksi Australian liittovaltion poliisin tiedotteen perusteella internet-petoksiksi[74] voidaan luokitella muun muassa roskaposti, erilaiset huijaukset, vakoiluohjelmat, identiteettivar-

[71] Rikollisuustyyppien määrittelyä voidaan lisäksi perustella oikeustieteellisten näkökohtien lisäksi yhteiskunnallisin argumentein. Koska rikos ja rikollisuus eivät ole vain juridinen, oikeustieteessä tutkittu kuriositeetti, vaan koko yhteiskunnan läpäisevä ilmiö, voidaan perusteita ja hyötyjä rikollisuuden tutkimiselle ja tarkalle määrittelylle hakea monista eri paikoista. Näitä ovat esimerkiksi viranomaistoiminnan häiriöiden korjaamisen tarpeet, kriminologiset ja sosiologiset perusteet sekä viime kädessä taloudellisen vaihdannan toiminnan turvaaminen.
[72] Eng. click fraud.
[73] Eng. social engineering.
[74] Kansainvälisissä ja kotimaisissakin lähteissä verkkoavusteisten petosten nimitys vaihtelee runsaasti. Yleisesti käytetyt termit kuten ”internet-petos” tai ”internet fraud”, ”nettihuijaus”, ”fraud”, ”online scam”, ”cyber crime”, ”cyber-fraud”, ”online fraud” ja joissakin yhteyksissä ”financial fraud” joko osittain tai kokonaan tarkoittavat verkkoavusteisia petoksia. Vaikka termeillä on joitain käsitteellisiä eroja, ne kaikki viittaavat verkon avulla tehtäviin rikoksiin.

kaudet, tietojenkalastelu[75] tai verkkopankkipetokset.[76] Euroopan unionin virallisilla verkkosivuilla verkkopetostyypeistä on annettu vastaavanlainen kuvaus.[77] Verkkorikollisuutta koskevassa kirjallisuudessa mainitaan myös nämä rikokset, minkä lisäksi yleisiksi verkkopetoksista nostetaan romanssipetokset, sähköpostipetokset ja verkkokauppapetokset.[78] Näistä määritelmistä puuttuu kuitenkin johdonmukaisuus – verkkopetoksia kuvailtaessa luetellaan vain esimerkinomaisesti yleisimmät viranomaisten tietoon tulleet verkkoavusteisten petosten lajit. Tällainen lähestymistapa johtaa väistämättä joidenkin verkkopetoslajien, kuten harvinaisempien yrityksiin kohdistuvien petosten, käsittelemättä jäämiseen. Samalla yleisten ja tunnettujen, mutta usein taloudellisilta vaikutuksiltaan vähäisten verkkopetosten analysoiminen siirtää taloudellisen rikollisuuden näkökulmasta huomiota liiaksi pois juuri kaikkein merkittävimmistä verkkoavusteisista petoksista.

Tarkoituksenmukaisempaan lopputulokseen on päästy akateemisen jaottelun keinoin. Stabek ym. määrittelivät empiirisen tutkimuksensa pohjalta seitsemän selvästi erotettavaa eri verkkopetosten lajia.[79] Tämän jaottelun mukaan verkkoavusteisten petosten lajit olisivat:

1. Matalatasoiseen huijaukseen perustuvat petokset.
2. Tarinapohjaisiin menetelmiin perustuvat petokset.
3. Työllisuuspohjaiseen menetelmään osallistumista edellyttävät petokset.
4. Näennäispakollisiin velvoitteisiin perustuvat petokset.
5. Tiedon keräämiseen perustuvat petokset.
6. Myynti- ja asiakkuuspohjaiset petokset.
7. Markkinointiperusteiset petokset.

Jaottelu perustuu verkossa tapahtuneita petoksia kokoaviin raportteihin viranomaistahoilta sekä muutamilta yksityisiltä toimijoilta.[80] Suuri osa näistä raportoiduista verkkopetoksista on kohdistunut yksityishenkilöihin, sillä luonnollisesti massarikoksina toteutettavia yksityishenkilöihin kohdistuvia petoksia saatetaan viranomaisten tietoon eniten. Tästä syystä jaottelun parantamiseksi listaukseen tulee lisätä kahdeksas ryhmä, joka huomioi monimutkaiset ja yritystoimintaan kohdistuvat verkkopetokset. Verkkopetosluokan nimeksi voidaan antaa yritystoimintaan erikoistuvat petokset.

[75] Eng. phishing.
[76] Australian Federal Police, Internet fraud.
[77] EU:n Muuttoliike- ja sisäasioiden pääosasto, Cybercrime.
[78] Ks. Gillespie 2016, s. 133–142; Haasio 2017, s. 75–87 ja Salmivuori 2016, s. 45–85.
[79] Stabek – Watters – Layton 2010, s. 41–51.
[80] Stabek – Watters – Layton 2010, s. 47.

Seuraavissa osioissa esitellään erilaisia verkkopetostyyppejä. Listauksen pohjana toimii edellä esitelty jaottelu, jota on kuitenkin muokattu tutkimuksen tarkoituksiin sopivaksi. Muokatun jaottelun päämääränä on esittää verkkoavusteiset petoslajit eräänlaisessa hierarkkisessa järjestyksessä, jossa alimpana ovat taloudellisilta kokonaisvaikutuksiltaan vähäisimmät petostyypit. Taloudellisten kokonaisvaikutusten täydellinen mittaaminen ei ole kuitenkaan mahdollista rikosten kansainvälisen luonteen, riittävän rikosraportoinnin sekä informaation hajanaisuuden vuoksi. Seuraavaksi esitettävien petostyyppien taloudellisten vaikutusten järjestys pohjautuu siten eri lähteistä kerätyn tiedon perusteella muodostettuun kokonaiskuvan arvioon. Lisäksi jaotteluesityksen yhteydessä yleisimmät eri verkkopetostyypit asetetaan omiin petosluokkiinsa. Mainittujen verkkopetostyyppien esittely ei kuitenkaan ole tyhjentävä, sillä erilaisia verkkopetostyyppejä on lukematon määrä ja uusia kehitetään jatkuvasti. Toisaalta tässä piilee petosten yleispiirteisiin perustuvan luokittelun etu suhteessa toimintatapoihin pohjautuvaan jaotteluun – ennestään tuntemattomatkin petokset voidaan asettaa johonkin näistä kahdeksasta luokasta, kun taas yksittäisten verkkopetoslajien listaaminen johtaisi listojen jatkuvaan päivitystarpeeseen.

3.2.1 Matalatasoiseen huijaukseen perustuvat petokset

Ensimmäinen verkkopetosluokka koostuu petostapauksista, joihin liittyy suhteellisen yksinkertaisia menetelmiä. Tällaisia ovat esimerkiksi huijaukset, joiden suunnittelu ja yksityiskohdat eivät välttämättä ole erityisen perusteellisia. Näiden petostapauksien uhrit suhtautuvat petoksiin ja petolliseen viestintään nimellisarvoisesti eivätkä siten käytä aikaa tai energiaa huijausviestien tai niiden takana olevien ihmisten tutkimiseen. Nämä huijaukset kohdistuvat yksilöön tai yritykseen aluksi kertaluonteisin tapahtumin, ja mikäli huijausta olisi mahdollista laajentaa lisävarojen hankkimiseksi uhrilta, tätä toimintaa voidaan jatkaa. Petosluokan sisältämien tekojen ilmeisin yhteinen tekijä on varojen maksaminen huijarille.

Ensimmäinen petosluokka sisältää huijauksia, jotka toteutetaan kaikkein yksinkertaisimmalla tasolla. Petosten tavoitteena ovat uhrin käteisvarat tai lainojen saanti. Ovelta ovelle -huijauksiin liittyy usein sellaisten palvelujen myymistä, joista maksetaan ja joita ei koskaan suoriteta. Psyykkiset ja selvänäköhuijaukset liittyvät sellaisten palvelujen tai tavaroiden kauppaamiseen, joista maksetaan ja jotka eivät ole sitä, mitä niiden oli luvattu olla. Shekkien avulla tehtäviin liiallisen maksun huijauksiin liittyy ostoksen korvaaminen liian isolla shekillä ja pyyntö liikaa maksetun summan siirtämisestä takaisin lähettäjälle. Tässä

tilanteessa shekki on vilpillinen ja ”palautetut” varat jäävät huijarille. Vaikka tällaiset teot tapahtuvatkin yleensä fyysisesti, kaupat sovitaan useimmiten verkon välityksellä.[81] Taloudellisiin neuvontahuijauksiin liittyy oletettujen taloudellisten neuvojen pyytäminen ennakkomaksua vastaan. Sillä, ovatko neuvot hyödyllisiä vai ei, ei ole merkitystä, sillä uhri on juuri maksanut huijarille, joka on voinut myös mahdollisesti saada uhrin henkilökohtaisia tietoja käytettäväksi tulevissa identiteettivarkauksissa.

3.2.2 Tarinapohjaisiin menetelmiin perustuvat petokset

Toinen petosluokka koostuu petostyypeistä, joihin liittyy yksityiskotaisesti suunnitellut ja mahdollisesti monimutkaiset peitetarinat. Nämä petokset perustuvat suuren yleisön opportunistiseen luonteeseen.[82] Tämän ryhmän petoksia määrittää ennen kaikkea petoksen tekijän ja teon uhrin välille muodostuva sosiaalinen suhde. Näiden petosten perimmäinen tavoite on raha tai toissijaisesti henkilökohtaiset ja sensitiiviset tiedot, mutta menetelmät tämän tavoitteen toteuttamiseksi poikkeavat ensimmäisestä petosluokasta. Petosluokalle ominaisia petostyyppejä ovat esimerkiksi hyväntekeväisyyspetokset, niin kutsutut 419-petokset sekä romanssipetokset.

Hyväntekeväisyyspetos perustuu luonnon katastrofin, inhimillisen tragedian tai muun ihmisten sympatian herättävän tapahtuman verukkeella tehtävään petolliseen varainkeruuseen, joka voi tapahtua esimerkiksi sähköpostilla tai verkkosivuston kautta. Lahjoitetut varat päätyvät tietenkin petoksentekijöille. Edelleen odottamattomiin palkintoihin ja ketjukirjeisiin perustuvat petokset perustuvat samankaltaiseen tarinankerrontaan, mutta eri aihein. Uhrin uskoessa kerrottuun viestiin, kuten palkinnon voittamiseen, voi uhri päätyä haittaohjelmia uhrin päätteelle lataavalle sivustolle. Joskus tällaisilla petoksilla tavoitellaan sähköpostitilien salasanoja tai muita luottamuksellisia tietoja.[83] Tarinapohjaiseen petosluokkaan kuuluvat myös sangen tunnetut 419-petokset, jotka tunnetaan myös nigerialaiskirjeinä. Verkkopetosmuotoa kuvaa kuitenkin paremmin termi ennakkomaksupetos.[84] Tämän petostyypin yhteinen tekijä on lupaus suurista summista varallisuutta uhrin maksamaa etukäteissummaa vastaan. Petokset toteutetaan yleensä sähköpostin avulla ja niiden seli-

[81] Gillespie 2016, s. 137.
[82] Stabek – Watters – Layton 2010, s. 44–45.
[83] Salmivuori 2016, s. 55–56.
[84] Eng. advance fee fraud. Termi nigerlialaishuijaus juontuu siitä, että huijausviestejä on lähetetty suhteellisen paljon Nigeriasta sekä lukuisista muista Afrikan maista. Huijaustyyppiin viitataan myös numerolla 419 tekoihin soveltuvan Nigerian rikoslain pykälän mukaisesti.

tykset vaihtelevat. Selitys voi olla esimerkiksi arpajaisten voitto. Vaikka nämä petokset ovat logiikaltaan yksinkertaisia, niihin lankeaa päivittäin suuri määrä ihmisiä.[85] Yksittäiselle uhrille aiheutuvat vahingot voivat muodostua erittäinkin suuriksi ennen kuin hän ymmärtää tulleensa petetyksi.[86]

Romanssipetos kohdistuu tavanomaisesti internetin seuranhakusovelluksiin ja -verkkosivustoihin. Petoksentekijät keskittyvät näihin sovelluksiin houkutellakseen uhreja lähettämään rahaa ja jakamaan henkilökohtaisia tietoja uusien seurustelukumppaneiden kanssa. Huijarit luovat tyypillisesti väärennettyjä profiileja ollakseen vuorovaikutuksessa käyttäjien kanssa, kehittääkseen suhdetta, rakentaakseen hitaasti luottamusta heidän kanssaan, luodakseen uskottavan tarinan ja pyytääkseen käyttäjältä taloudellista apua.[87]

3.2.3 Työllisuuspohjaiseen menetelmään osallistumista edellyttävät petokset

Kolmas petosluokka koostuu tapauksista, joihin liittyy samanlaista monimutkaista suunnittelua ja yksityiskohtaisuutta kuin tarinapohjaisiin verkkopetoksiin, mutta työllisyyspetokset poikkeavat edellisestä siinä mielessä, että he perustuvat uhrien osallistumiseen. Tämän petosluokan teoille on tunnuksenomaista eräänlainen työsuhde uhrin ja petoksentekijän välillä, jossa uhri osallistuu petolliseen järjestelmään.

Perinteisessä työtarjouspetoksessa uhrille voidaan tarjota työpaikkaa, joka kuitenkin vaatii maksullisen kurssin suorittamisen tai maksullisen työhakemuksen lähettämisen. Työlli-

[85] Stabek – Watters – Layton 2010, s. 45. Kaikkein tunnetuimmissa 419-petoksissa lähtökohtana on varakas nigerialainen perhe tai henkilö, joka haluaa jakaa varallisuutensa vastineeksi avusta perintönsä saamisessa. Petoksentekijä hyödyntää tietojenkalastelutekniikoita lähettääkseen sähköposteja, joissa hahmotellaan emotionaalinen taustatarina, jonka jälkeen uhreja houkutellaan lupauksella merkittävästä taloudellisesta palkkiosta. Petos alkaa tyypillisesti pyytämällä pientä maksua, joka auttaa oikeudellisissa prosesseissa ja paperitöissä. Palkkioksi luvataan suuri summa rahaa myöhemmin. Huijari pyytää väistämättä laajempia maksuja kattamaan muut hallintokulut sekä transaktiokustannukset, joita tukevat laillisen näköiset vahvistusasiakirjat. Luvattu sijoitetun pääoman tuotto ei kuitenkaan koskaan toteudu. Tarkemmin 419-petoksista ks. Gillespie 2016, s. 137–139; Salmivuori 2016, s 45–48 sekä Haasio 2017, s. 78–80.

[86] Esimerkiksi Keski-Suomen käräjäoikeuden tapauksessa R 17/460 asianomistajalle oli aiheutunut yhteensä 46 500 euron vahingot, kun tämä oli lainannut internet-tutulleen yhteensä kymmenellä eri kerralla rahaa, jota tämä oli väittämänsä mukaan tarvinnut toimitusmaksuihin perintöasian hoitajalle Lontooseen. Rahat lainannut vastaaja kertoi itsekin olevansa huijauksen uhri, ja hän oli lähettänyt noin 16 miljoonan euron perinnön toivossa ulkomaille lainarahojen lisäksi omia sekä puolisonsa rahoja. Vastaaja oli lähettänyt rahat Western Union -palvelun välityksellä tuntemattomaksi jääneelle henkilölle. Käräjäoikeus hylkäsi syytteen, mutta määräsi vastaajan korvaamaan asianomistajalle tältä lainaamansa rahat.

[87] Tarkemmin romanssipetoksista ks. Gillespie 2016, s. 139–140; Salmivuori 2016, s. 79–82 sekä Haasio 2017, s. 76–78.

syyspetoksiin voi liittyä myös rahanpesua, johon osallistumisesta petoksen kohteet saavat taloudellisen palkinnon. Nämä huijaukset voivat usein johtaa identiteettivarkauteen ja muihin identiteettirikoksiin, koska osallistuessaan johonkin näistä huijauksista työpaikkaa hakeva uhri on saattanut todella uskoa kyseessä olevan aito työmahdollisuus. Hakemuksellaan uhri voi toimittaa petoksentekijälle täydellisen työ- ja koulutushistoriansa, koko nimensä, syntymäaikansa sekä pankkitilitietonsa palkanmaksua varten. Töiden lisäksi tämän luokan petoksissa voidaan tarjota esimerkiksi lainaa tai pikavippiä edullisin ehdoin.[88]

3.2.4 Näennäispakollisiin velvoitteisiin perustuvat petokset

Velvoitteisiin perustuva petosluokka koostuu petostapauksista, jotka vaativat uhrien takaisinsoittoja tai vastauksia petoksen onnistumiseksi. Tämän luokan petosten tarkoituksena on erehdyttää uhri vastaamaan yhteydenottoon tai ilmoitukseen, minkä seurauksena uhrille esitettään odottamattomia syytteitä. Tällaiset näennäisesti pakottavat velvoitteet ovat luonnollisesti perusteettomia, joten niiden laiminlyömisestä ilmoitetut seuraukset jäävät realisoitumatta. Huijauksen menetelmästä tai uhrin roolista riippumatta tämä petosluokan yhteinen tekijä on tarkoitus hankkia taloudellista hyötyä uhrin kustannuksella tavoilla, jotka vaikuttavat tarpeellisilta tai tilanteen kannalta merkityksellisiltä.[89]

Velvoitepetosten luokkaan voidaan lukea esimerkiksi verkkokampanjat, joihin osallistumiseksi tulee soittaa tai lähettää viesti maksulliseen numeroon. Tähän luokkaan on luettu myös netissä myönnettävien vilpillisten luottojen tai lainojen takaisinmaksu. Lisäksi voidaan mainita yrityksiin kohdistuvat tekaistut laskut esimerkiksi toimistotarvikkeista.

3.2.5 Tiedon keräämiseen perustuvat petokset

Tiedonkeruuseen perustuvia verkkopetoksia on runsaasti erilaisia ja petoskeinot sisältävät enemmän varianssia kuin edellisissä luokissa. Tämä petosluokka koostuu petostapauksista, joihin liittyy petoksentekijöiden kattava ymmärrys tietojärjestelmien toiminnasta ja jotka sisältävät syntaktisesti ohjattuja petoksia, kuten vakoiluohjelmien käyttöä ja näppäinnauhurihuijauksia. Petosluokka sisältää myös petostyyppejä, joilla yritetään hankkia tietoja henkilöllisyyteen liittyvien jatkorikoksien tekemistä varten. Tällaisia rikoksia ovat esimerkiksi

[88] Salmivuori 2016, s. 62–64.
[89] Stabek – Watters – Layton 2010, s. 45.

identiteettivarkaudet ja maksuvälinepetokset. Vakoiluohjelmia ja näppäinnauhuriteknologiaa käyttävät syntaktiset huijaukset kulkevat usein käsikädessä identiteettivarkauksien ja maksuvälinepetoksien kanssa, koska syntaktiset hyökkäykset keräävät uhrin henkilöllisyystodistuksia tai muita tietoja hankkiakseen taloudellista hyötyä – pelkkä tietojen saaminen ei suoraan johda rikoshyötyyn. Näin ollen vakoiluohjelmat ja näppäinnauhuripetokset tunnistetaan työkaluksi tiedonkeruuhuijausten onnistumiseen.[90]

Tässä yhteydessä on hyvä huomauttaa, että suuri osa verkkorikollisuudesta ja erisyisesti tietojenurkintapetoksista keskittyy nykyään identiteettivarkauksiin ja niiden tekemiseen. Nämä teot viittaavat nimenomaan todellisen henkilön henkilökohtaisten tunnistetietojen varkauteen ja käyttöön, toisin kuin kuvitteellisen henkilöllisyyden käyttöön. Tähän voi sisältyä joko elävien tai kuolleiden henkilöiden henkilökohtaisten tietojen varastaminen ja tunnistaminen. On huomattava, että vaikka identiteettivarkaudet usein liittyvät verkkoavusteisiin petoksiin, ne eivät kuitenkaan ole suoraan luettavissa petosrikoksiksi. Petoksen avulla tai muutoin hankittuja henkilötietoja käyttämällä rikoksentekijä syyllistyy RL 38:9a mukaiseen identiteettivarkauteen, joka kuuluu tieto- ja viestintärikoksiin. RL 38 luvun 9a §:n mukaan rangaistavaa on toiminta, jossa erehdytetään kolmatta osapuolta siten, että henkilö käyttää oikeudettomasti toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee. Teosta tuomitaan sakkorangaistus. Tietojenurkintapetosten avulla laittomasti hankittuja henkilötietoja käyttämällä uusien petoksien tekemiseen tekijä syyllistyy siten sekä petostunnusmerkistön mukaiseen tekoon että identiteettivarkaustunnusmerkistön mukaiseen tekoon. Usein näiden tekojen lisäksi rikoskokonaisuudessa voi olla mukana myös väärennettyihin tai varastettuihin tietoihin perustuva maksuväline. Mikäli petoksella hankittuja henkilötietoja käytetään esimerkiksi luottokortin hankkimiseen ja käyttämiseen uusien petosten tekemiseksi, syyllistyy tekijä edellä mainittujen tunnusmerkistöjen lisäksi RL 37 luvussa kriminalisoituun maksuvälinepetokseen (RL 37:8–10) tai muihin tämän luvun mukaisiin tekoihin. Vaikka maksuvälinepetokset tapahtuvatkin usein tietoverkkoympäristössä ja liittyvät monesti verkkopetoskokonaisuuksiin, ovat ne selkeästi oma rikoslajinsa ja sääntelyllinen kokonaisuutensa, johon kohdistuu erilliset oikeudelliset periaatteet ja kriminaalipoliittiset näkökohdat. Sekä identiteettivarkaudet että maksuvälinepetokset ovat siten erotettava verkkoavusteisista petoksista, vaikka ne kuuluvatkin usein samoihin rikoskokonaisuuksiin.

