Virtuaalivaluutat rahanpesu- ja terrorismin rahoittamisrikoksissa sääntelyn ja rikosten ennaltaehkäisyn näkökulmasta

Lapin yliopisto
Oikeustieteiden tiedekunta
Maisteritutkielma
Talousrikosoikeus
Hanne-Mari Juntunen
2022

Lapin yliopisto, oikeustieteiden tiedekunta
Työn nimi: Virtuaalivaluutat rahanpesu- ja terrorismin rahoittamisrikoksissa sääntelyn ja rikosten ennaltaehkäisyn näkökulmasta
Tekijä: Hanne-Mari Juntunen
Oppiaine: Talousrikosoikeus
Työn laji: Pro gradu-tutkielma
Sivumäärä: XII + 80
Vuosi: 2022

Tiivistelmä:

Tämän tutkimuksen tarkoituksena oli selvittää, mitä haasteita ja muutostarpeita virtuaalivaluutoista aiheutuu rahanpesu- ja terrorismin rahoittamissääntelylle ja rikollisuuden estämis- ja ennaltaehkäisytoimille. Tutkimuksessa on erilaisten haasteiden kuvailun lisäksi keskitytty tarkastelemaan sitä, mihin suuntaan sääntelyä tulisi kehittää ja miten nykyinen lainsäädäntö ja keskeiset viranomaiset kykenevät vastaamaan tämän uuden teknologian luomiin haasteisiin.

Tutkimuksen metodina on käytetty lähtökohtaisesti lainoppia, mutta siinä on myös vahva oikeuspoliittinen painotus, johon siihen sisältyy lisäksi yhteiskunnallista ja oikeustaloustieteellistäkin pohdintaa. Aiheen uutuuden takia tutkimusongelmia pyritään lähestymään suhteellisen yleisestä näkökulmasta, minkä takia tiukan lainopillisessa tutkimusmetodissa pysyttäytyminen ei ole tarkoituksenmukaista.

Tutkielmassa selvitetään, mitä virtuaalivaluutat ja niiden taustalla oleva lohkoketjuteknologia ovat ja käydään läpi niihin liittyviä haasteita rahanpesun ja terrorismin rahoittamisen sääntelyn ja ennaltaehkäisyn näkökulmasta. Tutkielmassa esitellään valtiovarainministeriön laatiman kansallisen riskiarvion pohjalta niitä haavoittuvuuksia ja riskejä, joita virtuaalivaluutoista aiheutuu kansalliselle terrorismin rahoittamis- ja rahanpesusääntelylle ja alan toimijoille ja pyritään samalla löytämään näihin ongelmiin ratkaisuja. Kansallisen näkökulman lisäksi keskeisessä roolissa ovat EU:n ja FATF:n näkemykset rahanpesun ja terrorismin rahoittamisen sääntelyn riittävyydestä.

Tutkimuksen olennaisena havaintona oli sen ymmärtäminen, miten laaja virtuaalivaluuttoihin liittyvä ongelmakenttä on. Tutkimuskysymykseen vastaukseksi saatiin, että virtuaalivaluutat aiheuttavat haasteita lainsäädännölle niiden rajat ylittävän luonteen, anonymiteetin ja hajautuneen järjestelmän takia. Virtuaalivaluuttoja ja niiden avulla toteutettavaa rikollisuutta ei ole mahdollista säädellä pelkästään kansallisesti, vaan kansainväliset toimet ovat välttämättömiä. Virtuaalivaluuttojen sääntelyssä voidaan kansainvälisesti nähdä toisaalta jopa merkkejä ylilyönneistä ja tärkeänä johtopäätöksenä onkin myös se, että uutta teknologiaa säädellessä huomioon tulee ottaa myös esimerkiksi yleisten kriminalisointiperiaatteiden vaatimukset. Esiin nousi myös huomiot valvontaviranomaisten resurssipulasta ja kasvavasta tarpeesta löytää tehtävien hoitamiseksi ratkaisuja myös kehittyvästä teknologiasta ja esimerkiksi tekoälystä.

Avainsanat: virtuaalivaluutta, talousrikosoikeus, rikosoikeus, rahanpesu, terrorismin rahoittaminen, lohkoketjuteknologia, bitcoin, ethereum

Sisällys

Kirjallisuus

Albrecht, C., Duffin, K.M., Hawkins, S., Morales Rocha, V.M. The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control, 2019 Vol. 22 No. 2, pp. 210-216. 2019.