[90] Stabek – Watters – Layton 2010, s. 45.

Petosluokalle ominainen petostyyppi ovat tietojenkalastelusähköpostit, eli niin kutsuttu ”phishing” tai verkkourkinta, on tekniikka, jota käytetään henkilökohtaisten tietojen hankkimiseen esimerkiksi identiteettivarkautta varten. Verkkourkinnassa yritetään huijausviestein ja roskapostin avulla saada käsiin verkkopankkien tai muiden sivustojen käyttäjätunnuksia ja salasanoja, jotta päästäisiin käsiksi asiakkaiden tileillä oleviin varoihin. Kysymyksessä ovat usein ulkomailta toimivat rikolliset. Sen lisäksi, että tietojenkalastelusähköpostit kohdistuvat verkkopankkiasiakkaisiin, ne voivat kohdistua verkkohuutokauppasivustoihin tai muihin verkkomaksujärjestelmiin. Tietojenkalastelusähköpostissa voidaan pyytää esimerkiksi verkkopankkiasiakasta seuraamaan linkkiä henkilökohtaisten pankkitilitietojen päivittämiseksi. Jos linkkiä seurataan, uhrin päätteellä latautuu haittaohjelma, joka tallentaa hänen pankkitunnuksensa ja lähettää ne kolmannelle osapuolelle.[91]

Sähköpostitse tapahtuvan tietojenkalastelun rinnalle on noussut myös niin kutsutut ”pharming” -petokset. Termi "pharming" tulee englanninkielisistä käsitteistä ”phishing” ja ”farming” eli tietojenkalastelusta ja viljelystä. Pharming on eräänlainen käyttäjän manipuloinnin[92] tuotoksena syntyvä kyberhyökkäys, joka manipuloi verkkosivuston liikennettä saadakseen haltuunsa käyttäjän yksityisiä tietoja tai asentaakseen haittaohjelmia heidän päätteilleen. Pharming-petokset voivat toimia myös käänteisesti siten, että käyttäjän päätteelle asennettu haittaohjelma uudelleenohjaa käyttäjän huijausverkkosivulle. Tätä varten petoksentekijät luovat valheellisen verkkosivuston, joka on erehdyttävän samankaltainen kopio kohdesivustosta, ja käyttävät eri menetelmiä ohjatakseen käyttäjät väärennettyyn sivustoon. Tällainen keino voi olla esimerkiksi nostaa vilpillinen verkkosivu hakutulosten yläpäähän hakukoneyhtiön tarjoamien mainostusmahdollisuuksien kautta. Väärennetyt verkkosivujäljennökset tehdään usein pankkien ja verkkokauppasivustojen kaltaisiksi. Pharming- sekä phishing-petokset kohdistuvat usein lukuisiin henkilöihin kerrallaan.[93]

3.2.6 Myynti- ja asiakkuuspohjaiset petokset

Kuudes petosluokka koostuu verkkopetoksista, jotka sisältävät sekä myyjän että ostajan roolit petostapahtuman osapuolina. Petoksen tekijä voi olla joko myyjä tai ostaja. Yleisiä verkkokauppapetoksia ovat esimerkiksi shill-tarjoukset, tarjoussuojaus, tavaroiden toimittamatta jättäminen, maksun toimittamatta jättäminen ja väärien tai ominaisuuksiltaan puut-

[91] Ks. tarkemmin Gillespie 2016, s 141−142.
[92] Eng. social engineering.
[93] HE 52/2021 vp.

teellisten tuotteiden toimitus. Tällaisia petoksia kutsutaan myös yleisnimikkeellä huutokauppapetokset.[94] Tämän petosluokan tekojen tavoitteena on taloudellisen hyödyn hankkiminen, joka saavutetaan samantyylisten petosten eri versioilla ja sovelluksilla.[95]

Suomessa verkkokauppapetosten osuus kaikista poliisin tietoon tulevista verkkopetoksista on suuri.[96] Näin on myös ulkomailla. Esimerkiksi eBay, yksi maailman suurimmista verkkokauppa-alustoista, käyttää huomattavia summia erilaisten petosten kitkemiseksi alustaltaan sekä tekee aktiivista yhteistyötä viranomaisten kanssa petosrikollisuuden torjumiseksi.[97] Tyypillisessä verkkokauppahuijauksessa asiakas houkutellaan maksamaan tuote etukäteen myyjän väärennetyillä henkilötiedoilla avaamalle pankkitilille. Tili voi sinänsä olla myös myyjän oma ja aito. Suomessa erittäin tyypillisiä mainitunlaisia petoksia ovat tuotteiden myyminen verkon välityksellä ilman aikomusta lähettää tuotetta. Esimerkiksi asiassa HelHo 29.01.2016, R 15/631 A syyllistyi useisiin törkeisiin petoksiin myytyään Tori.fi -verkkokauppa-alustalla lukuisissa eri yhteyksissä puhelimia ja muita tuotteita, joita ei kuitenkaan tosiasiallisesti ollut olemassa.[98] Verkkokauppapetoksista tekee erityisen tuottoisia se tosiasia, että tällaisia petoksia ilmoitetaan poliisille liian vähän.[99] Suurin osa ihmisistä tuskin vaivautuu kääntymään verkkokauppa-alustojen asiakaspalvelun puoleen kymmenen euron arvoisten saapumattomatta jääneiden tuotteiden takia saati ilmoittamaan asiasta viranomaisille. Sata kertaa toistettuna petoksilla hankittu rikoshyöty on jo tuhat euroa ja joka viikko toistettuna petoskokonaisuus muuttuu merkittäväksi.

Tilauspetokissa tuote tilataan ilman aikomusta maksaa tuotteesta. Tämä voi tapahtua erehdyttämällä myyjä tai luottoyhtiö myöntämään osamaksun tai muun luoton. Usein tuote voidaan myös tilata kolmannen osapuolen nimissä. Esimerkiksi Helsingin hovioikeuden 31.05.2017 antamassa ratkaisussa R 16/2646 A ja B olivat tilanneet verkkokaupoista puhelimia ja muita elektroniikkatuotteita ilman aikomusta maksaa näistä tuotteista. Petostyypille ominaisesti syytekohtia oli varsin paljon, tässä tapauksessa 98 kappaletta, teot oli tehty

[94] Gillespie 2016, s. 134−137.
[95] Stabek – Watters – Layton 2010, s. 45.
[96] Myös rikosuhritutkimukset tukevat sitä, että tavaroiden ja palveluiden ostoon liittyvät petokset ovat viime vuosina yleistyneet. Ks. Danielsson – Näsi 2019. Lisäksi sisäministeriön Tietoverkkorikollisuuden torjuntaa koskeva selvitys nimeää nettikauppapetokset yleisimmäksi petosrikokseksi maksukorttipetosten kanssa. Ks. Sisäministeriö 2017, s. 12.
[97] Gillespie 2016, s. 134–135.
[98] Ks. myös HelHO 30.05.2016, R 16/807 sekä HelHO 09.02.2018, R 17/336.
[99] Gillespie 2016, s. 136–137.

pitkällä aikavälillä ja vastaajia oli sangen runsaasti.[100] Tietoverkkojen hyväksikäyttö lisää näihin sinänsä jo pitkään olemassa olleisiin huijausmenetelmiin monimutkaisuuden elementin, sillä huijauksien toteutuksessa voidaan hyödyntää esimerkiksi edellä käsiteltyjä identiteettivarkauksia ja maksuvälinepetoksia.

Shill-tarjouspetoksilla tarkoitetaan toimintaa, jossa myyjä tai hänen ystävänsä tekee väärennetyllä profiililla tarjouksen verkkohuutokauppakohteesta nostaakseen keinotekoisesti sen hintaa, haluttavuutta tai näkyvyyttä.[101] Näiden petosten havaitsemisesta ja torjumisesta tekee hankalaa se, etteivät useimmat pidä shill-tarjoustoimintaa petoksena.[102] Snyderin mukaan shill-tarjouspetos voidaan toteuttaa myös käänteisesti, jolloin puhutaan tarjoussuojauspetoksesta. Petoksen toimintalogiikkana on ensin mahdollisimman pienen tajouksen asettaminen tuotteesta, jonka jälkeen väärennetty käyttäjäprofiili asettaa niin suuren tarjouksen tuotteelle, ettei muita asiakkaita tule. Ennen huutokauppamyynnin sulkeutumista suurempi tarjous vedetään pois, minkä seurauksena huijari saa tuotteen erityisen edulliseen hintaan.[103] Gillespie puolestaan on kommentoinut näiden tekojen rikosoikeudellisesta arvioinnista tekevän hankalaa se, että vaikkakin tekomuoto katsotaan petokseksi tuotteen huutokaupattavaksi asettaessaan myyjä antaa ymmärtää olevansa valmis myymään tuotteen lähtöhintaan tai sen puuttuessa suurimman tarjouksen mukaisesti, vaikka tarjous olisikin hyvin pieni. Lisäksi ei voida varmuudella todeta olisiko kukaan tarjonnut suurempaa hintaa, mikäli tarjoussuojauspetosta ei olisikaan toteutettu.[104]

[100] Mielenkiintoinen kysymys tilauspetosten yhteydessä on tilausten noutamatta jättämisen vaikutus teon rikosoikeudelliseen arviointiin. Esimerkiksi Turun hovioikeuden (THO) ratkaisussa THO 2019:15 A ja B olivat tilanneet C:n nimissä eri verkkokaupoista tuotteita suorittamatta niistä maksua, vaikka tuotteet oli jätetty noutamatta ja ne olivat sittemmin palautuneet lähettäjille. Kysymyksenä oli, täyttyikö petoksen tunnusmerkistö siitä huolimatta, että tilatut tuotteet olivat palautuneet niiden lähettäjille ja oliko B:n mahdollista vapautua rikosoikeudellisesta vastuusta tehokkaan katumisen nojalla. B:n menettelyn katsottiin aiheuttaneen asianomistajille petosrikoksen tunnusmerkistössä tarkoitetun välittömän taloudellisen vahingon syntymisen vaaran jo siinä vaiheessa, kun määräysvalta tuotteisiin oli siirtynyt B:lle, vaikka tilatut tuotteet olivatkin sittemmin palautuneet asianomistajille. Koska petosrikoksen tunnusmerkistö oli jo tullut täytetyksi, B ei voinut vapautua rikosoikeudellisesta vastuustaan tehokkaan katumisen perusteella. Tuotteiden noutamatta jättäminen otettiin sen sijaan huomioon rangaistuksen mittaamisessa rangaistusta alentavana tekijänä. Ratkaisusta voidaan päätellä, että taloudellisen vahingon vaara olisi aiheutunut myös, mikäli tuotteet olisivat olleet tarkoitus noutaa, mutta tekijä olisi estynyt, missä tapauksessa rikosoikeudellinen vastuu ei olisi myöskään poistunut.
[101] Snyder 2000, s. 457.
[102] Gillespie 2016, s. 136.
[103] Snyder 2000, s. 457.
[104] Gillespie 2016, s. 136.

3.2.7 Markkinointiperusteiset petokset

Seitsemäs petosluokka koostuu huijaustapauksista, joihin liittyy sijoitusmahdollisuuksien hyväksikäyttöä sekä vilpillisen liikeidean markkinointia laillisena toimintana. Markkinointipetoksiin voidaan lukea kuuluvaksi esimerkiksi niin kutusutut ponzi- ja pyramidihuijaukset, sijoituspetokset ja affiniteettipetokset sekä jotkin ennakkomaksupetosten muodot. Petosluokan huijauksia markkinoidaan rahantekomahdollisuuksina, olipa kyse sitten sijoittamisesta, liiketoimintamahdollisuuksista, osakkeista tai uhkapeleistä. Huijarin tavoitteena on taloudellinen hyöty, mutta joissakin tapauksissa myös tiedonkeruu.

Europolin johto on arvioinut, että sijoituksiin liittyvät verkkopetokset ovat yksi nopeimmin kasvavista rikollisuuteen liittyvistä uhkista Euroopassa.[105] Vuonna 2021 sijoituspetokset olivatkin kaikkein hallitsevin verkkopetostyyppi Euroopassa.[106] Ammattimaisesti toimivat rikollisryhmät myyvät verkossa sekä puhelimitse valesijoituksia esimerkiksi kryptovaluuttaan. Sijoittaja ei luonnollisesti saa rahojaan takaisin. Sijoituspetokset ovat merkittävä haaste lainvalvontaviranomaisille. Kryptovaluuttojen käytön vuoksi petoksentekijät voivat pestä hankkimansa rikollishyödyn nopeasti ja tehokkaasti, kun taas yhteistyöhaluttomat pörssitoimijat tai ne, joilla on heikot asiakkaantunnistusjärjestelmät eli KYC-toimenpiteet,[107] vaikeuttavat petostentekijöiden ja rikoshyödyn tunnistamista. Samaan aikaan väärennetyt sijoitussivustot eivät suoraan kohdista toimintaansa laillisiin rahoituslaitoksiin, vaan väärinkäyttävät näiden tuotemerkkejä kohdistaakseen toimintansa tavallisiin kansalaisiin, mikä on johtanut finanssialan alentuneisiin haluun ryhtyä toimiin sijoituspetostoimintaa vastaan. Koska monet uhrit ovat kärsineet merkittäviä tappioita, joissakin tapauksissa koko eliniän säästönsä, investointipetoksia voidaan pitää hyvin vakavana rikosmuotona.[108]

Sijoituspetosten muotoja on monia ja petostyypin tuottavuuden vuoksi rikolliset kehittävätkin jatkuvasti toimintatapojaan. Rikolliset voivat esimerkiksi iskeä uhreihinsa nykyään jopa kahdesti. Sijoitusten varastamisen jälkeen rikolliset ottavat yhteyttä uhreihin teeskennellen olevansa asianajajia tai lainvalvontaviranomaisia, jotka tarjoavat apua menetettyjen

[105] Helsingin sanomat 2020.
[106] IOCTA 2021, s. 32.
[107] KYC-toimenpiteillä (eng. know your customer measures) tarkoitetaan pankkitoimijoille asetettua velvollisuutta tunnistaa asiakkaansa riittävästi rikollisen rahanpesun estämiseksi.
[108] IOCTA 2021, s. 32.

varojen saamiseksi takaisin. Tuntien tekemiensä huijausten ja varkauksien yksityiskohdat he pystyvät usein jatkamaan uhriensa huijaamista.[109]

Affiniteettipetokset ovat sijoituspetosten muoto, jossa petos kohdistetaan tunnistettaviin ryhmiin, kuten uskonnollisiin tai etnisiin yhteisöihin, kielivähemmistöihin, vanhuksiin tai ammattiryhmien jäseniin. Vilpillistä sijoitusta markkinoiva petoksentekijä esittää yleensä olevansa ryhmän jäsen voittaakseen ryhmän jäsenten luottamuksen. Petos voi koskea esimerkiksi uuden kirkon rahoittamista yhteisesti, mutta rahoitukseen annetut rahat päätyvät petoksentekijöille.

Pyramidihuijaukset eli pyramidipelit ovat suhteellisen vanha petosmuoto, jonka toimintamallina on eräänlainen verkostomarkkinointi. Vilpillistä toiminnasta tekee se, että verkostossa markkinoidut tuotteet tai palvelut eivät rahoita toimintaa, vaan uusien mukaan liittyvien jäsenten lunastamat aloituspaketit. Ponzi-huijaus eli ponzi-järjestelmä on puolestaan pyramidihuijauksen muoto, jossa joku kerää pääomia kuviteltua tai olemassa olevaa sijoituskohdetta varten. Sijoitukselle luvataan korkea ja nopea tuotto, mikä kuitenkin perustuu uusien sijoittajien maksamiin varoihin eikä väitetyn sijoituskohteen tuottoihin. Siten ponzihuijaukset romahtavat aina viimeistään silloin, kun riittävästi uusia sijoittajia ei saada mukaan järjestelmään maksamaan edellisten osallistujien sijoitustuottoja.

Lain esitöiden mukaan pyramidipeli rinnastuu luonteeltaan ketjukirjeeseen.[110] Pyramidipelin käsite otettiin ensi kertaa lakiin rahankeräyslainsäädännön kokonaisuudistuksessa, jonka tuloksena säädettiin 1.7.2006 voimaan tullut, asiassa sovellettava rahankeräyslaki (255/2006). Rahankeräyslain 4 §:n 4 kohdassa on sanamuodoltaan olennaisesti aikaisempaa sääntelyä vastaava ketjukirjetoimintaa koskeva määritelmä ja 5 kohdassa pyramidipeliä koskeva määritelmä. Hallituksen esityksessä pyramidipelit-otsikon alla on todettu, että erityisesti internetin välityksellä tapahtuvat toiminnot sisältävät sekä kaupankäynnin että arpajais- ja rahankeräystoiminnan muotoja, jotka perustuvat pyramidijärjestelmän mukaiseen asiakashankintaan. Mukaan liittyvien tulo-odotukset riippuvat heidän organisaatioidensa kautta tulevien asiakkuuksien ja tehtyjen tilausten määrästä. Ominaista näille toiminnoille on toiminnan alkuvaiheessa erittäin nopeasti kasvava asiakasmäärä. Päätelmänä lausuttiin, että tällaista rahankeräyksen toimeenpanoa voitiin pitää ketjukirjeisiin verrattavalla tavalla toimeenpantuna ja siten kiellettynä ja rangaistavana. Puhtaat pyramidipelit, joihin ei sisältynyt lainkaan muuta tuotteiden, tavaroiden tai palvelujen vaihtoa kuin mah-

[109] IOCTA 2021, s. 32.
[110] HE 102/2005 vp, s. 35.

dollisuus värvätä uusia osanottajia mukaan toimintaan, ovat yleistyneet.[111] Tietoverkkoympäristö on tarjonnut tälle petostyypille runsaasti uusia mahdollisuuksia esimerkiksi markkinoinnin ja ihmisten tavoittamisen helppouden suhteen.

Tunnetussa WinCapita-tapauksessa eli korkeimman oikeuden ratkaisussa KKO 2014:7 oli kyse pyramidihuijauksesta.[112] Pyramidipelin aloittaja tuomittiin törkeästä petoksesta, mutta tapauksessa arvioinnin kohteena eivät olleet tietoverkkoelementit. WinCapita-klubin markkinointi ja tietojenlevitys toimi kuitenkin klubin internet-sivujen kautta. Petoksen laajuuden ja sen uhreille realisoituneiden taloudellisten menetysten suuruus osoittavat kuitenkin verkkoympäristön tarjoaman näkyvyyden merkityksen tällaisten petosten toiminnassa.

3.2.8 Yritystoimintaan erikoistuvat petokset

Edellä mainitut petostyypit kohdistuvat suurimmalta osalta yksityishenkilöihin. Yritystoimintaan kohdistuvilla petoksilla voidaan kuitenkin saavuttaa huomattavasti suurempia taloudellisia hyötyjä kuin yksityishenkilöihin kohdistuvilla petoksilla. Isoilla organisaatioilla voi olla erilliset petostentorjuntaprotokollansa, minkä vuoksi yrityksiin kohdistuvat petokset ovat usein verrattain monimutkaisia sekä toteutustavoiltaan monimuotoisempia. Organisaatioihin voi kohdistua esimerkiksi tietomurtoja tai palvelunestohyökkäyksiä verkkopetosten osana. Myös tietojenkalastelua kohdistuu hyvin laajamittaisesti organisaatioihin. Erityisesti pankit ja muut rahoituslaitokset ovat verkkorikollisten suosiossa.

Finanssialan toimijoiden lisäksi myös sähköistä liiketoimintaa harjoittavat organisaatiot ovat verkkoavusteisten petosten kohteina. Esimerkiksi teleoperaattori-, teknologia- ja mainosyritykset voivat joutua petoksen kohteeksi. Niin kutsuttu klikkauspetos on tästä yksinkertainen esimerkki. Näissä petoksissa käytetään hyväksi yritysten sähköisiä markkinointikanavia kuten puhelinsovelluskauppojen kampanjoita, jotka käyttävät napsautuskohtaisesti

[111] HE 102/2005 vp, s. 16–17.

[112] Tapauksessa KKO 2014:7 A oli antanut perustamansa klubin toiminnasta tietoja, joiden mukaan klubi harjoittaisi tuottoisaa vedonlyöntitoimintaa ja valuuttakauppaa, ja maksaisi klubin jäsenille näin saatuja tuottoja. Tuhannet ihmiset olivat sijoittaneet rahoja A:n hallinnoimille tileille. Tosiasiassa väitetty toiminta oli ollut tappiollista eikä valuuttakauppaa ollut käyty. Varoja oli A:n kehittämien laskenta- ja tuotonjakosääntöjen perusteella maksettu pääasiassa klubiin hyvin aikaisessa vaiheessa liittyneille jäsenille. Voitto-osuuksina maksetut määrät olivat siten olleet klubiin myöhemmin liittyneiden jäsenten suorittamista maksuista saatua laskennallista tuotto-osuutta. Klubiin toiminnan loppuvaiheessa liittyneet jäsenet olivat yleensä menettäneet kaikki sijoittamansa varat ja jääneet ilman luvattuja tuottoja. Lukuisille henkilöille oli näin aiheutettu taloudellista vahinkoa tai sen vaaraa ainakin 57 miljoonan euron arvosta. A oli tuomittu törkeästä petoksesta. Korkeimman oikeuden oli ratkaistava, oliko A voitu tuomita myös rahankeräysrikoksesta. Äänestysratkaisun lopputuloksena A katsottiin syylliseksi myös rahankeräysrikokseen.

maksettavaa verkkomainontatekniikkaa. Tämäntyyppisessä mainonnassa mainoksia lähettävien verkkosivustojen omistajat saavat maksun sen mukaan, kuinka moni sivuston kävijä napsauttaa mainoksia. Napsautuksesta saatava maksu voi koskea myös esimerkiksi sovellusten lataamista puhelimelle. Huijarit käyttävät bottien generoimia väärennettyjä napsautuksia tuottaakseen keinotekoisen kävijämäärän kohdesivustolle tai -palveluun. Joskus napsautuksien tekemiseen käytetään oikeita ihmisiä, joille maksetaan mainosten klikkaamisesta useilta laitteilta samanaikaisesti. Petoksen seurauksena yritykset voivat maksaa verkkosivun ylläpitäjälle tai muulle taholle suuria summia rahaa mainostensa saaman näkyvyyden vuoksi, vaikka todellisuudessa maksettu mainonta ei ole hankkinut yritykselle yhtään uusia asiakkaita. Napsautuspetokset osoittavat verkkoteknologian, kuten bottien käytön, merkityksen yritysten kohtaaman modernin rikollisuuden suhteen.

Tälle petosluokalle eräs keskeinen petoslaji on yrityssähköpostin murto eli BEC-petos.[113] BEC-petos on varsin kehittynyt pankkimaksuja suorittaviin yrityksiin kohdistuva hyökkäysmuoto. Hyökkäyksen tarkoituksena on murtautua yrityksen tai organisaation työntekijöiden todellisiin sähköpostitileihin käyttäjän manipulointitekniikoiden avulla, jotta yrityksen tekemiä rahatransaktioita voidaan petollisesti ohjata tai lähettää rikostentekijöiden tileille tai muihin heidän määritelmiinsä osoitteisiin. Yhdessä toimitusjohtajapetosten kanssa BEC-petokset ovat määrällisesti mitattuna nimenomaisesti yrityksiin kohdistuvien verkkopetoslajien kärkisijalla.[114]

Yrityksiin kohdistuvan verkkopetosrikollisuuden toinen tyyppitapaus on niin sanottu toimitusjohtajapetos.[115] Nämä petokset ovat yleistyneet Suomessa 2010-luvulta alkaen. Toimitusjohtajapetoksella tarkoitetaan huolellisesti toteutettua erehdyttämispetosta, joka vaatii pitkällistä valmistelua sekä riittävää tietojen keräämistä kohdeyrityksen henkilöstöstä ja itse yrityksestä. Petostyypissä yrityksen työntekijä erehdytetään suorittamaan maksu petoksentekijän hallinnassa olevalle tilille toimittamalle hänelle esimerkiksi väärennetty sähköpostiviesti tämän esimiehenä taikka yrityksen toimitusjohtajana esiintyen. Petokseen voi tietenkin liittyä myös toisenlaisia yhteydenottomuotoja kuten tekstiviestejä. Lisäksi petostyypissä voi esiintyä taitavia psykologisia painostuskeinoja kohdeyrityksen henkilöstöä

[113] Eng. Businnes email compromise.
[114] Interpol IOCTA 2021, s. 32.
[115] Eng. CEO fraud.

kohtaan. Onnistuessaan toimitusjohtajapetos johtaa usein euromääräisesti suuriin menetyksiin kohdeyrityksen kannalta.[116]

Toimitusjohtajapetoksia muistuttava verkkopetostyyppi niin kutsuttu spear phishing -petos. Spear phishing -termi tarkoittaa kohdennettua tietojen kalastelua sähköpostiviestin, tekstiviestein, puheluin tai väärennettyjen verkkosivujen avulla. Kohdennetun tietojen kalastelun tavanomaisen tietojen kalastelun periaate on sama. Tarkoituksena on houkutella henkilö käyttäytymään tavalla, joka palvelee rikollisen päämääriä. Kyseessä on käyttäjän manipulointikeino, jonka tuloksena viestin vastaanottaja saadaan kokemaan luottamusta vastapuolen sanomaa kohtaan. Kohdennetussa tietojenkalastelussa huijausviesti räätälöidään tarkasti tietylle kohdeyritykselle. Tavoitteena on useimmiten liikesalaisuuksiin liittyvien tietojen hankinta. Vilpillinen sähköpostiviesti voi sisältää linkin tai liitetiedoston, jonka klikkaaminen johtaa monien erilaisten tietojenurkintaan tarkoitettujen haittaohjelmien latautumiseen tietokoneelle. Tavanomainen tietojen kalastelu on vielä toistaiseksi Suomessa yleisempää kuin kohdennettu tietojenkalastelu. Toisaalta tarkasti tiettyyn yritykseen kohdennettua sähköpostihuijausta on huomattavasti haastavampi havaita kuin tavallista tietojen kalastelua, joten havainnot eivät ole täysin tarkkoja. Petoksentekijä hankkii huijauksessa tarvittavat tiedot, kuten henkilötiedot, tietokannan tietojen nimet, sähköpostiosoitteet ja muut tunnistetiedot, ostamalla ne tietoverkkorikollisuutta tukevilta markkinoilta tai itse tietojenkalastelupetosten avulla. Lopputuloksena käyttäjän sähköpostilaatikkoon tuleva sähköpostiviesti näyttää saapuneen tutun yrityksen omasta autenttisesta osoitteesta, henkilökuntaan kuuluvalta käyttäjältä tai muusta luotettavasta lähteestä. Huijausviestiä on tällöin käytännössä mahdotonta erottaa normaalista sähköpostiviestistä.

Myös tietomurrot luetaan joissain yhteyksissä verkkoavusteisien petosten joukkoon. Näin on erityisesti yrityksiin kohdistuvien tietomurtojen osalta.[117] Vuonna 2013 alkaneet niin sanotut Carbanak-hyökkäykset kuvaavat hyvin yrityksiin kohdistuvan talousrikollisuuden sekä petosten nykyistä kyberprofiilia. Teot olivat haittaohjelmiin ja tietojenkalastelupetoksiin perustuvia pankkivarkauksia, joilla hankittu rikollinen hyöty nousi yli miljardiin Yhdysvaltain dollariin. Espanjasta käsin toiminut Carbanak-niminen järjestäytynyt rikollisryhmä pääsi ympäri maailmaa sijaitsevien pankkien tietojärjestelmiin pankkivirkailijoihin kohdistetun tietojenkalastelun ja sähköpostin kautta pankin päätteille ladattavien haittaoh-

[116] Riekkinen 2018, s. 78–79. Ks. myös Europol Internet Organised Crime Threat Assessment (IOCTA) 2015, s. 38; Europol IOCTA 2016, s. 32–33 sekä Europol IOCTA 2017, s. 57–58. Toimitusjohtajapetoksista Suomessa ks. esim. Yle Uutiset 2017 ja Yle Uutiset 2016.
[117] Esimerkiksi Suomessa yritykset joutuvat hyvin usein tietomurtojen kohteiksi. Ks. Yle Uutiset 2018a.

jelmien avulla, minkä jälkeen rikolliset siirsivät petollisesti paisutettuja saldoja omille tileilleen sekä uudelleen ohjelmoiduille pankkiautomaateille, joista ulkopuoliset kuriirit nostivat käteisen ja veivät rahat mukanaan.[118]

Huomionarvoista on, että tämä rikoskokonaisuus oli koordinoidusti ja samanaikaisesti toteutettu verkkoavusteinen hyökkäys lukuisia pankkeja vastaan. Hyökkääjät osoittivat edistyksellistä tietotaitoa tietoverkkoympäristöstä, kattavaa ymmärrystä pankkiprosesseista ja yksityiskohtaista tietoa kohteina olleiden finanssilaitosten valvonnasta sekä haavoittuvuuksista, jotka johtuivat siiloutuneista organisaatioista ja huonosti järjestetystä hallinnosta. Rikolliset käyttivät hyväkseen myös monia sähköisiä maksuvälineitä kuten luotto- ja pankkikortteja, pankkisiirtoja sekä pankkiautomaatteja. Hyökkäysten toteutuksesta ja onnistumisesta nähdään, että selkeät erot tietoverkkohyökkäysten, petosten ja talousrikollisuuden välillä ovat häviämässä. Pankit eivät ole vielä käsitelleet näitä uusia leikkauspisteitä, jotka rikkovat rikostyyppien välillä aiemmin vallinneita rajaviivoja.[119]

Carbanak-hyökkäyksissä tiivistyy organisaatioiden kohtaaman taloudellisen verkkoavusteisen petosrikollisuuden yleisimmät piirteet. Organisaatioihin erityisesti kohdistuva petosrikos on monimutkainen, suunnitelmallinen ja harkittu kokonaisuus, johon liittyy kohdennettua tietojenkalastelua, varastettuja identiteettejä käyttäviä vilpillisiä sähköposteja, käyttäjän manipulointia, haittaohjelmien hyödyntämistä, tietomurtoja, maksuvälinepetoksia, kansainvälinen toimintaympäristö ja suurimmassa osassa tapauksista järjestäytyneen rikollisuuden läsnäolo. Tietojenkeruu ja muu petoksen valmistelu voi viedä hyvinkin pitkän ajan, minkä seurauksena rikoskokonaisuudet ovat vaikeasti hahmotettavissa. Rikoskokonaisuuteen liittyy monia rikostunnusmerkistöjä petoksen lisäksi, mutta samalla rikokset ikään kuin sulautuvat yhteen verkkoympäristön vaikutuksesta. Tämä paitsi osoittaa muista verkkopetosluokista täysin poikkeavia ominaisuuksia, myös todistaa verkkopetosten muodostaman varsin uniikin ja haastavan rikosoikeudellisen ja -torjunnallisen ongelman olemassaolon.

[118] Yle Uutiset 2018b ja Hasham – Joshi – Mikkelsen 2019.
[119] Hasham – Joshi – Mikkelsen 2019.

4 Verkkoavusteisten petosten sääntely

4.1 Sääntelyn yleiset piirteet

Vaikka Suomen rikoslaissa petoksia koskevat pykälät ovat pääosin yleisluontoisia, on verkon vaikutuksia petosrikollisuuteen arvioitu silti säädöksiä valmisteltaessa. Esimerkiksi hallintovaliokunnan lausunnossa on todettu, että tietoverkkoja hyödynnetään rikollisiin tarkoituksiin muun muassa verkkoavusteisia petoksia tehtäessä.[120] Lisäksi Euroopan Unionin tasolla on huomioitu, että tietoverkkoja voidaan käyttää myös rikollisiin tekoihin laillisten tarkoitusperien ohella. Tietoverkkoja voidaan hyödyntää rikosten tekemisessä, mutta toisaalta rikokset voivat myös kohdistua itse tietoverkkoihin. Euroopan unioni on nykyään keskeinen rikosoikeudellinen toimija sekä itsenäisesti että rikoslainsäädännön harmonisoinnin kautta tiettyjen rikollisten toimintamallien suhteen. Näitä ovat esimerkiksi tietoverkkorikollisuus, maksuvälineiden väärentäminen ja järjestäytynyt rikollisuus.[121] Itsenäisenä toimijana Euroopan unioni on edistänyt jäsenvaltioiden poliisiyhteistyötä ja perustanut lukuisia rikoksentorjuntaan ja rikollisuuden tutkimiseen tähtääviä toimielimiä.

Verkkopetosten sääntelyä leimaa teknologianeutraalius. Toisaalta samalla säännökset ovat jätetty hyvin väljiksi ja kansallisesta lainsäädännöllisetä tarkentamisesta riippuvaiseksi. Puhtaasti verkkoavusteisia petoksia koskevaa oikeuskäytäntöä ei myöskään vielä ole. Tilanne on sama sekä EU:n että Suomen tasolla. Verkkopetosten rajat ylittävästä luonteesta johtuviin lainsäädännöllisiin ongelmiin on vastattu ennenkaikkea tukemalla viranomaisyhteistyötä ja perustamalla kansainvälisiä petosten torjuntaan tähtääviä toimielimiä. Näin ollen verkkoavusteisia petoksia ympäröivä sääntelyllinen kehikko ei ole puhtaan normatiivinen ainakaan kansainvälisestä näkökulmasta.

4.2 Sääntelyn EU-oikeudellinen viitekehys

Petokset ovat tunnustettu erityiseksi taloudelliseksi uhaksi Euroopan unionin alueella esimerkiksi Euroopan petostentorjuntaviraston (OLAF) vuonna 2016 julkaisemassa kansallisia petostentorjuntastrategioita koskevassa työryhmämietinnössä.[122] Myös tietoverkkori-

[120] Valiokunnan lausunto HaVL 23/2021 vp. Valiokunta kiinnittää huomiota myös siihen, että tietoverkkorikollisuuden kasvu ja kehittyminen edellyttävät poliisilta entistä enemmän kyvykkyyttä ja panostusta poliisin oman tietoturvallisuuden ylläpitoon ja kehittämiseen.
[121] Kimpimäki 2015, s. 27 ja 439.
[122] Euroopan petostentorjuntavirasto (OLAF) 2020, s. 25.

kollisuus tunnistetaan vakavaksi uhaksi.[123] Näin ollen EU:n tasolla onkin annettu lukuisia direktiivejä ja asetuksia petosten ja kyberrikollisuuden ehkäisemisestä, joissa on myös käsitelty verkkoavusteisia petoksia tai joita voidaan soveltaa verkkopetosten torjumiseen.

Lähtökohtana on Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 310 ja 325 artiklat, joiden mukaan unioni ja jäsenvaltiot suojaavat unionin taloudellisia etuja petolliselta menettelyltä ja muulta laittomalta toiminnalta. Jäsenvaltiot toteuttavat samat toimenpiteet suojatakseen unionin taloudellisia etuja petolliselta menettelyltä kuin ne toteuttavat suojatakseen omia taloudellisia etujaan petolliselta menettelyltä. Jäsenvaltiot sovittavat yhteen toimintansa, jonka tarkoituksena on suojata unionin taloudellisia etuja petolliselta menettelyltä, sanotun kuitenkaan rajoittamatta sopimuksen muiden määräysten soveltamista. Tätä varten ne yhdessä komission kanssa järjestävät hallintonsa toimivaltaisten yksiköiden kiinteän ja säännöllisen yhteistoiminnan.[124] EU:n jäsenvaltioiden yhteistoiminta on siten keskeisessä asemassa petostentorjunnan suhteen.

EU:n direktiivissä unionin taloudellisiin etuihin kohdistuvien petosten torjunnasta rikosoikeudellisin keinoin[125] on tunnistettu tietoverkkojen rajat ylittävä luonne ja otettu askelia ongelman torjumiseen. Petosdirektiivissä todetaan, että otettaessa huomioon erityisesti rikoksentekijöiden ja unionin taloudellisten etujen kustannuksella tapahtuvasta laittomasta toiminnasta saadun hyödyn liikkuvuus sekä tästä liikkuvuudesta johtuvat monimutkaiset rajat ylittävät tutkinnat, kunkin jäsenvaltion olisi määritettävä lainkäyttövaltansa tavalla, joka mahdollistaa tällaisen toiminnan torjumisen. Kunkin jäsenvaltion olisi tällä tavoin varmistettava, että sen lainkäyttövallan piiriin kuuluvat myös rikokset, jotka on tehty tieto- ja viestintätekniikan avulla sen alueelta.[126]

Rajat ylittävissä rikostutkinnoissa ja tuomioistuinkäsittelyissä lainkäyttövalta nousee myös merkittäväksi tekijäksi. EU:n petosdirektiivi ei vaikuta kurinpidollisten seuraamusten tai muiden kuin rikosoikeudellisten toimenpiteiden tai seuraamusten asianmukaiseen ja tehokkaaseen soveltamiseen. Seuraamukset, joita ei voida rinnastaa rikosoikeudellisiin seuraamuksiin ja jotka on määrätty samalle henkilölle samasta toiminnasta, voidaan ottaa huomi-

[123] Neuvoston päätös jäsenvaltioiden valtuuttamisesta ratifioimaan Euroopan unionin edun mukaisesti tietoverkkorikollisuutta koskevan yleissopimuksen toinen lisäpöytäkirja, joka koskee yhteistyön tiivistämistä ja sähköisten todisteiden luovuttamista 2021/0383 (NLE), s. 1.
[124] Euroopan petostentorjuntavirasto (OLAF) 2020, s. 9.
[125] Euroopan parlamentin ja neuvoston direktiivi (EU) 2017/1371, annettu 5 päivänä heinäkuuta 2017, unionin taloudellisiin etuihin kohdistuvien petosten torjunnasta rikosoikeudellisin keinoin. Jäljempänä EU:n petosdirektiivi.
[126] EU:n petosdirektiivi (EU) 2017/1371.

oon, kun henkilö tuomitaan tässä direktiivissä määritellystä rikoksesta. Petosdirektiivi ei näin ollen vaikuta muihin petosrikoksiin liittyviin vaateisiin kuten vahingonkorvauskanteisiin, jotka jäävät rikosoikeudellisen katsannon ulkopuolelle. Muiden seuraamusten osalta olisi noudatettava täysimääräisesti periaatetta, joka koskee kieltoa syyttää ja rangaista rikosoikeudellisessa menettelyssä kahdesti samasta rikoksesta.[127] Näissä rajat ylittävissä rikoksissa tulee siten ottaa huomioon *ne bis in idem* -kielto. Luonnollisesti myös muut kansainvälistä rikosprosessia ja lainvalintaa koskevat säädökset tulevat noudatettaviksi.[128]

EU:n maksuvälinepetosdirektiivissä säädetään tietokoneavusteisista petoksista, mutta vain maksuvälineiden osalta.[129] Laajemmissa tietomurtoa muistuttavissa petostapauksissa voidaan hakea johtoa direktiivistä 2013/40/EU, mutta tämäkään ei suoraan sääntele verkkopetoksia.[130] Sen sijaan vuonna 2001 tehty tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus[131] on ensimmäinen kansainvälinen kyberrikollisuutta koskeva sopimus, joka ottaa kantaa verkkopetoksiin, vaikkakin varsin väljällä tavalla. Budapestin yleissopimuksen 8 artikla velvoittaa sopimuksen jäsenmaat kriminalisoimaan tietokoneavusteiset petokset, jotka toteutetaan dataa muuttamalla, poistamalla tai lisäämällä.[132] Artiklan väljyys voidaan nähdä toisaalta etuna sen huomioidessa myös uudenlaiset verkkopetokset, mutta toisaalta väljä muotoilu ei tarjoa johtoa kriminalisoinnin sopivaan toteutukseen. Artikla ei ota myöskään kantaa verkkopetoksiin, jotka tapahtuvat ilman dataelementtiä.[133]

[127] EU:n petosdirektiivi (EU) 2017/1371.
[128] Yleisesti kansallisten tuomioistuinten toimivallasta rikosasioissa ks. Kimpimäki 2015, s. 535–593. EU:n maksuvälinepetosdirektiivin (EU) 2019/713 12 artiklassa säädetään myös tarkemmin lainkäyttövallasta verkkopetosten osalta. Artiklan mukaan rikos katsotaan tehdyksi kokonaan tai osittain jäsenvaltion alueella, kun rikoksentekijä tekee rikoksen ollessaan fyysisesti kyseisellä alueella riippumatta siitä, onko rikos tehty kyseisellä alueella sijaitsevaa tietojärjestelmää käyttäen.
[129] Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/713, annettu 17 päivänä huhtikuuta 2019, muihin maksuvälineisiin kuin käteisrahaan liittyvien petosten ja väärennysten torjunnasta ja neuvoston puitepäätöksen 2001/413/YOS korvaamisesta.
[130] Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta.
[131] Jäljempänä Budapestin yleissopimus.
[132] Budapestin yleissopimus, 8 artikla: ”Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi tahallisen ja oikeudettoman taloudellisen vahingon aiheuttamisen toiselle, kun teko on tehty:
a) dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla;
b) tietojärjestelmän toimintaa häiritsemällä,
tarkoituksin saada itselle tai toiselle taloudellista hyötyä petoksella tai muulla epärehellisellä keinolla”.
[133] Tällaisia petoksia ovat esimerkiksi myyntipetokset, jossa tuotetta ei toimiteta. Ks. Gillespie 2016, s. 143–144.