Andersen, Atso. Rahanpesun Estäminen. Helsinki: Alma Talent, 2020.

Berg, C., Davidson, S. and Potts, J. Capitalism after Satoshi:Blockchains, dehierarchicalisation, innovation policy, and the regulatory state", Journal of Entrepreneurship and Public Policy, Vol. 9 No. 2, pp. 152-164. 2020.

Brochado, Ana and Troilo, Michael Louis., "Initial coin offerings: an emergent research area", Digital Policy, Regulation and Governance, Vol. 23 No. 2, pp. 113-131. 2021.

Campbell-Verduyn, Malcolm. Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance. Abingdon, Oxon ; New York, NY: Routledge, 2018.

Casey, M., Crane, J., Gensler, G., Johnson, S. & Narula, N. The impact of blockchain technology on finance: A catalyst for change. Geneva Reports on the World Economy, 21. 2018.

Chohan, Usman W.: Assessing the Differences in Bitcoin and Other Cryptocurrency Legality across National Jurisdictions, University of New South Wales Business School, Sydney, 2017.

Diniz, R., Prince, D.d. and Maciel, L. Bubble detection in Bitcoin and Ethereum and its relationship with volatility regimes, Journal of Economic Studies, Vol. ahead-of-print No. ahead-of-print. 2022.

Freeman, M. & Ruehsen, M.. Terrorism financing methods: An overview. Perspectives on Terrorism, 7(4), 5–26, 2013.

Frisby, Dominic. Bitcoin: The Future of Money? Unbound 2014.

Garcia-Teruel, R.M., Legal challenges and opportunities of blockchain technology in the real estate sector, Journal of Property, Planning and Environmental Law, Vol. 12 No. 2, pp. 129-145. 2020.

Gigi ja Brand, Thomas. 21 Oppituntia: Mitä Olen Oppinut Pudottuani Bitcoinin Kaninkoloon. Ensimmäinen painos, versio 1.0.0. Tallinna, Viro: Konsensus Network OÜ, 2020.

Hautamäki, Jon, Max Atallah, ja Karri Koskikare. Virtuaalivaluutan Tarjoaminen: Käsikirja Virtuaalivaluuttalain Soveltamiseen. Helsinki: Edita Publishing Oy, 2019.

Hashemi Joo, M., Nishikawa, Y. and Dandapani, K., ICOs, the next generation of IPOs, Managerial Finance, 2020 Vol. 46 No. 6, pp. 761-783. 2020.

Hirvonen, Ari. Mitkä metodit? Yleisen oikeustieteen julkaisuja 17, Helsinki 2011.

Howell, S.T., Niessner, M., Yermack, D.,. Initial coin offerings: financing growth with cryptocurrency token sales. Rev. Financ. Stud. 2019 .

Humayun, M. and Belk, R.W. , Satoshi is Dead. Long Live Satoshi: The Curious Case of Bitcoin's Creator", Cross, S.N.N., Ruvalcaba, C., Venkatesh, A. and Belk, R.W. (Ed.) Consumer Culture Theory (Research in Consumer Behavior, Vol. 19), Emerald Publishing Limited, Bingley, pp. 19-35. 2018.

Hyttinen, Tatu. Kansallinen rikoslaki kansainvälisessä paineessa – itsepesun rangaistavuus Suomessa. Lakimies 3-4/2017, s. 334-361. 2017.

Hyttinen, Tatu. Rahanpesu Ja Rikosvastuu: Teoria Ja Käytäntö. Helsinki: Alma Talent, 2021.

Irwin, A.S.M. and Milad, G.,The use of crypto-currencies in funding violent jihad, Journal of Money Laundering Control, 2016 Vol. 19 No. 4, pp. 407-425.

Johansson, Patrik Elias, Mikko Eerola, Antti Innanen, Juha Viitala, ja Mikko Alasaarela. Lohkoketju: Tiekartta Päättäjille. Helsinki: Alma Talent Oy, 2019.

Kimpimäki, Minna. Kansainvälinen Rikosoikeus. Kauppakamari, 2015.

Marobhe, M.I., Cryptocurrency as a safe haven for investment portfolios amid COVID-19 panic cases of Bitcoin, Ethereum and Litecoin, China Finance Review International. 2021.