Artikla 7 on hieman tarkempi, mutta jää silti erittäin löyhäksi.[134] Artiklasta voidaan kuitenkin hakea johtoa esimerkiksi tietojenkalastelun yhteydessä.[135]

Vaikka useissa yhteyksissä EU-tasolla on todettu verkkopetosten olevan erittäin vakava rikollinen ilmiö, ei EU-oikeus kuitenkaan tarjoa tämän ilmiön torjumiseen kovin edistyksellisiä työkaluja. EU-oikeus vain lähinnä velvoittaa jäsenmaat kriminalisoimaan verkkoavusteiset petokset riittäväksi katsomillaan tavoilla. Kriminalisointia selkeyttävää oikeuskäytäntöä ei myöskään ole saatavilla. Verkkoavusteisiin petoksiin liittyy kuitenkin kiinteästi datan käyttö, joka on tällaisten petosten rikostutkinnassa tärkeässä roolissa. Informaationkäsittely johtaa tietosuojaoikeudellisiin kysymyksiin, varsinkin kun petokseen liittyy henkilötietoja. EU-oikeus on tietosuojakysymysten osalta huomattavasti tarkempaa kuin verkkopetossääntely.

4.3 Tietosuojaoikeudellinen ulottuvuus

4.3.1 Sähköisen todistusaineiston rajat ylittävä saatavuus

Suomessa Riekkinen on tehnyt tutkimusta sähköisestä todistelusta.[136] Verkkoavusteiset petokset toteutetaan nimensä mukaisesti tietoverkkojen välityksellä ja tietoteknisiä laitteita hyödyntäen. Tästä syystä valtaosa laittomasta toiminnasta jäävistä jäljistä on digitaalisessa muodossa. Tällainen sähköisessä muodossa oleva todistusaineisto muodostuu näin ollen päätteillä sekä muilla tietoteknisillä laitteilla sijaitsevasta ja ohjelmistojen avulla käsiteltävissä olevasta datasta. Riekkinen on todennut, että tällaisia todisteita voidaan nimittää sähköisdigitaalisiksi tai yksinkertaisemmin sähköisiksi todisteiksi.[137] Yleisesti ottaen sähköiset

[134] Budapestin yleissopimus, 7 artikla: ”Kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin säätääkseen lainsäädäntönsä mukaisesti rangaistavaksi sellaisen tahallisen ja oikeudettoman datan syöttämisen, muuttamisen, tuhoamisen tai poistamisen, jonka tuloksena syntyvä väärä data on tarkoitettu käytettäväksi oikeudellisissa tarkoituksissa harhauttavana todisteena, riippumatta siitä onko data sellaisenaan luettavissa tai ymmärrettävissä. Sopimuspuoli voi asettaa rikosvastuun syntymisen edellytykseksi sen, että teko on toteutettu petostarkoituksin tai muuta epärehellistä tarkoitusta varten”.

[135] Gillespie 2016, s. 145.

[136] Ks. Riekkinen 2019. Sähköisestä todistelusta verkkopetoksien kontekstissa ks. Riekkinen 2018, s. 75–102.

[137] Riekkinen 2018, s. 83. Sähköisillä todisteilla viitataan toisinaan myös analogisilla, ei-digitaalisilla laitteilla tallennettuun materiaaliin, jolloin sähköiset todisteet ovat yläkäsite, joka kattaa sekä analogiset että digitaaliset todisteet. Sähköisen todisteen käsitteestä tarkemmin ks. Schafer –Mason 2012, s. 23–30. Pohjoismaisessa keskustelussa sähköis-digitaalisista todisteista on käytetty myös nimityksiä tietotekniset todisteet ja datatodisteet. Terminologiaa on analysoinut Jonas Ekfeldt. Ks. Ekfeldt 2016, s. 364–395 ja 434–435. Ks. myös Sunde 2015, s. 599–633.

todisteet ovat niiden muodosta johtuen helposti ja nopeasti hävitettävissä, piilotettavissa ja muokattavissa, mikä luonnollisesti aiheuttaa haasteita rikostutkinnalle.[138]

Sähköiset todisteet ovat yhä tärkeämpiä rikostutkinnassa. Euroopan komissio on arvioinut, että 85 prosentissa rikostutkinnoista, mukaan lukien tietoverkkorikollisuuden tutkinnassa, lainvalvonta- ja oikeusviranomaiset tarvitsevat nykyään sähköistä todistusaineistoa.[139] Ulkomaisilla lainkäyttöalueilla toimivien palveluntarjoajien hallussa on nykyään enenevissä määrin sähköisessä muodossa olevia todisteita rikoksista, ja tehokkaat rikosoikeudelliset toimet edellyttävät asianmukaisia toimenpiteitä tällaisten todisteiden hankkimiseksi ja oikeusvaltioperiaatteen noudattamiseksi. Rikostutkintaa varten tarvittavien sähköisten todisteiden rajat ylittävää saatavuutta pyritään parantamaan kaikkialla maailmassa, kansallisella tasolla, Euroopan unionissa[140] ja kansainvälisellä tasolla. Yhteensopivien sääntöjen varmistaminen on tärkeää kansainvälisellä tasolla lainvalinnasta johtuvien ongelmien ehkäisemiseksi, kun viranomaiset pyytävät saada sähköistä todistusaineistoa rajojen yli.

Lainvalvontaviranomaisten on usein vaikea saada käyttöönsä toisessa maassa olevaa todistusaineistoa. EU:n tasolla vireillä olevan lainsäädäntötyön tuloksena voidaan auttaa lainvalvonta- ja oikeusviranomaisia saamaan käyttöönsä toisessa jäsenvaltiossa sijaitsevaa välttämätöntä, mutta mahdollisesti salattua todistusaineistoa. Rikosten tuloksellinen tutkinta ja syytteeseenpano edellyttävät asianmukaista oikeudellista kehystä. Esimerkiksi Suomessa poliisin tietoon tulleista petosrikoksista vuonna 2016 oli yli 40 prosentissa epäilty on ulkomaalainen henkilö.[141] Luonnollisesti myös suomalaisten tekemillä petosrikoksilla voi olla kansainvälisiä liityntöjä. Tällaisissa tapauksissa rikostukinnan edellyttämien todisteiden hankinta vaatii useissa tapauksissa kansainvälisen oikeusapupyynnön toimittamista, ellei ulkomaalainen palveluntarjoaja ole yhteistyöhalukas ja luovuta tietoja vapaaehtoisesti. Petosrikosten valtavan suuren määrän vuoksi kansainvälistä oikeusapua ei kaikissa maissa merkitykseltään vähäisissä tapauksissa anneta lainkaan. Muutoinkin oikeusapupyyntöihin vastaaminen vie hyvin pitkiä aikoja, joskus jopa vuosia. Koska sähköiset jäljet ovat helposti hävitettävissä ja eräät tiedot, kuten internet-liikenteen ja puhelinviestinnän välitystiedot,

[138] Riekkinen 2018, s. 83.
[139] SWD(2018) 118 final.
[140] COM(2018) 225 final ja COM(2018) 226 final.
[141] Sisäministeriö 2017, s. 23.

hävitetään ajan kuluessa usein automaattisesti, tutkinnan viivästyminen voi tarkoittaa tutkinnan estymistä.[142]

Oman ongelmansa muodostaa myös Euroopan yleinen tietosuoja-asetus.[143] Sähköiset todisteet sisältävät usein tietoja, joiden avulla voidaan tunnistaa luonnollisia henkilöitä. Tällaiset tiedot katsotaan yleisen tietosuoja-asetuksen sääntelemiksi henkilötiedoiksi, joiden suojaamiseen asetus tähtää. Esimerkiksi valvontakamerakuva tai IP-osoite ovat tietosuoja-asetuksen tarkoittamia henkilötietoja. Asetuksen mukainen henkilötietojen suoja määrittää tietyt reunaehdot rajoittaen todisteiden varmistamiseen tähtäävää toimintaa. Tietosuojalainsäädännössä on toisaalta asetettu nimenomaisia suojaamis- ja lokinpitovelvollisuuksia juuri henkilötietojen suojan turvaamiseksi. Näillä velvollisuuksilla pyritään takaamaan tiettyjen arkaluonteisia henkilötietoja sisältävien tietojärjestelmien asianmukainen käyttö muun muassa poliisitoiminnan sekä sosiaali- ja terveydenhuollon alalla.[144]

On huomattava, ettei yleinen tietosuoja-asetus sen 2 artiklan 2 kohdan d alakohdan seurauksena sovellu suoraan sellaiseen toimivaltaisen viranomaisen suorittamaan henkilötietojen käsittelyyn, joka tapahtuu rikosten ennalta estämisen, paljastamisen tai tutkinnan vuoksi. Näin ollen asetusta ei sovelleta koko laajuudessaan rikosasian yhteydessä poliisin suorittamaan henkilötietojen käsittelyyn, vaan sovellettavaksi tulee erikseen rikosasioiden yhteydessä tapahtuvaa henkilötietojen käsittelyä koskeva direktiivi[145] sekä sen kansallisesti täytäntöön panema laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018). Yleisen tietosuoja-asetuksen sääntely korostuu kuitenkin nimenomaisesti siirrettäessä sähköisiä todisteita EU:n ulkopuolelle, kuten Yhdysvaltoihin. Tällöin sovellettavaksi tulevat yleisen tietosuoja-asetuksen

[142] Riekkinen 2018, s. 92. Kansainvälisen todisteiden hankinnan ongelmista ja ratkaisuehdotuksista ks. sisäministeriö 2017, s. 42–43. Lisäksi kansainvälistä yhteistyötä tietoverkkorikosten tutkinnassa on käsitelty yleisesti Yhdistyneiden kansakuntien (YK) huumeiden ja rikollisuuden torjunnasta vastaavan toimiston (UNODC) selvityksessä. Ks. UNODC 2013, s. 183–223.

[143] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

[144] Riekkinen 2019, s. 14–15. Näistä velvollisuuksista säädetään esimerkiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 5.2 §:ssä ja henkilötietojen käsittelystä poliisitoimessa annetun lain (761/2003) 19 b §:ssä (1181/2013). Lisäksi väestötietojärjestelmältä edellytetään lokinpitovelvollisuutta, josta säädetään väestötietojärjestelmästä ja väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) 56 §:ssä.

[145] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta.

48 artikla sekä 49 artiklan poikkeusperusteet. Näiden artiklojen sisällön tulkintatavoista on ollut erimielisyyksiä, minkä seurauksena viranomaisyhteistyö esimerkiksi EU:n ja Yhdysvaltojen välillä on ollut haastavaa.[146] Artiklojen soveltamisesta ei ole vielä päästy yhteisymmärrykseen, joten henkilötietoja sisältävien sähköisten todisteiden jakaminen EU:n ulkopuolisten toimijoiden kanssa ei selkeää. Yhdysvaltojen ja EU:n viranomaiset ovat kuitenkin päässeet yhteisymmärrykseen sähköisten todisteiden jakamisen tarpeesta, minkä seurauksena ja Euroopan komissio ja Yhdysvallat ilmoittivat maaliskuussa 2022 sopineensa uuden transatlanttisen tietosuojakehyksen yleisistä periaatteista.[147] Osapuolet viimeistelevät tällä hetkellä sopimuksen yksityiskohtia ja muuttavat sen tulevaisuudessa säädöksiksi, jotka muodostavat perustan komission ehdottamalle tietosuojan riittävyyttä koskevalle päätösluonnokselle. Onnistuessaan sopimus parantaisi huomattavasti viranomaisyhteistyön laatua sähköisten todisteiden rajat ylittävän jakamisen osalta selkiyttämällä henkilötietojen suojaan liittyviä tulkintaongelmia.

Tämän lisäksi Euroopan komissio esitti vuoden 2018 alkupuolella todistusaineiston rajat ylittävien siirtojen suhteen keinoja, joiden tarkoituksena on helpottaa sähköisen todistusaineiston rajat ylittävää saatavuutta.[148] Ehdotukset ovat koottu ehdotukseen asetuksesta sähköistä todistusaineistoa rikosoikeudellisissa asioissa koskevista eurooppalaisista esittämis- ja säilyttämismääräyksistä.[149] Tämän lisäksi maaliskuussa 2022 EU:n jäsenmailla annettiin valtuutus allekirjoittaa Budapestin yleissopimuksen lisäpöytäkirja, joka tähtää rajat ylittävien tietosiirtojen helpottamiseen rikostutkintaa suoritettaessa.[150]

Samaan aikaan komissio toteuttaa käytännön toimenpiteitä, joiden tarkoituksena on parantaa sähköisen todistusaineiston rajat ylittävää saatavuutta rikostutkintaa varten.[151] Näihin sisältyy muun muassa rahoitusta rajat ylittävää yhteistyötä koskevaan koulutukseen, sähköisen alustan kehittäminen EU:ssa tapahtuvaa tietojenvaihtoa varten sekä jäsenvaltioiden välisten oikeudellisten yhteistyömuotojen standardointi. Näillä toimenpiteillä pyritään tukemaan viranomaisten toimintaa esimerkiksi tietojen salauksesta johtuvien ongelmien suhteen.

---

[146] Ks. Christakis 2019, s. 7−14.
[147] Euroopan komissio 2022: Trans-Atlantic Data Privacy Framework.
[148] COM(2018) 225 final ja COM(2018) 226 final.
[149] Ks. ehdotus Euroopan parlamentin ja neuvoston asetus sähköistä todistusaineistoa rikosoikeudellisissa asioissa koskevista eurooppalaisista esittämis- ja säilyttämismääräyksistä COM/2018/225 final - 2018/0108 (COD).
[150] Tietoverkkorikollisuutta koskevan yleissopimuksen toinen lisäpöytäkirja, joka koskee tiiviimpää yhteistyötä ja sähköisten todisteiden luovuttamista 2021/0383 (NLE).
[151] Ks. Euroopan komissio 2018b.

4.3.2 Tietojen salaus

Tietojen salausta pidetään tehokkaana tapana huolehtia kyberturvallisuudesta, tietosuojasta sekä yksityisyyden suojasta. Se voi auttaa kansalaisia ja yrityksiä puolustautumaan tietotekniikan väärinkäytöltä, kuten hakkeroinnilta, identiteetti- ja henkilötietojen varkauksilta, petoksilta ja luottamuksellisten tietojen luvattomalta paljastamiselta. Kuten muihinkin tietoteknisiin sovellutuksiin, myös tietojen salaukseen liittyy ongelmia. Rikolliset, kuten verkkopetosten tekijät, voivat käyttää erilaisia salaustapoja piilottaakseen toimintansa lainvalvontaviranomaisilta. Tämä hankaloittaa sähköisen todistusaineiston saatavuutta tai pahimmillaan estää laillisen pääsyn siihen. Lisäksi salauksen käyttö tekee lainvalvontaviranomaisten työstä haastavampaa ja vaikeuttaa rikostutkintaprosessia.

Salauksen käyttö on välttämätöntä kyberturvallisuuden ja henkilötietojen suojan takaamiseksi. EU:n yleisessä tietosuoja-asetuksessa mainitaan erikseen salauksen merkitys asianmukaisen suojan varmistamiseksi henkilötietojen käsittelyssä.[152] Toisaalta lainvalvonta- ja oikeusviranomaiset kohtaavat yhä useammin rikostutkinnan yhteydessä haasteita, jotka johtuvat rikollisten käyttämästä salauksesta. Salaus heikentää lainvalvonta- ja oikeusviranomaisten mahdollisuuksia saada tietoja, joita tarvitaan todisteeksi rikostutkinnassa sekä syytteiden nostamista ja rikollisten tuomitsemista varten. Salauksen käyttö rikollispiireissä on lisääntynyt viime vuosina ja ilmiö vaikuttaa vain jatkavan kasvuaan. Samalla myös salauksen vaikutus rikostutkintaan tulee ainoastaan lisääntymään.[153]

Euroopan komission tasolla on keskusteltu salauksen vaikutuksesta rikostutkintaan sekä teknisten että oikeudellisten näkökohtien kannalta. Ongelma tiedostetaan vakavaksi, ja keskusteluissa onkin ollut mukana keskeisiä toimijoita kuten Europolin, Eurojustin, Euroopan oikeudellisen kyberrikollisuusverkoston (EJCN), Euroopan unionin verkko- ja tietoturvaviraston (ENISA), Euroopan unionin perusoikeusviraston (FRA) ja jäsenvaltioiden lainvalvontavirastojen asiantuntijoita sekä toimialan ja kansalaisyhteiskunnan organisaatioiden edustajia. Komissio totesi raportissaan, että lainvalvonta- ja oikeusviranomaisten kohdatessa rikollisten käyttämää salaustekniikkaa rikostutkinnan yhteydessä niitä tulisi tukea sekä oikeudellisilla toimenpiteillä että teknisillä toimenpiteillä. Oikeudellisilla toi-

[152] Yleinen tietosuoja-asetus, 32 artikla.
[153] Euroopan komissio 2017a, s. 9.

menpiteillä helpotettaisiin pääsyä salattuun todistusaineistoon ja teknisillä toimenpiteillä puolestaan parannettaisiin salauksenpurkuvalmiuksia.[154]

Lainvalvonta- ja oikeusviranomaiset saattavat pystyä palauttamaan osan salatuista tiedoista riippuen siitä, millä tavoin rikolliset ovat käyttäneet salausta. Monet jäsenvaltiot ovat perustaneet kansallisia yksiköitä, joilla on asiantuntemusta salaukseen liittyvien haasteiden ratkaisemisesta rikostutkinnan yhteydessä. Useimmilla jäsenvaltioilla ei kuitenkaan ole käytettävissään tarvittavaa asiantuntemusta ja resursseja. Tämä vaarantaa vakavasti lainvalvonta- ja oikeusviranomaisten mahdollisuudet saada käyttöönsä salattuja tietoja rikostutkintaa varten. Tämän vuoksi komissio on ehdottanut konkreettisia, muita kuin lainsäädännöllisiä toimenpiteitä jäsenvaltioiden viranomaisten tukemiseksi ilman, että salausta kielletään, rajoitetaan tai heikennetään.[155]

Ensinnäkin komissio on esittänyt Europolia salauksenpurkuvalmiuksien kehittämisessä edelleen. Tätä varten komissio ehdotti vuotta 2018 koskevan EU:n talousarvion laatimisen yhteydessä, että Europoliin perustettaisiin yhteensä 86 uutta turvallisuusalan toimea, joilla vahvistettaisiin erityisesti Europolin yhteydessä toimivaa Euroopan kyberrikostorjuntakeskusta. Toiseksi lainvalvonta- ja oikeusviranomaisten tukemisesta esitettiin, että jäsenvaltioiden tasolla tulisi perustaa asiantuntijakeskusten verkosto. Sen avulla kansallisen tason valmiuksia ja asiantuntemusta voitaisiin jakaa paremmin, kansallisia aloitteita kuitenkaan korvaamatta. EU:n tasolla komissio tukee Europolia verkoston keskustoimintojen tarjoamisessa kansallisten asiantuntijakeskusten yhteistyön helpottamiseksi. Kolmanneksi jäsenvaltioilla ehdotettiin vaihtoehtoisten tutkintamenetelmien käyttöön ottamista, jotta voitaisiin helpottaa sellaisten toimenpiteiden kehittämistä ja käyttöä, joiden avulla rikollisten salaamat tiedot saadaan avattua. Ehdotetun asiantuntijakeskusten verkoston olisi osallistuttava tällaisten vaihtoehtoisten tutkintamenetelmien laatimiseen. Neljänneksi komission ehdotti, että huomiota olisi kiinnitettävä palveluntarjoajien ja muiden toimialakumppaneiden merkittävään rooliin vahvaa salausta tarjoavien ratkaisujen toimittamisessa. Ottaen huomioon komission sitoutuminen vahvaan salaukseen, parempi ja jäsennellympi yhteistyö viranomaisten, palveluntarjoajien ja muiden toimialakumppaneiden kesken edistäisi eri osapuolia koskevien nykyisten ja tulevien haasteiden ymmärtämistä. Viidenneksi korostettiin lainvalvonta- ja oikeusviranomaisille suunnattujen koulutusohjelmien merkitystä. Näiden avulla vastuuhenkilöille katsottiin syntyvän paremmat valmiudet hankkia tarvittavat,

[154] Euroopan komissio 2017a, s. 9.
[155] Euroopan komissio 2017b, s. 6.

rikollisten salaamat tiedot. Kuudenneksi tähdennettiin jatkuvan arvioinnin tärkeyttä teknisten ja oikeudellisten näkökohtien suhteen, jotka liittyvät salauksen rooliin rikostutkinnassa, sillä salausmenetelmät kehittyvät jatkuvasti ja rikolliset käyttävät niitä yhä enemmän, jolloin myös niiden vaikutus rikostutkintaan lisääntyy tulevaisuudessa.[156]

Kaiken kaikkiaan salausteknologia muodostaa edelleen jatkuvan ja kasvavan haasteen niin EU:n toimijoiden kuin jäsenvaltioidenkin harjoittamassa rikostutkinnassa. Vuoropuhelut asiantuntijoiden ja keskeisten sidosryhmien kanssa tarjoavat edelleen erilaisia näkökulmia ja näkemyksiä uudesta kehityksestä ja mahdollisista pitkän aikavälin strategioista, kun otetaan huomioon salausvälineiden lisääntyvä hienostuneisuus ja laaja käyttö viestinnässä sekä tarve suojata käyttäjien henkilötietoja. Toisaalta ongelmaan tarvittaisiin myös ripeämpiä sekä selkeämpiä vastauksia, mikä vaatisi tarpeeksi järeiden ja selkeiden lainsäädännöllisten työkalujen kehittämistä viranomaisyhteistyön tukemisen rinnalle.

4.3.3 Tietojen säilyttäminen

Rajat ylittävien tietosiirtojen sekä tietojen salauksen lisäksi tietojen säilyttämisajat muodostavat rikosoikeudellisen ongelman rajat ylittävissä verkkopetostutkinnoissa – vaikka tietojensiirto ja muu viranomaistoiminta toimisivatkin, voi todisteiksi tarvittavat tiedot tulla poistetuksi ennen niihin käsiksi pääsemistä tietojen säilytysajoista johtuvien sääntöjen johdosta. Sähköisten tietojen saatavuus on tärkeää, jotta poliisi ja yleiset syyttäjät voivat tutkia rikoksia, myös silloin, kun ne on tehty verkossa tai ne on otettu käyttöön internetin tai televiestintäverkkojen avulla. Pääsy metadataan[157] puolestaan riippuu siitä, ovatko viestintäpalveluntarjoajat pitäneet metatiedon saatavilla ja säilyttäneet ne. Pääsy metadataan on aina takautuvaa. Tyypillinen rikostutkijan kysymys voi olla esimerkiksi: ”Kuka käytti Internettiä tällä IP-osoitteella kaksi kuukautta sitten?". Tähän kysymykseen vastaamiseksi palveluntarjoajan olisi säilytettävä tiedot kaikesta IP-osoitteiden käytöstä, mukaan lukien kaikkien niiden henkilöiden tiedot, jotka eivät ole syyllistyneet rikoksiin. Näin ollen tietojen säilyttämistä koskevissa säännöissä on kunnioitettava perusoikeuksia, kuten yksityisyyttä ja tietosuojaa sellaisina kuin ne on vahvistettu Euroopan unionin perusoikeuskirjassa.

[156] Euroopan komissio 2017a, s. 10–11.
[157] Eng. non-content data. Metadata eli metatieto tarkoittaa tietoa tiedosta. Esimerkiksi sähköisen viestin lähettämisaika ja viestin osoite ovat metatietoja.

Jäsenvaltioiden erilaiset lähestymistavat metatietojen säilyttämistä koskeviin lakeihin, asetuksiin ja teknisiin määräyksiin johtivat siihen, että EU:n tasolla tarvittiin yhdenmukaistettua lähestymistapaa.[158] Tietojen säilyttämistä koskeva direktiivi hyväksyttiin 15. maaliskuuta 2006.[159] Direktiivillä otettiin käyttöön yleinen velvoite säilyttää tietyt dataluokat kaikkien käyttäjien osalta rikollisuuden torjumiseksi. Tietojensäilytysdirektiivi velvoitti yleisesti saatavilla olevien sähköisten viestintäpalvelujen ja yleisesti saatavilla olevien viestintäverkkojen tarjoajat säilyttämään metadataa 6–24 kuukauden ajan sen varmistamiseksi, että tiedot ovat käytettävissä vakavan rikollisuuden tutkintaa, selvittämistä ja syytteeseenpanoa varten.

Euroopan unionin tuomioistuin (EUT) totesi vuonna 2014 Digital Rights Ireland -tuomiossa,[160] että vaikka tietojen säilyttäminen täyttikin yleisen edun mukaisen tavoitteen vakavan rikollisuuden torjunnasta, tietojensäilytysdirektiivi ei ollut linjassa suhteellisuusperiaatteen kanssa, sillä perusoikeuksiin puuttuminen ei rajoittunut siihen, mikä katsottiin ehdottoman välttämättömäksi rikosten torjumisen suhteen. Näin ollen direktiivi julistettiin pätemättömäksi.[161] Tämän jälkeen unionin tuomioistuin vahvisti vuonna 2016 antamassaan tuomiossa Tele2 Sverige, että sähköisen viestinnän tietosuojadirektiivi[162] on esteenä kansalliselle lainsäädännölle, jossa säädetään tietojen yleisestä ja ilman asianmukaista eristystä tapahtuvasta säilyttämisestä.[163] Euroopan unionin tuomioistuin täsmensi kuitenkin myös, että sähköisen viestinnän tietosuojadirektiivi ei ole esteenä sille, että kansallisessa lainsäädännössä säädetään tietojen kohdennetusta säilyttämisestä vakavan rikollisuuden torjumiseksi edellyttäen, että tällainen tietojen säilyttäminen rajoittuu siihen, mikä on ehdottoman välttämätöntä.[164] Lisäksi EUT määritteli Tele2-päätösessä suojatoimia, joita olisi noudatettava kansallisia tietojensäilyttämislakeja säädettäessä. Nämä suojatoimien vaatimukset olivat:

---

[158] Komission ehdotus Euroopan parlamentin ja neuvoston direktiiviksi yleisten sähköisten viestintäpalvelujen tarjoamisen yhteydessä käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, COM(2005) 438 final, 21.9.2005.
[159] Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettujen tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, EUVL L 105, 13.4.2006, s. 54–63.
[160] Yhdistetyt asiat C-293/12 ja C-594/12 Digital Rights Ireland ja Seitlinger ym.
[161] EUT perusteluiden mukaan tietojensäilytysdirektiivissä ei vahvistettu selkeitä ja täsmällisiä sääntöjä, jotka olisivat koskeneet Euroopan unionin perusoikeuskirjan 7 ja 8 artiklassa tunnustettujen yksityisyyttä ja henkilötietojen suojaa koskevien oikeuksien soveltamisalaa ja perusteltuja rajoituksia. Tapauksen taustoista tarkemmin ks. Dupont – Cilli – Omersa 2020, s. 24–25.
[162] Direktiivi 2002/58/EY.
[163] Ks. Yhdistetyt asiat C-203/15 ja C-698/15 Tele2 Sverige.
[164] EUT täsmensi tarkemmin rikoksen vakavuuden käsitettä asiassa C 207/16 Ministerio Fiscal.

1. Muiden kuin sisältötietojen säilyttämisen olisi oltava poikkeus.
2. Tarkoitus olisi rajoitettava vakavan rikollisuuden torjuntaan.
3. Säilyttäminen olisi rajoitettava siihen, mikä on ehdottoman välttämätöntä.
4. Tuomioistuimen tai riippumattoman viranomaisen olisi valvottava etukäteen pääsyä tietoihin.
5. Tietoja olisi säilytettävä vain EU:ssa.

Kuitenkin Privacy Internationalin raportissa vuodelta 2017 todettiin, että useimmissa jäsenvaltioissa tietojensäilyttämisjärjestelmät perustuivat edelleen aiemmin kumottuun tietojensäilytysdirektiiviin.[165] Mietinnössä todettiin lisäksi, että kansalliset tietojensäilyttämisjärjestelmät olivat usein vanhentuneita ja ne eivät olleet oikeudellista selkeitä. Vain muutamat maat ovat sittemmin ottaneet käyttöön uusia oikeudellisia lähestymistapoja noudattaakseen Euroopan unionin tuomioistuimen oikeuskäytäntöä.[166]

Ranskasta[167], Belgiasta sekä Yhdistyneenestä kuningaskunnasta[168] on esitetty ennakkoratkaisupyyntöjä koskien Tele2-vaatimusten ja sähköisen viestinnän tietosuojadirektiivin 15 artiklan sovellettavuutta kansallisen turvallisuuden ja lainvalvonnan alalla, erityisesti sitä, olisiko unionin tuomioistuimen oikeuskäytäntöä sovellettava lainsäädännöllisiin instrumentteihin, joilla turvataan kansallinen turvallisuus ja terrorismin torjunta. Tällaiset keinot koskisivat myös verkkopetosten ja muiden tietoverkkorikosten kannalta tärkeiden sähköisten todisteiden säilyttämistä. EU:n julkisasiamiehen lausunnot näistä ennakkoratkaisupyynnöistä noudattavat unionin tuomioistuimen aiemmin vakiintunutta tulkintalinjaa, jonka mukaan metadatan yleinen säilyttäminen ei ole sallittua jäsenvaltioiden turvallisuus- ja tiedustelupalveluille ja että kaiken pääsyn tällaisiin tietoihin on täytettävä Tele2-tuomiossa vahvistetut edellytykset.[169]

Euroopan unionin tuomioistuimen oikeuskäytäntöä on kritisoitu jäsenvaltioiden keskuudessa, sillä EUT:n linjaukset ovat herättäneet huolta nykyisen lainsäädäntökehyksen oikeusvarmuudesta suhteessa rikosten havaitsemiseen, tutkintaan ja syytteeseenpanoon sekä

[165] Ks. Privacy International 2017.
[166] Dupont – Cilli – Omersa 2020, s. 25.
[167] C-511/18 ja C-512/18 Ranskan dataverkko, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet assosiatiivit v Premier ministre, Garde des Sceaux, Ministre de la Justice.
[168] C-623/17 Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others.
[169] Dupont – Cilli – Omersa 2020, s. 26.

oikeudelliseen yhteistyöhön rajat ylittävissä tapauksissa.[170] Metatietojen käytöstä todisteena rikosoikeudellisissa syytetoimissa liittyy oikeudellista epävarmuutta myös siksi, että puolustusasianajajat ympäri Eurooppaa ovat kyseenalaistaneet tällaisten tietojen käytön hyväksyttävyyden.[171]

Europolin mukaan EUT:n asettamat vaatimukset eivät vastaa todellisuutta rikostorjunnan tarpeiden kannalta. Europol ehdottaakin, että tarkasti kohdennetun, valvotun ja eristetyn säilyttämisjärjestelmän sijaan olisi pyrittävä sallimaan pääsy säilytettyihin kaikenlaisiin sähköisiin todisteisiin ja metatietoihin.[172]

EU-oikeudellisen sääntelyn lisäksi tietojen saatavilla oloa rikostutkintaa varten yritetään turvata myös muilla tavoin. Esimerkiksi EU:n komission tavoitteena on korjata tietopuutteita ja kerätä tietoa rikostutkintaa sekä syytetoimia koskevien pakollisten tietojensäilyttämiskehysten oikeudellisista, operatiivisista ja perusoikeuksiin liittyvistä haasteista, todisteiden hyväksyttävyyteen liittyvistä kysymyksistä sekä vaikutuksista sähköisten viestintäpalvelujen tarjoajiin ja niiden käyttäjiin. Lisäksi Euroopan komissiossa ja Euroopan unionin neuvostossa on käyty asiantuntijakeskusteluja Euroopan unionin lainvalvontayhteistyöviraston Europolin ja Euroopan unionin rikosoikeudellisen yhteistyön viraston Eurojustin kansa tarkoituksena määrittää tietojen säilyttämisen tärkeimmät näkökohdat.[173]

Kansallisella tasolla tietojen säilyttämistä säädetään erikseen useissa laeissa erityisesti henkilötietojen osalta. Nämä kansalliset lait ovat EU:n linjassa yleisen tietosuoja-asetuksen kanssa, jossa tietojen säilytysajoista säädetään 5 artiklassa. Lähtökohtana on rekisteröityjen valta määrätä itse tietojensa säilyttämisestä, eikä henkilötietoja sisältävän rekisterinpitäjän tule säilyttää henkilötietoja pidempään kuin on kulloinkin tarve. Verkkopetostutkintojen kannalta tärkeimpiä sähköisiä todisteita hallitsevat yleensä erilaiset verkkopalveluntarjoajat, ja näiden hallinnoiman datan säilyttämisestä säädetään laissa sähköisen viestinnän palveluista (2014/917). Sähköisen viestinnän palvelulain (SVPL) 19 luvussa tele- ja internetyhteyspalveluja tarjoaville yrityksille asetetaan velvollisuus säilyttää välitystietoja viranomaistoiminnan tarpeita varten, kuten esimerkiksi rikosten selvittämiseksi ja syytehar-

[170] Dupont – Cilli – Omersa 2020, s. 27. EU:ssa sähköisten todisteiden säilytysajat ovat yleisen tietosuoja-asetuksen 5 artiklasta johtuen lyhyitä ja vaihtelevat runsaasti. Maailmalla vakiintunut teleyirtysten datan säilytysaika on kaksi vuotta. Esimerkiksi Australian telecommunications act säätää säilytysajan vähintään kahden vuoden mittaiseksi.
[171] Tutkittavaksi ottamista koskeva kysymys on esitetty esimerkiksi EUT:n tapauksessa C-140/20 Commissioner of the Garda Síochána ym.
[172] Dupont – Cilli – Omersa 2020, s. 26.
[173] Privacy International 2017.

kintaan saattamiseksi. SVPL 157 § määrittelee säilytysvelvollisuuden sisällön ja säilytysajat, 158 § puolestaan säätää tietojen käsittelyssä noudatettavista velvoitteista ja menettelytavoista ja 159 § sisältää sisäministeriölle suunnatun velvollisuuden toimittaa eduskunnan oikeusasiamiehelle tilastotiedot säilytettävien tietojen hyödyntämisestä.[174] SVPL:n sääntely perustuu käytännössä edelleen jo kumottuun direktiiviin 2006/24/EY, jonka EUT totesi pätemättömäksi Digital Rights Ireland -tuomiollaan.[175] SVPL:n EU-oikeudellinen pohja on siten epävakaa. Toisaalta EUT:n oikeuskäytännössä tai muutoinkaan EU-oikeuden piirissä ei ole vielä määritetty uutta harmonisoitua tapaa toteuttaa tietojen säilyttämisvelvollisuutta. Näin ollen sähköisille palveluntarjoajille asetettavan datan säilytysvelvollisuuden suhteen on kansallista liikkumavaraa. Tämä on huomionarvoista, sillä verkkoavusteisten petosrikosten tutkinnoissa dataa voidaan tarvita todisteena varsin myöhään itse petostapahtuman jälkeen. Erityisesti rajat ylittävissä tutkinnoissa voi kestää hyvinkin pitkään.[176] Tällöin datan häviäminen tai hävittäminen ennen todisteiden keräämistä muodostaa rikostutkinnalle ongelman. Luonnollisesti itse datan riittävän säilyttämisajan lisäksi on tärkeää, että viranomaisilla on myös riittävä valtuudet päästä käsiksi näihin sähköisiksi todisteiksi katsottaviin tietoihin. Tästä säädetään sähköisen viestinnän osalta pakkokeinolain 10 luvun 6 §:ssä.[177] Datan säilytysaikojen ja viranomaisen dataan pääsyn tulee olla yhtä pitkiä ja mahdollistaa verkkopetosten riittävä tutkinta. Vallitsevaa lainsäädännön tilaa voidaan perustellusti tältä osin kritisoida, sillä esimerkiksi lievien verkkoavusteisten petosten osalta poliisilla ei ole mahdollisuuksia saada haltuunsa tarvittavia sähköisiä todisteita PKL 10:6.2:n teleosoitteita ja telepäätelaitteita käyttäviä rikoksia koskevan kohdan sanamuodosta johtuen.

Kansallisten ja EU:n lainsäätäjien suurimpana haasteena on löytää oikeudenmukainen tasapaino kahden vastakkaisen tarpeen välillä – toisaalta tulisi turvata yksilön oikeudet yksityisyyteen ja henkilötietojen suojaan, mutta toisaalta pitäisi pystyä vastaamaan lainvalvontaviranomaisten tarpeeseen saada tietoja tutkintaa ja syytetoimia varten ottaen samalla huomioon unionin tuomioistuimen oikeuskäytännön vaatimukset. Erilaisten ja jossain mää-

[174] Alun perin tietoyhteiskuntakaarena tunnetulla SVPL:lla kumottiin sähköisen viestinnän tietosuojalaki (516/2004), joka oli suurimmaksi osaksi SVPL:a vastaava säilyttämisvelvollisuutta koskevilta säännöksiltään (14 a § – 14 c §). Ks. tarkemmin HE 221/2013 vp s. 155–157.
[175] Yhdistetyt asiat C-293/12 ja C-594/12 Digital Rights Ireland ja Seitlinger ym. Riekkinen on huomauttanut, että direktiivin pätemättömyyden ei lakia valmisteltaessa katsottu edellyttävän merkittäviä muutoksia sääntelyn sisältöön. Riekkinen 2019, s. 258. Ks. myös PeVL 18/2014 vp s. 4–9 ja LiVM 10/2014 vp s. 24–27, 37–39.
[176] Riekkinen 2019, s. 254.
[177] Pakkokeinolaissa säädetään myös datan säilyttämismääräyksen sisällöstä ja antamisesta. Säilyttämismääräyksestä tarkemmin ks. Riekkinen 2019, s. 256–259.

rin epäselvien oikeudellisten kehysten aiheuttamien vaikeuksien lisäksi sähköisten todisteiden ja metatietojen säilyttämiseen liittyy tulevaisuudessa haasteita, jotka johtuvat televiestintäalan tulevista teknologisista muutoksista.

4.4 Kansallinen sääntely ja oikeuskäytäntö

Suomessa todisteiden hankintaa ja esitutkintaa koskevat oikeudelliset säännökset ovat suurimmaksi osaksi kirjattu esitutkintaa yleislakina ohjaavaan esitutkintalakiin (805/2011, ETL) sekä pakkokeinojen käyttöön ja käytön edellytyksiin sovellettavaan pakkokeinolakiin. Näiden lakien lisäksi poliisin toimivaltuuksia säännellään poliisilaissa (872/2011, PolL).[178]

Sähköisten todisteiden käyttämisen ja datan säilyttämisen lisäksi edellä on käsitelty jo verkkopetoksia sääntelevää petostunnusmerkistöä, maksuvälinepetoksia sekä verkkopetoksiin liittyviä identiteettivarkauksia. Lisäksi kansallisen sääntelyn näkökulmasta verkkopetoksiin on luotu talousrikosoikeudellinen katsaus. Näiden katsantojen jälkeen tulee käsitellä oikeuskäytäntöä kokonaisvaltaisen sääntelyllisen kuvan muodostamiseksi. Verkkoavusteisista petoksista ei ole kuitenkaan annettu ennakkopäätöstasoista ratkaisua, ja alempien tuomioistuimien antamat ratkaisut koskevat pääasiallisesti olemattoman tavaran myyntiä, tilauspetoksia sekä muita taloudellisilta vaikutuksiltaan pieniä tai muutoin sangen yksinkertaisesti toteutettuja petoksia.[179]

Verkon universaalisia vaikutuksia tai verkkopetoksille ominaista problematiikkaa käsittelevää tai oikeuskäytäntöä ei siis ole. Tästä on pääteltävissä kolme asiaa. Ensinnäkin voidaan sanoa, että mitään verkkoavusteisille petoksille ominaista juridista ongelmaa ei ole olemassa, koska sellaista ei ole vielä tänäkään päivänä käsitelty ylimmillä oikeusasteilla. Tämä voisi viitata siihen, että verkkopetosten oikeudellisessa arvioinnissa ei ole ongelmallista sopivien tunnusmerkistöjen puute tai täyttyminen.[180] Nykyinen sääntelykonteksti olisi riittävän selkeä verkkoavusteisten petosten kattavaksi käsittelemiseksi, minkä seurauksena monimutkaisetkin petostapaukset on käsitelty alempien oikeusasteiden puitteissa. Toisaalta tähän voidaan vastata, että oikeuskäytännön puute voi yhtä hyvin johtua siitä, ettei juridista problematiikkaa korostavia petosrikostapauksia ole kohdistunut Suomen alueelle, eikä

[178] Sähköisestä todistelusta petosrikosten osalta Suomessa ks. Riekkinen 2018, s. 87–91.
[179] Näin on esimerkiksi Helsingin ja Rovaniemen hovioikeuksien vuoden 2016 jälkeen annettujen julkisten verkkopetostuomioiden kohdalla, jotka käytiin läpi tutkimusaineistoa kerätessä.
[180] Ks. myös Riekkinen 2018, s. 94.

merkittävistä verkkopetoksista vain yksinkertaisesti ole jääty kiinni Suomessa.[181] Kolmanneksi suurten ja monimutkaisten verkkoavusteisten petosten tutkinnat ja mahdolliset oikeudenkäynnit ovat voinee tapahtuneet ulkomailla rikollisten kansalaisuuden vuoksi.[182]

Analogista tulkintaa hyväksikäyttämällä voidaan kuitenkin hakea hieman johtoa oikeuskäytännöstä. Tapaus KKO 2011:84 on tähän tarkoitukseen sopiva ennakkopäätös, sillä se käsittelee rajat ylittävää ja laajamittaista petosrikossarjaa. Tapauksessa itävaltalainen yhtiö oli lähettänyt lukuisille suomalaisille tavaramerkin haltijoille kirjeen, jonka otsikossa oli viitattu vastaanottajan tavaramerkin rekisteröintiin. Kirjeessä oli kuvattu vastaanottajan tavaramerkki ja sen rekisteröintitiedot. Siinä oli esitetty vastaanottajan maksettavaksi maksua, jonka maksamiseksi kirjeeseen oli liitetty myös esitäytetty tilisiirtolomake eräpäivämerkinnöin. Tapauksessa oli kysymys siitä, oliko vastaanottajia erehdytetty maksamaan maksu siinä käsityksessä, että maksu liittyi heidän tavaramerkkinsä ylläpitoon, vaikka se tosiasiassa koski tavaramerkin julkaisemista itävaltalaisyhtiön verkkosivuilla, ja oliko kirjeen lähettämisestä vastuussa ollut yhtiön toimitusjohtaja syyllistynyt petokseen.

Tapauksen analoginen arviointi keskittyy tarkastelemaan ratkaisua organisoituna, laajamittaisena ja kansainvälisenä petosrikoksena. Valitulle näkökulmalle on kolme perustetta. Ensinnäkin kuten aiemmin on mainittu, nimenomaisesti verkkoavusteisia petoksia ei ole arvioitu Suomessa ylimmän tuomioistuimen tasolle. Myöskään Euroopan Unionin tuomioistuimessa tai Euroopan ihmisoikeustuomioistuimessa ei ole ollut käsiteltävänä vastaavia tapauksia. Tästä puutteesta johtuen riittävän samankaltaisen tapauksen analysoiminen analogian keinoin verkkopetosten näkökulmasta on mielekästä. Toiseksi erehdyttävästi laskulta vaikuttavan viestin lähettäminen laajasti ja suunnitelmallisesti eri elinkeinonharjoittajille ulkomailta käsin muistuttaa pitkälti verkkopetosten toiminta-ajatuksen ydintä − toiminta on suunnitelmallista ja rikoksella saatavat hyödyt suuria suhteessa rikoksesta aiheutuvaan vaivaan ja kiinnijäämisriskiin. Viesti on myös rinnastettavissa sähköpostiin ja muihin elektronisiin viesteihin. Kolmanneksi itävaltalaisen yhtiön toiminta sijoittui verkkoon, ja huijauslaskujen lähettäminen oli suuntautunut useisiin eri Euroopan maihin, mikä osaltaan vaikeutti tapauksen arviointia. Näin ollen tapauksen analyysissä voidaan perustellusti käyttää analogiaa hyödyntävää näkökulmaa verkkoavuteisten petosten suhteen.

[181] Lisäksi Riekkinen on todennut, että verkkopetoksiin voi hyvin liittyä myös näytön arvioinnin kannalta huomionarvoisia kysymyksiä. Ks. Riekkinen 2018, s. 94–100.
[182] Ks. esim. Eurojust 2022. Kyseessä oli internetissä ja puhelimitse sijoituspetoksia tekevän järjestäytyneen rikollisorganisaation puhelinkeskuksien ja yli viidenkymmenen rikollisten petoksiin käyttämän verkkopalvelimen sulkeminen. Rikollisorganisaatio toimi useissa eri maissa ja verkossa. Operaatioon osallistui viranomaisia Suomesta, Hollannista, Latviasta, Ranskasta, Saksasta sekä Ukrainasta.

Tarkemmin avattuna tapauksessa itävaltalaisen Trademark Publisher GmbH -nimisen yhtiön toimitusjohtaja ja määräysvallan käyttäjä 1.1. ja 30.4.2004 välisenä aikana oli erehdyttänyt tai yrittänyt erehdyttää 6694 suomalaista elinkeinonharjoittajaa kutakin erikseen maksamaan yhtiölle vähintään 587 euroa hankkiakseen itselleen ja toiselle oikeudetonta taloudellista hyötyä. Korkein oikeus tuomitsi yhtiön toimitusjohtajan törkeästä petoksesta.

Trademark Publisher GmbH:n toiminta-ajatus oli ollut ylläpitää internetissä kotisivuillaan tietokantaa eri maissa rekisteröidyistä tavaramerkeistä. Yhtiö oli lähettänyt ulkomaisille elinkeinonharjoittajille erehdyttävästi laskun näköisiä kirjeitä, joita yhtiö kutsui markkinointikirjeiksi. Suomessa 315 vastaanottajaa suoritti yhtiölle maksun luullen näitä kirjeitä laskuiksi tavaramerkeistään. Kukaan asiassa kuulluista asianomistajien edustajista ja työntekijöistä ei ollut jälkikäteen pitänyt tarpeellisena edustamansa yrityksen tai yhteisön tavaramerkin saamista Trademark Publisher GmbH:n tietokantaan. Asiassa ei ollut tullut ilmi, että yritykset edes olisivat voineet saada jotain hyötyä Trademark Publisher GmbH:n tarjoamasta palvelusta.

Trademark Publisher GmbH ja sen toimitusjohtaja katsoivat, että tavaramerkin haltija oli saanut maksusuorituksen vastikkeeksi tavaramerkkinsä rekisteröidyksi yhtiön tietokantaan. Se, että kirjeeseen liittyi tililleпanolomake, ei tehnyt heidän mukaansa siitä laskua. Vastaajien mielestä vastaanottajat eivät olleet riittävän huolellisesti perehtyneet kirjeeseen, mikäli he olivat maksaneet maksun erehdyksessä.

Korkeimman oikeuden perusteluissa tarkastellaan kirjeiden ulkoasua erittäin tarkasti. Vaikka vastaajien mukaan kirjeet lukemalla vastaanottajan tuli ymmärtää palvelun markkinaidea, ei korkein oikeus ollut samaa mieltä. Esimerkiksi kirjeiden kääntöpuolella on ollut palvelusta hajanaisia tietoja, mutta korkeimman oikeuden mukaan niidenkään perusteella ei ole voinut saada selvää kuvaa siitä, mitä merkitystä tavaramerkkien julkaisemisella on ollut asianomaisten merkinhaltijoiden kannalta. Kaiken kaikkiaan korkein oikeus katsoi varsin kattavin ja vakuuttavin perustein kirjeen olevan sisällöltään ja ulkoasultaan laadittu tavalla, joka on ollut omiaan antamaan vastaanottajalle harhaanjohtavan käsityksen siitä, että kysymys olisi ollut hänen tavaramerkkinsä rekisteröintiin perustuneen tai sen voimassa pysymiseen liittyneen maksun perimisestä.[183]

Lisäksi hovioikeuden tavoin korkeimmassa oikeudessa katsottiin, että yhtiö ei tosiasiallisesti saanut asiakkaita juurikaan muutoin kuin kysymyksessä olevien kirjeiden kautta, mi-

[183] Ks. KKO 2011:84 kohdat 8–16.

kä osaltaan osoitti, ettei kirjeiden kohdeyrityksillä ollut tällaiselle palvelulle tarvetta. Korkein oikeus katsoi, että Trademark Publisher GmbH oli näin ollen hankkinut tai yrittänyt hankkia huomattavaa hyötyä erehdyttämällä kirjeen saajia maksamaan palvelusta, jota nämä eivät todellisuudessa olisi halunneet ostaa. Suurelle joukolle yrityksiä oli siten aiheutunut taloudellista vahinkoa niiden erehtyessä maksamaan tarpeettomasta palvelusta. Oikeuden mukaan toimitusjohtaja oli menetellyt mainitulla tavalla, vaikka hänen oli täytynyt tietää, että hänen menettelynsä oli Itävallassa nimenomaisesti kiellettyä. Näin ollen korkein oikeus katsoi tavoitellun taloudellisen hyödyn olleen oikeudetonta.[184]

Petoksen tunnusmerkistö edellyttää tahallisuutta. Näin ollen korkeimman oikeuden arvioitavana oli myös Trademark Publisher GmbH:n toimitusjohtajan tahallisuus. Toimitusjohtaja oli vastannut kirjeen ulkoasusta ja ollut eri tahojen toimesta tietoinen sen erehdyttävyydestä. Toisaalta hän oli kuitenkin pyrkinyt suomalaisen asianajajan avulla varmistamaan kirjeiden sisällön olevan linjassa suomen lainsäädännön kanssa. Tämä ei kuitenkaan korkeimman oikeuden mukaan ollut riittävää poistamaan tahallisuutta, sillä asianajaja oli nähnyt vain viestien luonnokset. Näin ollen toimitusjohtajan toiminta katsottiin tahalliseksi.[185]

Lopulta arvioitiin myös elinkeinonharjoittajien omaa selvitysvelvollisuutta, minkä osalta korkein oikeus totesi suhteellisen yksioikoisesti, että tarjoukseksi tarkoitetun asiakirjan laatiminen erehdyttävästi laskua muistuttavaksi ei ole sellainen toimintatapa, jota edes elinkeinoelämän piirissä olisi syytä suojata asettamalla vastaanottajalle ankara ja lähettäjän rikosoikeudellisen vastuun poistava selonottovelvollisuus. Näin ollen vastaaja oli syyllistynyt petokseen.

Tapauksen kansainvälisyyden osalta on syytä huomata, että korkeimman oikeuden käsittelyssä oli myös muissa valtioissa annettujen ratkaisujen vaikutus, sillä yhtiö oli harjoittanut samanlaista toimintaa myös muissa maissa. Tältä osin korkein oikeus katsoi, että niin sanotun *ne bis in idem* -kiellon mukainen kielto syyttää tai rangaista kahdesti samasta asiasta ei soveltunut tilanteeseen, koska ei ollut tullut näytetyksi, että asianomistajat olisivat olleet samoja tai markkinoinnissa käytetty kirje olisi ollut sama kuin korkeimmassa oikeudessa käsitellyssä asiassa.[186] Näin ollen tapauksen kansainvälisiä ulottuvuuksia ei käsitelty enempää.

[184] Ks. KKO 2011:84 kohdat 17–20.
[185] Ks. KKO 2011:84 kohdat 21–24.
[186] Ks. KKO 2011:84 kohdat 1–2.

Tapauksen perustelut ovat kattavat ja loogiset. Lisäksi perustelut ovat linjassa alempien oikeuksien perusteluiden sekä tuomioiden kanssa. On kuitenkin huomattava, että niin hovioikeuden kuin korkeimmankin oikeuden päätökset olivat äänestysratkaisuja. Eri kannalla olleiden oikeusneuvoksien mielestä kirjeitä ei olisi pitänyt tulkita erehdyttäviksi. He korostivat yritysten selonottovelvollisuutta sekä suomalaisen asianajajan kautta tehdyn kirjeen laillisuusselvityksen merkitystä. Lopputuloksena he olisivat hylänneet syytteet törkeästä petoksesta vahingonkorvausvaateiden ohella. Äänestysratkaisulla ei kuitenkaan ole merkitystä tapauksen analogisten verkkopetoksia koskevien vaikutusten suhteen, joten äänestysratkaisun merkitystä ei tässä yhteydessä käsitellä enempää.

Tapauksella on ensinnäkin huomattavia vaikutuksia rikosten yksiköinnin kannalta, vaikka tapauksessa rikosten yksiköinti on sivuutettu ilman merkittäviä perusteluja.[187] KKO 2011:84 perusteella voidaan esimerkiksi todeta, että tietyissä sarjarikoksissa, kuten internetissä usealle myydyissä tuotteissa ilman tosiasiallista tarkoitusta toimittaa tuotetta ostajalle, ollaan siirtymässä yksittäisistä asianomistajakohtaisista petosrikoksista yhdeksi rikokseksi yksiköitäväksi tekokokonaisuudeksi.[188] Tämä on huomionarvoista erityisesti verkkopetosrikosten arvioinnin ja käsittelyn suhteen. Verkkopetokset kohdistuvat usein laajoihin ihmisryhmiin tai useisiin organisaatioihin. Esimerkiksi tapauksessa pelkästään Suomessa petosyritys kohdistui vajaaseen seitsemääntuhanteen suomalaiseen elinkeinonharjoittajaan. Tästä huolimatta yksittäisiä petoksia arvioitiin kuitenkin yhtenä laajamittaisena tekona. Näin ollen tapauksesta on nähtävissä, että vastaavanlaiset petosrikokset tulee nähdä sekä arvioida yksittäisinä kokonaisuuksina erillisten rikosten sijaan.

Lisäksi tapaus on jossain määrin merkittävä yleisesti verkkorikosten näkökulmasta. Tapauksesta on nimittäin nähtävissä laaja-alaisisten petosrikoksisten tapaan, kuten verkkopetoksissa, että tapausten oikeudellisessa arvioinnissa annetaan organisaatioiden omalle selonottovelvollisuudelle enemmän painoarvoa kuin muutoin. Elinkeinonharjoittajilla on yleensä yksityishenkilöjä paremmat resurssit erilaisiin selvitystoimenpiteisiin. Toisaalta myös liiketoimeen liittyvä sekä mahdollisesti suurempi rahamääräinen intressi voi puoltaa riskien tarkempaa selvittämistä. Ratkaisun KKO 2011:834 mukaan, siinä määrin kuin annettu informaatio on selkeästi tarkoituksellisen harhaanjohtavaa, myös elinkeinoelämän osalta rangaistusvastuun poistavan myötävaikutuksen raja on säädetty varsin korkealle.[189]

[187] Ripatti 2020, s. 223.
[188] Kukkonen 2016, s. 736. Ks. myös Koponen 2015, s. 614–616.
[189] Riekkinen 2018, s. 93–94.

Tässä suhteessa on huomattava, että varsin laajalla vastaanottajakunnalle kohdistunut viesti tulkittiin kuitenkin harhaanjohtavaksi ilman vastaanottajien sen suurempaa perehtymistä itse viestiin. Näin ollen on tulkittavissa, että mitä suuremmalle yleisölle petosviesti kohdistuu, sitä suurempi merkitys petosviestin mahdolliselle harhaanjohtavuudelle on annettava. Verkkopetosten osalta tällä huomiolla voi olla suurikin vaikutus.

Tapauksesta on lisäksi nähtävissä, että rajanylittävätkin petostapaukset ovat suomen tuomioistuimien toimivallan puitteissa, vaikka teot olisivat ulottuneet muihin maihin asti ja tekijät toimivat muusta maasta käsin. Tämä on vastaavanlaisten kansainvälisten tapausten suhteen merkittävä havainto. Se seikka, että petosteot kohdistuvat tiettyyn maahan, ei estä kyseistä maata käyttämästä oikeuttaan tekijää kohtaan. Lisäksi yksittäisten rikosten lukuisa määrä ei estä käsittelemästä tekoja yhtenä laaja-alaisena kokonaisuutena. Toisaalta on myös huomattava, että tapaus ei ole lopulta puhdas verkkopetos, joten liian pitkälle meneviä johtopäätöksiä ei teeman suhteen ole tehtävissä.

Lopulta on myös annettava painoarvoa sille, että vaikka petollisesta viestistä vastuussa ollut toimitusjohtaja on yrittänyt selvittää kohdemaan lainsäädäntöä viestilleen sopivaksi, tällä ei ole ollut lopulta ratkaisevaa merkitystä sen kanssa, että teon mukainen menettely on katsottu törkeäksi petokseksi. Näin ollen voidaan tehdä se havainto, että vaikka verkkopetosten tekijät olisivat kotimaisia tai heillä olisi jonkinlainen kotimainen selvitys petoksensa pohjaksi, eivät nämä seikat poista petoksesta seuraavaa rikosoikeudellista vastuuta. Verkkopetokset voivatkin olla mitä eri näköisempiä, mutta lopulta petoksen tunnusmerkistön ytimessä olevat erehdyttämisen, taloudellisen hyödyn tavoittelun sekä tahallisuuden kriteerit määrittelevät rikoksen tunnusmerkistön täyttymisen.

Korkeimman oikeuden ratkaisu 2011:84 käsittelee ulkomailta Suomeen käsin kohdistuvaa petosvyyhtiä, joka on yksiköitävissä omaksi rikosoikeudelliseksi kokonaisuudekseen. Samalla tapaus on yksi ainoita laatuaan Suomessa verkkopetosten näkökulmasta. Verkkopetosten kohteena on yleisimmin yksityishenkilö elinkeinonharjoittajan sijaan. Kuitenkin suurin taloudellinen vahinko syntyy eri organisaatioihin ja yrityksiin kohdistuvista petosrikoksista, joiden alustana toimii yhä etenevissä määrin internet. Tapauksen perusteella tärkein johtopäätös on, että ulkomailta tehdyt, useisiin eri kohteisiin suuntautuneet petokset voidaan nähdä ja käsitellä yhtenä petoksena, jossa teon systemaattisuudelle ja järjestelmäl-

lisyydelle on annettava merkitystä asianomistajina olleiden yhtiöiden oman selonottovelvollisuuden ohi.[190]

5 Verkkoavusteisten petosten haasteet rikostorjunnassa

5.1 Rikostorjunnan haasteiden määrittämisestä

Taloudellisesti motivoitunut verkkoavusteinen rikollisuus on merkittävä, kasvava ja koko yhteiskunnan läpäisevä rikollisuuden muoto. Aiemmissa kappaleissa esiteltyjen erilaisten verkkoavusteisten petosten monimuotoisuuden ja yleisyyden valossa nähdään käsillä olevan varsin problemaattinen ilmiö sekä kansallisen että kansainvälisen rikostorjunnan kannalta. Haasteita verkkorikollisuuden ja -petosten torjunnalle ja sääntelyn kautta tapahtuvalle rikosten ehkäisylle asettavat esimerkiksi rikostorjuntaan osoitettujen resurssien vähäisyys sekä rikosoikeudelle tyypillinen, mutta verkkopetosten yhteydessä erityisesti korostuva lainsäätäjän hidas reagoimismahdollisuus uudenlaisen rikollisuuden esiintymisen suhteen.[191]

Ennen kuin verkkoavusteisen petosrikollisuuden luontoa ja sen aiheuttamia haasteita voidaan *de facto* ymmärtää oikeudellisessa kontekstissa, tulee luoda katsaus tietoverkkojen luomiin universaalisiin vaikutuksiin rikollisuuden suhteen. Lisäksi rikostorjunnan haasteiden erittelemiseksi on tunnettava nykyiset sääntelylliset keinot verkkorikoksia vastaan toimimisesta. Tätä tukee yritysten rikostorjunnallisen näkökulman ymmärtäminen. Kun tietoverkkojen rikosoikeudellisia vaikutuksia reflektoidaan sääntelyn nykytilaan, voidaan tehdä perusteltuja johtopäätöksiä sääntelyn mahdollisista aukoista ja kehitystarpeista rikostorjunnan tulevaisuuden suhteen. Samalla on muistettava, että sääntely yksinään ei vastaa rikollisuuden ehkäisemisestä, vaan ongelma on myös kriminologisesti ja kriminaalipoliittisesti arvioitava yhteiskunnallinen ilmiö.

[190] Toisaalta juuri selonottovelvollisuus oli yksi tapauksen kiistakysymyksistä. Mikäli vastaava tapaus tulisi uudestaan korkeimman oikeuden käsiteltäväksi, voitaisiin tapaus hyvin mahdollisesti ratkaista myös toisin. Elinkeinonharjoittajan korostunutta selonottovelvollisuutta voitaisiin peräänkuuluttaa erityisesti siinä tapauksessa, että käsiteltävä petos kohdistuisi suureen yksittäiseen organisaatioon, jolla on käytössään paljon resursseja sekä petosten torjuntaan osoitettua henkilöstöä ja protokollia.
[191] Sisäministeriö 2017, s. 31 ja Liite 1.

5.2 Talousrikoksista ja verkkopetoksista organisaatioiden näkökulmasta

Rikostorjuntaa tapahtuu myös lainsäädännön ja viranomaistoiminnan ulkopuolella. Kokonaisvaltaisen petosten torjunnan tilannekuvan luomiseksi on hyvä luoda katsaus myös yritysten sisäiseen rikostorjuntaan ja riskienhallintaan. Verkkoavusteisten petosten ja talousrikoksien asettama paine organisaatioihin onkin suurta. Esimerkiksi PwC:n vuonna 2022 tuottaman kansainvälisen talous- ja petosrikoskyselyn mukaan 46 % kyselyyn vastanneista organisaatioista ilmoitti kokeneensa petoksia, korruptiota tai muita talousrikoksia viimeisen 24 kuukauden aikana.[192] Tästä syystä monet liike-elämän toimijat yrittävät luonnollisesti ehkäistä itseensä kohdistuvia sekä ulkoisia että sisäisiä talousrikoksia.[193] Kuten aiemmin on tuotu esille, verkkopetosten torjuminen on kuitenkin haastavaa. Esimerkiksi monet finanssialan toimijat kuten pankit tarkastelevat talousrikoksia, petoksia ja tietoverkkorikoksia erillisinä ilmiöinä. Tällainen siiloutunut lähestymistapa näihin toisiinsa liittyviin riskeihin on muuttumassa yhä kestämättömämmäksi. Lisäksi talousrikollisuuden ja petosriskien aiheuttamat ja koko ajan kasvavat kustannukset ovat yksi organisaatioiden kohtaamista moderneista ongelmista.[194]

Kun pankit alkavat kohdistaa toimintaansa talousrikollisuuden muuttuvaan profiiliin, ne kohtaavat tietoverkkorikkomusten ja useimpien talousrikosten välisten yhteyksien syvenemisen. Tietoverkkoelementti ei ole tarkalleen ottaen uusi. Esimerkiksi viime aikoihin asti suurin osa petoksista on perustunut varallisuustransaktioihin. Rikolliset ovat hyödyntäneet näiden transaktioiden valvonnan heikkouksia. Pankit torjuvat tällaisia petoksia suhteellisen suoraviivaisella ja pistemäisellä valvonnalla, joka keskittyy aina yksittäiseen transaktiokanavaan.[195]

Identiteettivarkauksiin perustuvat petokset ovat kuitenkin yleistyneet 2010-luvulla huijareiden kehittäessä uusia sovelluksia tavallisen ja synteettisen datan hyödyntämiseen. Henkilötietojen tietosuojan ja tietoturvan kehittämisen merkitys organisaatioissa kasvaakin jatkuvasti tietoverkkopohjaisten petosten muuttuessa kunnianhimoisemmiksi ja laajuudeltaan yhä suuremmiksi.[196] Yritysten sisäinen riskienhallinta ja petosten torjunta on käytän-

[192] PwC 2022, s. 3.
[193] Vuonna 2022 petoksentekijöistä 43 % olivat organisaatioiden ulkopuolisia ja 31 % organisaatioiden sisäpuolisia. Loput 26 % petoksista toteutettiin organisaatioiden sisäisten ja ulkoisten toimijoiden yhteistyönä. Ks. tarkemmin PwC 2022, s. 8.
[194] Ks. Hasham – Joshi – Mikkelsen 2019.
[195] Hasham – Joshi – Mikkelsen 2019.
[196] Ibid.

nössä myös kokonaan käyttäjätietojen varassa. Tästä syystä yritysten tulee huolehtia myös yleisen tietosuoja-asetuksen noudattamisesta käyttäjätietojen käsittelyn suhteen.

Eräs huomio elinkeinonharjoittajien petostorjunnasta on se, että asiakkaat ottavat enää harvoin yhteyttä pankin henkilökuntaan digitaalisessa palveluympäristössä, vaan kaikki vuorovaikutus tapahtuu lähes kokonaan digitaalisten kanavien kautta, niin kutsutusta digitaalisesta luottamuksesta on nopeasti tullut merkittävä asiakaskokemusten erottelija. Verkkopetosten tekijät käyttävät yritysten asiakaskanavia hyväkseen petosten tekemisessä, joten yritysten petostorjunnan kannalta asiakkaiden luotettavuudesta varmistuminen on keskeistä. Integroimalla erillisten toimintojen tiedot sekä sisäisistä että ulkoisista lähteistä organisaatiot voivat parantaa asiakkaiden tunnistamista ja todentamista.[197]

Johtavissa laitoksissa pyritään tällä hetkellä yhdistämään talousrikollisuutta, petoksia ja tietoverkkorikollisuutta koskevat rikostorjuntamenetelmät. Riskienhallintatoimintoja ja sisäistä riskien sääntelyä kehitetään myös. Vaikka rahanpesun torjuntaa käsitellään vielä toistaiseksi pääasiassa sääntelykysymyksenä, se nähdään organisaatioissa seuraavana viranomaisten ja finanssialan toimijoiden välisenä integraation tasona. Erityisen tärkeää organisaatioiden petosten ehkäisyssä on selkeyttää riskienhallintatoimien luonne siten, että päällekkäiset toiminnot yhdistetään kokonaisuudeksi.[198]

Useimpien finanssialan toimijoiden riskienhallinnallisena lähtökohtana on aiemmin ollut yhteistyömalli, jossa on tehty yhteistyötä eri riskienhallintaosastojen välillä. Monet instituutiot työskentelevät nyt siiloutuneista rakenteista kohti mallia, jossa tietoturvallisuus, tavanomaiset petokset ja tietoverkkoja hyödyntävät petokset ovat osittain integroitu yhteiseksi lajikseen. Jokainen riskienhallintayksikkö säilyttää riippumattomuutensa, mutta toimii johdonmukaisesti osana laajempaa modernia petostentorjuntakontekstia. Organisaatioiden sisäisen rikostorjunnan kannalta on siten tärkeää keskittää organisaation rakennetta. Esimerkiksi siiloutunut datan säilytys on yksi suurimmista verkkopetoksiin johtavista tekijöistä, joten datajärjestelmien keskittäminen on merkittävä keino ennalta ehkäistä verkkopetoksia.[199]

Kuten huomataan, liike-elämässä toimivien organisaatioiden riskienhallinta on murrostilassa talousrikollisesti orientoituneen verkkoavusteisen petosrikollisuuden vuoksi. Talousrikollisuuteen ja tietoverkkoihin liittyviin riskeihin liittyy kolmenlaisia vastatoimia: asiak-

[197] PwC 2020, s. 12.
[198] Hasham – Joshi – Mikkelsen 2019.
[199] Ks. PwC 2022, s. 12.

kaan tunnistaminen ja todentaminen, transaktio- ja käyttäytymispoikkeamien seuranta ja havaitseminen sekä tietoturvasta ja organisaation henkilöstön henkilötietojen suojasta huolehtiminen. Näiden vastatoimien kehittäminen on olennaista yritysten sisäisen rikostorjunnan suhteen. Lisäksi organisaatioiden riskienhallinnallisen integraation avulla datan, automaation ja analytiikan petostentorjuntapotentiaali voidaan toteuttaa täydellisemmin. Kaiken kaikkiaan kuvatun uudenlaisen toimintamallin tavoitteena on kokonaisvaltainen näkökulma talousrikollisuuden kehittyvästä toimintaympäristöstä.

5.3 Tietoverkkojen universaalit vaikutukset rikollisuuteen

Verkkoavusteisia petoksia ei tule tarkastella yksittäisenä rikollisena ilmiönä, vaan näiden rikosten juridinen olemus avautuu paremmin tutkittaessa verkkopetoksia osana laajempaa rikosoikeudellista muutosta. Tietoverkot ovat paitsi tarjonneet rikollisille uusia työkaluja, myös muuttaneet perinteisen rikollisuuden toimintaa. Verkkopetosten eri muotoja tarkastelemalla on mahdollista löytää joukko tekijöitä, jotka ovat selkeästi ominaisia nimenomaan tietoverkkoja hyödyntävälle rikollisuudelle. Globaalista digitalisaatiosta johtuen tietoverkkojen vaikutuksia rikollisuuteen voidaan luonnehtia universaaleiksi. Tässä tutkimuksessa nämä tietoverkkojen universaalit vaikutukset jäsennetään seuraaviksi:

1. Rikollisen toimintakentän kansainvälistyminen. Rikolliset voivat kohdistaa toimintansa sellaisiin oikeusjärjestelmiin, joissa sääntelyn vajavaisuus tai muu suotuisuus esimerkiksi kryptovaluuttakaupan suhteen mahdollistaa optimaalisen rikollisen toiminnan.[200]
2. Kiinnijäämisen epätodennäköisyys. Kansainvälisestä toimintaympäristöstä johtuva poliisitutkinnan hankaluus vähentää rikollisten riskiä jäädä kiinni. Lisäksi taloudellisilta vaikutuksiltaan pienistä verkkopetoksista ei useimmiten vaivauduta ilmoittamaan poliisille.
3. Piilorikollisuuden lisääntyminen. Verkkopetosten suuri määrä ja yksityisten tahojen rikosraportoinnin haluttomuus nostavat rikosten todellista, mutta todennäköisesti suurelta osin piiloon jäävää kokonaismäärää. Lisäksi tietoverkkorikoksia voi olla hyvin vaikeaa havaita.
4. Rikosten määrällinen lisääntyminen ja rikoskohteiden virtuaalinen loputtomuus. Maailman globalisoituessa ja digitalisoituessa tietoverkkojen avulla rikollisille tar-

[200] Europol IOCTA 2021, s. 32.

joutuu tilaisuus kohdistaa toimintansa minne tahansa maailmassa ja melkeinpä mihin tahoon tahansa, kunhan kohteella on jokin liittymä tietoverkkoon.

5. Tiedon liikkuvuuden lisääntyminen. Globaalista ja digitaalisesti toimintaympäristöstä johtuen informaation saatavuus on räjähtänyt. Tätä voidaan käyttää hyväksi tiedon jakamiseen, petosten markkinointiin sekä kaupantekoon. Esimerkiksi pimeän verkon eli darknetin[201] alustoilla voi myydä petoksella hankittuja henkilö- ja maksuvälinetietoja tai muutoin jakaa laitonta dataa kuten paljon julkisessa diskurssissa esillä ollutta lasten seksuaalista hyväksikäyttöä sisältävää materiaalia.[202]
6. Tietoverkkojen mahdollistama anonymiteetti. Pimeässä verkossa tapahtuvaa rikollista toimintaa on hyvin haastavaa valvoa tai säännellä. Lisäksi kryptovaluuttojen käyttöä on haastavaa seurata tai säännellä, minkä vuoksi esimerkiksi rahanpesu verkossa on aiempaa helpompaa.
7. Rikollisten ammattimaisuuden ja järjestäytymisen lisääntyminen. Tietoverkot ovat saaneet rikolliset toimimaan organisoidummin sekä tukeneet jo olemassa olevien rikollisjärjestöjen toimintaa. Paikallisten puhelinkeskusten perustaminen sekä johtaminen eri kielisten henkilöiden huijaamiseksi, laillisen näköisten verkkosivustojen luominen, etäkäyttöohjelmistojen käyttäminen uhrien tilien kaappaamiseksi ja monimutkaisten rahamuuliverkostojen käyttäminen rahanpesua varten ovat esimerkkejä rikollisten keinojen ammattimaistumisesta.[203]

Listaus perustuu tutkimuksen ja tutkimusaineiston perusteella tehtyihin havaintoihin verkkoavusteisten rikosten yhtäläisyyksistä, mutta samalla myös niiden eroista perinteiseen rikollisuuteen verrattuna. Näin ollen listausta ei tule tulkita tyhjentäväksi.

5.4 Verkkoavusteisten petosrikosten torjunta

5.4.1 Rikostorjunnan nykytila

Verkkopetosten ja muiden kyberrikosten sääntelyn sekä tietoverkkojen universaalien vaikutusten kautta voidaan lopulta tarkastella rikostorjunnan nykytasoa verkkopetosten suhteen. Tarkastelun tukena käytetään liitteestä 1 löytyvää haastattelututkimusta. Rikostorjunnan nykytilaa arvioitaessa on pidettävä mielessä verkkopetosten suuri piiloon jäävä osuus.

[201] Käsitteestä tarkemmin ks. Biddle – England – Peinado – Willman 2002, s. 155–176 ja Wood 2010, s. 16–19.
[202] Europol IOCTA 2021, s. 25–26.
[203] Kyberturvallisuuskeskus 2020, s. 4 ja Europol IOCTA 2021, s. 32.

Suomessa tehdyt nettipetokset saadaan tutkinnassa pääosin selvitettyä. Kuitenkin ulkomailta käsin tehtävien rikosten, joiden seuraukset ilmenevät Suomessa, tutkinta on huomattavan haasteellista.[204] Eurooppalainen yhteistyö EU:n jäsenvaltioiden ja EU:n organisaatioiden välillä osaltaan tukee silti osaltaan rajat ylittävien rikosten selvittämistä ja torjuntaa. Esimerkiksi vuonna 2015 keskusrikospoliisi alkoi tutkia laajaa kansainvälistä petosrikoskokonaisuutta, jossa satojen suomalaisten yksityishenkilöiden ja pienyritysten pankkitileiltä onnistuttiin vuosina 2011–2013 siirtämään rahaa uhrien tietokoneet saastuttaneen ja pankkitunnukset kalastelleen haittaohjelman avulla. Tutkintaa tehtiin yhteisessä kansainvälisessä tutkintaryhmässä[205] muun muassa Itävallan, Belgian, Hollannin ja Norjan lainvalvontaviranomaisten kanssa lähes kolmen vuoden ajan. Mukana rikoskokonaisuuden tutkinnassa olivat lisäksi Eurojust ja Europol.

Sisäministeriön vuonna 2017 tuottamassa tietoverkkorikollisuuden torjuntaa koskevassa selvityksessä on käyty läpi tietoverkkorikollisuuden ilmenemistä ja rikostorjuntaan vaikuttavia seikkoja Suomessa.[206] Nämä tulokset heijastavat rikostorjunnan tilaa myös verkkopetosten osalta. Rikostorjunnan vahvuuksiksi listattiin selvityksessä seuraavat tekijät:

1. Lainsäädäntöön lisätyt uudet pakkokeinot. Tässä yhteydessä muistutetaan kuitenkin puutteiden jatkuvasta läsnäolosta.
2. Tietoverkkorikostutkijoiden motivoituneisuus ja ammattitaitoisuus heidän vähäisestä määrästänsä huolimatta.
3. Tietoverkkorikostutkijoiden hyvä verkostoituneisuus kansainvälisesti ja kansallisesti, sekä hyvin toimiva yhteistyö kyberturvallisuuskeskuksen ja finanssisektorin kanssa.
4. Suomen kansallisen kyberturvallisuusstrategian toimeenpanoehdotukset, jotka tukevat tietoverkkorikostorjunnan kehittämistä.[207]
5. Keskusrikospoliisin alaisuuteen perustettu poliisin kyberrikostorjuntakeskus ja sinne panostetut resurssit.
6. Poliisin myönteinen julkisuuskuva ja kansalaisten kokema luottamus poliisia kohtaan.

[204] Sisäministeriö 2017, s. 23.
[205] Eng. joint investigation team.
[206] Sisäministeriö 2017, s. 31.
[207] Vuonna 2019 annetussa valtioneuvoston periaatepäätöksessä Suomen kansalliseksi kyberturvallisuusstrategiaksi jäsennetään kansainvälisen yhteistyön kehittäminen, kyberturvallisuuden johtamisen, suunnittelun ja varautumisen parempi koordinaatio sekä kyberturvallisuuden osaamisen kehittäminen. Ks. turvallisuuskomitea 2019.

Rikostorjunnan heikkouksiksi puolestaan listattiin:

1. Lainsäädännön puutteet liittyen tiedon tallentamiseen ja käsittelyyn. Näistä puutteista mainittiin uhkien paljastaminen sekä ennaltaehkäisy.
2. Resurssien epätasainen jakaantuminen ja toiminnan kehittämiseen tarvittavien määrärahojen puute.
3. Osaamisvaje erityisesti tietoverkkorikostutkijoiden ulkopuolisilla tahoilla sekä osin myös ydinryhmässä.
4. Tietoteknisen tutkinnan epäyhtenäiset työprosessit ja raportointikäytännöt.
5. Tietoteknisen tutkinnan epäyhtenäiset työvälineet, kuten palvelin- ja verkkoympäristö.
6. Tiedonhankinta tietoverkoista. Tähän katsottiin vaikuttavan lainsäädännön haasteet, osaamishaasteet sekä organisoinnin ja välineiden epäyhtenäisyys.
7. Verkkoa hyödyntävien rikosten esim. petosrikosten käsittelyn hajanaisuus.
8. Syyttäjien erikoistumisen hajanaisuus ja liian suuri työkuorma.
9. Oikeusapuprosessin hitaus ja kansainvälisen järjestäytyneen tietoverkkorikollisuuden torjunnan haasteet kansallisen oikeudenkäytön osalta.

Sisäministeriön selvityksestä on ensinnäkin todettava, että vaikka osa heikkouksista on poliisin sisäisiä organisatorisia ongelmia, niin listatut rikostorjunnan haasteet ovat yleisesti ottaen linjassa tässä tutkimuksessa tehtyjen havaintojen ja päätelmien kanssa. Lainsäädäntö EU:n tasolla sääntely tietojen säilyttämisen suhteen on sirpaleinen kokonaisuus, joka ei tarjoa selkeää mallia tietojen oikeanlaisesta ja oikeudellisesti hyväksyttävästä säilytyksestä. EUT:n oikeuskäytäntö ei ole myöskään selkiyttänyt tilannetta, vaan pikemmin sekavoittanut sitä. Myöskään sähköisen todistusaineiston rajat ylittävä hankkiminen ei ole oikeudellisesti selkeää, vaan sääntely on jätetty väljäksi. EU on lainsäädännön sijaan keskittynyt enemmän uusien viranomaisten perustamiseen ja viranomaisyhteistyön kehittämiseen. Poliisin resurssien puute on myös sangen selvästi todettavissa julkisen diskurssin perusteella sekä jo verkkoavusteisten petosten valtavasta määrästä johtuen.[208] Kaikkien verkkopetosten tutkintaan tarvittaisiin valtavat resurssit. Resurssien puute vaikuttanee myös suoraan poliisin osaamisvajeeseen ja syyttäjien työmäärään. Tietoverkkoympäristö, verkkopetosten moninaisuus, oikeusprosessin hitaus sekä järjestäytyneen rikollisuuden aiheuttamat haasteet on myös tunnistettu tutkimuksen puitteissa rikostorjunnan ongelmakohdiksi samoin kuin sisäministeriön listauksessa.

[208] Esimerkiksi Europol ei ole priorisoinut verkkopetosten tutkintaa. Ks. Helsingin sanomat 2020.

Selvityksessä listatut vahvuudet eivät vakuuta täysivaltaisesti. Uusien pakkokeinojen osalta muistutetaan lainsäädännön puutteista, ja poliisin osakseen saama luottamus ei ole kuitenkaan saanut kansalaisia raportoimaan verkkopetoksista ainakaan tilastojen ja viranomaisasiakirjojen valossa. Toisaalta Euroopan unioninkin tasolla panostettu viranomaistoiminta ja -yhteistyö pitänevät hyvin paikkansa. Nämä ovat listattu vahvuuksiksi useista näkökulmista.

Selvityksessä on myös listattu tietoverkkorikostutkinnan uhkia ja mahdollisuuksia.[209] Uhiksi nimettiin muun muassa poliisin resurssien jatkuva heikkeneminen, tutkinnan vaikeutuminen uusien teknologisten syiden kuten kryptovaluuttojen ja pimeän verkon käytön vuoksi sekä järjestäytyneiden tietoverkkorikollisten foorumishoppailu. Sittemmin poliisin resurssit eivät ainakaan ole merkittävästi lisääntyneet ja tietoverkkorikosten ja verkkopetosten määrä on vain noussut, mikä aiheuttaa rikostutkinnalle ja -torjunnalle lisäkuormitusta. Lisäksi kryptovaluuttojen käyttö esimerkiksi rahanpesussa on lisääntynyt huomattavasti, tietoverkkorikolliset ovat järjestäytyneet yhä enemmän ja petostentekijät ovat jatkaneet rikosten tekemiselle lainsäädännöllisesti suotuisten maiden suosimista.[210] Merkittävät uhat ovat siis osittain realisoituneet tai vähintään pysyneet samoina. Toisaalta tietoverkkorikostutkinnan mahdollisuuksiksi listatut yritysten ja viranomaisten välinen yhteistyö sekä koulutus verkkopetoksista näyttäytyvät edelleen hyvinä rikostorjuntaa tukevina seikkoina.

Selvityksen julkaisemisen jälkeen verkkopetosten määrä on vain kasvanut ja petokset muuttuneet monimutkaisemmiksi. Samalla rikolliset ovat muuttuneet entistä ammattimaisemmiksi. Vuonna 2020 alkanut ja tutkimuksen kirjoitushetkellä edelleen jatkuva Covid-19-pandemia on myös osaltaan lisännyt verkkoavusteisten petosten määrää rikollisille menetettyjen kokonaissummien noustessa vuosi vuodelta.[211] EU:n tasolla uutta relevanttia oikeuskäytäntöä tai lainsäädännöllistä uudistusta ei ole vielä tullut. Budapestin yleissopimuksen toisen lisäpöytäkirjan ratifiointiin jäsenvaltiot oikeuttava päätös on ollut merkittävin EU:n tasolla tapahtunut verkkopetoksiin liittyvä oikeudellinen kehitys vuoden 2017 jälkeen, jolloin käsitelty sisäministeriön selvitys julkaistiin. Budapestin yleissopimuksen toinen lisäpöytäkirja koskee kansainvälisen viranomaisyhteistyön tiivistämistä ja sähköisten todisteiden luovuttamista. Viranomaisyhteistyötä voidaan toki aina parantaa, mutta tätä on kehitetty jo pitkään ja viranomaisyhteistyön voidaankin sanoa olevan jo hyvällä tasolla.

[209] Sisäministeriö 2017, s. 31.
[210] Europol IOCTA 2021, s. 32.
[211] Ks. tilastokeskus 2020a ja Europol IOCTA 2021, s. 29–33.

Sähköisten todisteiden jakamisesta rikostutkintaa varten eri valtioiden viranomaisten välillä ei puolestaan todeta lisäpöytäkirjassa harmillisesti mitään erityistä. Pöytäkirjassa tyydytään sopimaan todisteiden luovuttamisen helpottamisesta ja jakamisen kehittämisestä sopimuksen ratifioineiden valtioiden välillä. Väljäksi jätetyt sopimuskohdat tekevät sopimuksen ratifioinnista tietenkin helpompaa useammille valtioille, mutta samalla lisäpöytäkirja ei tarjoa mitään uutta oikeudellista ratkaisua sähköisten todisteiden jakamista koskevaan ongelmaan. Näin ollen rikostorjunnan tila verkkoavusteisten petosten suhteen ei vaikuta erityisen valoisalta.

5.4.2 Haastattelututkimuksen vastaukset

Rikostorjunnan tilaan voidaan hakea johtoa tätä tutkimusta varten toimitetusta haastattelututkimuksesta.[212] Helsingin poliisilaitoksen rikostutkintayksikössä talous- ja petosrikoksien kanssa työskentelevä rikoskomisario Teemu Haapalan havainnot ovat paitsi mielenkiintoisa, myös linjassa tutkimuksen kanssa:

> Haastattelukysymys 1. *Millä tasolla taloudellisesti motivoituneiden ja verkkoa hyväksi käyttävien petosrikosten torjunta ja selvittäminen on? Onko tällaisilla rikoksilla jotain erityisiä ongelmakohtia?*
>
> ”Yleisesti totean tietoverkkoa hyväksi käyttävien petosrikosten torjunnan olevan tyydyttävällä tasolla, joskin tässä on havaintojeni mukaan paljonkin poliisilaitoskohtaisia eroja. Niissä poliisilaitoksissa ja valtakunnallisissa poliisiyksiköissä, joissa tietoverkkoavusteisia (TVA) petoksia selvitetään omassa rikosalaan erikoistuneessa tutkintaryhmässä sekä osaaminen että esitutkintaan käytettävät resurssit ovat parempia, kuin poliisilaitoksissa, joissa tva-petoksia tutkitaan niin sanotuissa yleisryhmissä, joiden toimenkuvaan kuuluu kaikkien rikoslakirikosten esitutkinta.
>
> Luokiteltavien ”nettipetosten” osalta rikosten lukumäärä kasvaa jatkuvasti. Vuonna 2020 poliisissa on valtakunnallisesti tutkittu 20 603 tva-petosta ja vuonna 2021 näitä tekoja oli jo 26 696. Oletan, että vuonna 2022 rikoksia on edelleen edeltävää vuotta enemmän. Erityisseurattavien tva-petosten rikoshyöty Suomessa on poliisin tietojen mukaan vuonna 2021 ollut noin 33 miljoonaa euroa, joten näiden rikosten osalta voidaan jo puhua yhteiskunnallisestikin merkittävästä vahingosta, etenkin kun vahinko kohdistuu suuressa määrin yksittäisiin kansalaisiin tai pienyrityksiin.

[212] Ks. liite 1.

Keskeistä tva-petosrikosten torjunnassa on poliisilla käytettävissä olevien pakkokeinojen ja poliisilain mukaisten tiedonsaantioikeuksien hallinta. Pakkokeinolain ja poliisilain soveltamiseksi tehokkaasti tulee lisäksi olla osaamista eri tietojärjestelmien käytöstä ja avointen lähteiden tarjoamista mahdollisuuksista esitutkinnan ja rikostiedustelun välineenä. Torjunnan kannalta merkityksellistä on myös seurata ja ymmärtää erilaisia ilmiöitä, joita tva-petosrikoksiin liittyy. Oman näkemykseni mukaan poliisissa ja etenkin Helsingin poliisilaitoksessa on hyvät edellytykset suorittaa esitutkintaa tva-petoksiin liittyen. Tutkijat, joiden toimenkuvaan näiden rikosten esitutkinta kuuluu, osaavat käyttää eri tietojärjestelmiä hyvinkin monipuolisesti sekä soveltaa rikosten tutkintaan liittyvää lainsäädäntöä. Helsingin poliisilaitoksessa työskentelevillä tutkijoilla on myös erittäin hyvät valmiudet analysoida sidosryhmien tuottamaa aineistoa ja selvittää rikoksia aineiston avulla. Tämän mahdollistaa käytännössä se, että tutkijoiden ei tarvitse tutkia muita rikoslakirikoksia.

Yleisesti voidaan todeta, että uudet ilmiöt ja tekotavat tulevat poliisin tietoon ilmoitettujen rikosten kautta, jonka jälkeen poliisin tutkintatoimenpiteitä kehitetään vastaamaan mahdollisesti uuteen tekotapaan. Tva-petosrikosten torjunta edellyttää tiivistä yhteistyötä muun muassa teleoperaattoreiden ja pankkien sekä rahoitusyhtiöiden kanssa. Kaiken tva-petosrikollisuuden ennalta estäminen on käytännössä mahdotonta niin kauan, kun ihmisillä on vapaa pääsy tietoverkkoihin ja mahdollisuus hoitaa esimerkiksi omia pankkiasiointejaan sähköisesti, mutta muun muassa EU:n toisen maksupalveludirektiivin (PSD2) myötä tietyt tva-petosrikokset ovat romahtaneet. Rikolliset onnistuvat kuitenkin kehittämään jatkuvasti uusia tapoja tehdä tva-petoksia ja hyödyntämään tietoverkkoihin liittyviä haavoittuvuuksia.

Tietoturvallisuus yleisesti on keskeisin ongelma, mikä tva-petoksiin liittyy. Tässä yhteydessä vakavin tietoturvallisuuteen liittyvä aukko on loppukäyttäjissä eli yleensä rikosten asianomistajissa, jotka eivät suojaa omaa toimintaansa tietoverkoissa riittävästi tai sitten itse aktiivisesti omalla toiminnallaan mahdollistavat rikosten tekemisen.

Toisena ongelmakohtana koko tietoverkkorikollisuuteen liittyen on tietoverkkojen globaalius ja mahdollisuus tehdä rikoksia kansainvälisesti. Ulkomaille siirtyvien varojen seuranta on, jos ei mahdotonta, niin hyvin vaikeaa, ja näitä saadaan hyvin harvoin palautettua rikoksen asianomistajille, vaikka rikoksella saatuja varoja pystyttäisiinkin seuraamaan tiettyyn pisteeseen saakka.

Kolmantena ongelmakohtana näen henkilökohtaisesti virtuaalivaluuttojen kehittymisen sekä niillä suoritettavien siirtojen yleistymisen. Virtuaalivaluuttoihin liittyen

osaaminen poliisissa on rajattua ja virtuaalivaluuttoihin kohdennettavien pakkokeinojen osalta vieläkin rajatumpaa.”

Haastattelukysymys 2. *Pitäisikö lainsäädäntöä kehittää vastaamaan rikostorjunnan ja rikosten selvittämisen tarpeita verkkopetosten suhteen? Jos pitäisi, niin miten?*

”Lainsäädäntöä on uudistettu ja esimerkiksi valmisteilla olevan pakkokeinolain uudistusten myötä poliisin mahdollisuudet puuttua rikollisuuteen ylipäätään ovat hyvällä tasolla. Pakkokeinojen käyttämiseen liittyvän kohtuusperiaatteen mukaisesti pakkokeinoja tulee käyttää ensisijaisesti vakavammissa rikoksissa ja lievemmissä tekomuodoissa pakkokeinojen käyttäminen laajalti ei yleensä ole mahdollista.

Tva-petosrikoksiin keskeisesti liittyvää lainsäädäntöä on pakkokeinolain 10 luvun 6 § televalvonta ja sen edellytykset. Pakkokeinolaki mahdollistaa televalvonnan käyttämisen petosrikoksissa lieviä tekomuotoja lukuun ottamatta silloin kun teko on tehty teleosoitetta tai telepäätelaitetta käyttäen. Tätä soveltamisalaa ei ole mielestäni tarpeen laajentaa koskemaan lieviä tekomuotoja, vaikka se tarkoittaakin sitä, että lievissä tva-petoksissa tekijää ei aina saada selvitettyä. Poliisilla ei tällä hetkellä ole myöskään riittäviä resursseja televalvonnan suorittamiseksi lievien rikosten osalta, vaikka lainsäädäntö sen mahdollistaisi.

Toinen keskeisesti tva-petosrikosten selvittämiseen liittyvä lainsäädäntö löytyy laista sähköisen viestinnän palveluista (2014/917), jonka 19 luvussa säädetään viranomaistoimintaan liittyvistä tiedoista ja 157 § säädetään teleyritysten tietojen säilytysvelvollisuudesta. Tällä hetkellä lainsäädäntö edellyttää teleyrityksiä säilyttämään muun muassa internetyhteyspalveluun liittyviä IP-tietoja 9 kuukautta viestintätapahtuman ajankohdasta lukien. Näitä tietoja poliisi saa käyttöönsä niissä rikoksissa, joissa on PKL 10:6 mukaiset edellytykset. Kun ottaa huomioon sen, miten tva-petosrikokset tulevat poliisin tietoon, niin säädetty 9 kk:n säilytysvelvollisuus ei aina riitä. Usein asianomistajat tulevat tietoiseksi heihin kohdistuneesta rikoksesta pitkänkin ajan kuluttua teon tapahtuma-ajankohdasta esimerkiksi perintäyhtiöiden lähettämien perintäkirjeiden kautta ja ilmoittavat vasta tällöin rikoksesta poliisille. Kun teosta on kulunut aikaa, ei poliisilla välttämättä ole enää mahdollisuutta saada tarvittavaa näyttöä rikoksesta ja syytteen tueksi teoissa, joista on jo ilmoitushetkellä kulunut yli 9 kk. Lievemmissä tekomuodoissa poliisilla on mahdollisuus saada teleyrityksiltä IP-tietoja 1–3 kk:n ajalta teleyrityksestä riippuen. Käytännössä tämä tarkoittaa sitä, että lievemmissä tekomuodoissa poliisilla ei ole edellytyksiä suorittaa esitutkintaa saatavilla olevan lisäselvityksen puutteen vuoksi ja esitutkinnat on tästä

> syystä keskeytettävä. Mikäli lainsäädäntöä tarkastellaan teleyritysten säilytysvelvollisuuden osalta, niin tämä tva-petosrikosten selvittämiseen liittyvä seikka tulisi huomioida lainvalmistelun yhteydessä."

Tämä asiantuntijalausunto heijastelee tutkimuksen tuloksia ja korostamia verkkopetoksiin liittyviä ongelmakohtia. Haastatteluvastausten ja muun tutkimuksessa esitetyn perusteella merkittävimmiksi verkkoavusteisten petosten rikostorjunnan piirteiksi voidaan nimetä kolme tekijää. Ensinnäkin rikostorjuntaan osoitetut resurssit ovat liian pieniä suhteessa verkkoavusteisten petosten alati kasvavaan määrään. Toiseksi verkkoavusteisten petosten kansainvälinen toimintaympäristö tekee rikosten tutkinnasta ja torjunnasta hyvin haastavaa, ja rikosten kokonaisvaltaisen torjunnan näkökulmasta jopa ylitsepääsemätöntä. Kolmanneksi sähköisten todisteiden kerääminen on haastavaa, osittain jopa mahdotonta.

Näitä piirteitä tarkastellen voidaan todeta, että rikostorjunnan resurssien pulaan voidaan puuttua, muttei oikeudellisesti. Rikostorjunnan tilanteen kohentaminen tältä osin vaatii kriminaalipoliittista päätöksentekoa. Verkkoavusteisten petosten kansainvälisyyden osalta rikostorjunnan kohentamisen käytännössä ainoaksi keinoksi jää kansainvälisen viranomaisyhteistyön parantaminen, joka voi tapahtua niin organisatorisesti kuin oikeudellisen viitekehyksen kehittämisen keinoinkin. Mitä sähköisten todisteiden keräämiseen tulee rikostorjunnan nykytilan kohentamisen osalta, todisteiden säilytysaikoihin voidaan puuttua lainsäädännöllisin keinoin niin kansallisesti kuin Euroopan unioninkin tasolla. Pohdintaa summaten verkkoavusteisten petosten rikostorjunnan tilan voidaan todeta olevan murrostilassa teknologisen kehityksen ja EU:n tasolla tapahtuvan lainsäädännöllisen viitekehyksen suhteen.

6 Johtopäätökset

Verkkoavusteiset petosrikokset ovat oikeustieteellisenä tutkimuskohteena mielenkiintoinen rikollisuudenlaji. Verkkoavusteisissa petoksissa yhdistyvät talousrikosoikeus, tietoverkkoihin ja datan käyttöön liittyvä sääntely sekä kansainvälinen rikosoikeus. Samalla verkkoavusteiset petokset ovat nopeimmin kasvava varallisuusrikosten muoto, ja erilaisia verkkoavusteisia petoksia kehitetään jatkuvasti lisää. Rikostyypillä on myös vahva liittymä teknologiseen kehityskulkuun, joten verkkopetosten tutkiminen on erittäin ajankohtaista – ja tulee olemaan jatkossakin.

Tutkimuksessa pyrittiin selvittämään, millaisia erilaisia verkkopetoksia on olemassa, mitkä ovat tietoverkkojen yleisluontoiset vaikutukset rikollisuuteen ja millainen on verkkoavusteisten petosten rikostorjunnan nykytila. Kaikkiin näihin kysymyksiin pystyttiin muodostamaan jäsennelty vastaus tutkimuksen puitteissa. Jäljelle jää vain tutkimuskysymys: miten tietoverkot vaikuttavat petosrikosten sääntelyn kehitystarpeisiin?

Tutkielman lähtökohtana on petosten tarkastelu tietoverkkojen näkökulmasta. Maksuvälinepetokset ja siten esimerkiksi kryptovaluuttoja koskevat liansäädännölliset kysymykset ovat rajattu ulos tutkielman pääasiallisesta katsannosta. Toistaiseksi rikoslain 36 luvun 1–3 pykälät ovat olleet tunnusmerkistöinä riittäviä petosrikosten arviointiin, vaikka petos olisikin tapahtunut tietoverkkoja hyväksikäyttämällä ja tietoverkkojen mahdollistamin keinoin. Tässä mielessä voidaan todeta, että verkkoavusteisia petoksia ei suoranaisesti tarvitse alleviivata esimerkiksi erillisen rikostunnusmerkistön säätämisen keinoin. Tämä ei ratkaisisi mitään olemassa olevaa ongelmaa. Sanottu ei kuitenkaan merkitse, etteikö verkkoavusteisten petosten oikeudelliseen arviointiin liittyisi rikoslajille ominaisia ja muista petoksista erillisiä piirteitä.

Tutkimuksessa on jäsennelty tietoverkkojen vaikutusta rikollisuuteen yleisesti sekä petoksiin erityisesti. Johtopäätöksenä voidaan todeta, että verkkoavusteisia petoksia ei tule tarkastella puhtaan normatiivisena ilmiönä, vaan sillä on myös talousrikosoikeudellinen ja yhteiskunnallisesti merkittävä ulottuvuus. Näin ollen tietoverkkojen aiheuttamia sääntelytarpeita tulee tarkastella verkkoavusteisten petosten yhteiskunnallisten vaikutusten kautta, jotka ovat todettu huomattaviksi. Koska verkkopetosten määrät ja näille rikoksille menetettävät summat kasvavat jatkuvasti, korostuu verkkopetosten rikostorjunnan merkitys. Tämä tarkoittaa verkkopetosten sääntelytarpeiden arviointia rikostorjunnan lähtökohdista. Näin ollen mainittu arvio kokonaisuudessaan muodostaa vastauksen tutkimuskysymykseen.

Verkkoavusteisten petosten rikostorjuntaa määritteleviksi ja perustavanlaatuisiksi ominaispiirteiksi voidaan tunnistaa ensinnäkin poliisin ja poliisin toimintaa tukevien muiden viranomaisten liian vähäiset resurssit verkkopetosten määrään suhteutettuna. Tähän ratkaisuna ei ole sääntelyn muuttaminen, vaan ratkaisuksi voidaan esittää kriminaalipoliittisia toimia. Kriminaalipoliittista päätöksenteon suuntaamista verkkopetostorjunnan resurssien lisäämistä kohti tukee puolestaan se, että verkkoavusteiset petokset voidaan mieltää talousrikoksiksi. Talousrikoksen käsite voidaan nähdä kriminaalipolitiikan työkaluna, ja tässä

mielessä sen hyödyntäminen argumentoinnin tukena olisi paitsi perusteltua, myös erittäin tarpeellista.

Toiseksi verkkopetosten rikostorjuntaan liittyväksi ominaispiirteeksi määriteltiin tietoverkkojen käytöstä johtuva kansainvälinen toimintaympäristö. Tämä kansainvälinen ulottuvuus aiheuttaa haasteita rikostorjunnalle. Näitä haasteita ei voida sinänsä poistaa, mutta niiden kohtaamisesta voidaan tehdä helpompaa järjestämällä viranomaisyhteistyö niin kansallisella, EU:n sisäisellä kuin kansainväliselläkin tasolla mahdollisimman saumattomaksi ja toimivaksi kokonaisuudeksi. Tältä osin sekä Suomessa että EU:ssa on jo prosesseja käynnissä. Tutkimuksen valossa näiden prosessien joustava tukeminen on tärkeää, eikä uusien organisatoristen keinojen käyttöä viranomaisyhteistyön kehittämiseksi voida korostaa liikaa.

Kolmanneksi ja viimeiseksi verkkoavusteisten petosten rikostorjunnan ominaispiirteeksi jää sähköisten todisteiden säilyttämisestä muodostuvat haasteet. Tältä osin ongelma on puhtaasti oikeudellinen. Tutkielmassa on tullut esille, että niin Suomessa kuin EU:n tasollakin rikostutkinnan edellyttämien sähköisten todisteiden kuten metadatan säilytysajat ovat liian lyhyitä. Tutkielman tuloksena voidaan todeta, että näitä aikoja tulisi pidentää rikostorjunnan tarpeiden mukaisesti. EU:n oikeuskäytännön ja sääntelykehikon muodostama kokonaisuus on tältä osin epäselkeä, ja tilanteen mahdollinen kehittyminen on epävarmaa tai vähintäänkin hidasta. Lisäksi monet EU:n jäsenmaat käyttävät tietojen säilytyksen suhteen omia lakejaan EU-oikeuden tosiasiallisesti estämättä. Kansallisen lainsäädännön muuttaminen on nopeampi prosessi kuin EU-oikeuden tarjoamat vaihtoehdot. Näin ollen oikeusdogmaattisena kannanottona voidaan todeta, että sähköisen viestinnän palvelulain 157 § ei vastaa riittävästi sähköisen rikostorjunnan tarpeita. Ainoa pykälän mukainen datan säilytystä absoluuttisesti rajoittava tekijä on yleisen tietosuoja asetuksen 5 artikla, joka ei kuitenkaan aseta ylärajaa datan säilytyksellä ja koskee muutoinkin vain henkilötietoja sisältäviä sähköisiä todisteita yleensä rajat ylittävissä tietopyynnöissä. Merkittävin säilytysaikaa määrittävä tekijä on siten säilytysperusteen merkittävyys. Lainopillisena tulkintakannanottona todettakoon, että verkkopetoksiin ja yleisemmin tietoverkkorikollisuuteen perustuva datan säilytys on siinä määrin tärkeä ja korkealle arvostettava peruste, ettei henkilötietojen osalta yleisen tietosuoja-asetuksen 5 artikla tai muun datan osalta epäjohdonmukainen EU-oikeus aseta esteitä nykyisten kansallisten tietojensäilytysaikojen nostamiselle. Näin ollen todettakoon *de le ge ferenda,* että sähköisen viestinnän palvelulain 157 §:n toisessa momentissa lueteltujen teleyrityksille määriteltyjen datansäilytystilanteiden osalta tulisi kai-

kissa tapauksissa datan minimisäilytysaika säätää kahden vuoden mittaiseksi, joka on kansainvälisesti vakiintunut datansäilytysaika. Samalla pakkokeinolain 10 luvun 6 §:n toisen momentin asettamaa oikeutta saada teleyrityksiltä tietoa tulee tulkita väljemmin tai muuttaa siten, että myös lievemmistä petosrikoksista voidaan saada säilytettyjä tietoja vähintään kahden vuoden ajan. Kuten tutkimuksessa on todettu, verkkoavusteisten petosten viitekehyksessä myös pienistä, lieviksi petoksiksi arvioitavista teoista voi koostua merkittävä kokonaisuus, mistä syystä myös rikostutkinnan on oltava *de facto* mahdollista näiden tekojen oikeasuhtaiseksi käsittelyksi ja rikostorjunnan toimivuuden varmistamiseksi.