McDowell, J., Consequences of money laundering and financial crime, Economic Perspectives, 2001 Vol. 6 No. 2.

Melander, Sakari. Kriminalisointiperiaatteet ja perusoikeuksien rajoitusedellytykset. Lakimies 6/2002, s. 938-961, 15.11.2002, Asiantuntija-artikkeli.

Pieth, M., Criminalizing the financing of terrorism, Journal of International Criminal Justice, 2006 Vol. 4 No. 5, pp. 1074-1086.

Quinones, Arantxa, Satoshi Nakamoto, ja Lauri Kaila. Bitcoin Ja Monero: Kryptovaluuttojen Kuninkaat. Helsinki: Oppian, 2021.

Rantala, Juho. Lohkoketjuteknologian yhteiskunta. Osa I: Bitcoinista Ethereumiin. Niin & Näin, 25(1), 45-58. 2018.

Rautio, Ilkka ym. Rikosoikeus. Helsinki: Sanoma Pro, 2004 (päivittyvä teos).

Riekkinen, Juhana. Postihuumetapaukset ja selitystaakka erityisesti Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa, Defensor Legis 2020/6, s. 997-1012.

Sahavirta, Ritva. Rahanpesu Rangaistavana Tekona. Helsinki: Suomalainen lakimiesyhdistys, 2008.

Teichmann, F.M., Current trends in terrorist financing. Journal of Financial Regulation and Compliance, 2022 Vol. 30 No. 1, pp. 107-125.

Tuomaala-Järvinen, Lotta. Uhkailu, kiristys ja ryöstäminen – Pysyvät metodit jihadistiryhmien varainhankinnassa. Teoksessa: Paronen, Antti & Saarinen, Juha (toim.) 2020: Karavaanin sotapolku: Näkökulmia jihadismiin. Helsinki, Maanpuolustuskorkeakoulu.

Tuori, Kaarlo. Oikeusjärjestys ja oikeudelliset käytännöt, Forum Iuris, Helsinki 2003.

Tuori, Kaarlo. Oikeuden kahdet kasvot. Tieteessä Tapahtuu, 1998 16(6).

Wang, Q., Li, R., Wang, Q. & Chen, S.. Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. 2021.

Wang, Y., Lucey, B., Vigne, S.A. and Yarovaya, L., "An index of cryptocurrency environmental attention (ICEA)", China Finance Review International, 2022 Vol. ahead-of-print No. ahead-of-print.

Wronka, Christoph. Money Laundering Through Cryptocurrencies - Analysis of the Phenomenon and Appropriate Prevention Measures." Journal of Money Laundering Control 25, no. 1 2022: 79-94.

Virallislähteet

HE 228/2016 vp, Hallituksen esitys eduskunnalle laiksi rahanpesun ja terrorismin rahoittamisen estämisestä, laiksi rahanpesun selvittelykeskuksesta sekä eräiksi niihin liittyviksi laeiksi.

HE 167/2018 vp, Hallituksen esitys eduskunnalle laiksi pankki- ja maksutilien valvontajärjestelmästä ja eräiksi siihen liittyviksi laeiksi.

HE 55/2020 vp, Hallituksen esitys eduskunnalle laiksi pankki- ja maksutilien valvontajärjestelmästä annetun lain muuttamisesta.

HE 135/2020 vp, Hallituksen esitys eduskunnalle terrorismin rahoittamista koskevien säännösten muuttamiseksi.

HE 183/2020 vp, Hallituksen esitys eduskunnalle rikoslain 1 luvun 11 §:n ja 32 luvun 11 §:n muuttamisesta.

HE 261/2020 vp, Hallituksen esitys eduskunnalle laeiksi rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain, rahanpesun selvittelykeskuksesta annetun lain sekä pankki- ja maksutilien valvontajärjestelmästä annetun lain 6 §:n muuttamisesta.

HE 236/2021 vp, Hallituksen esitys eduskunnalle laeiksi rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain ja finanssivalvonnasta annetun lain 3 ja 20 b §:n muuttamisesta.

Oikeusministeriön julkaisuja. Mietintöjä ja lausuntoja 2020:8 – Terrorismirikosten sääntelyn ajanmukaisuus ja vastaavuus vertailumaiden sääntelyn kanssa, työryhmämietintö.

Oikeusministeriön julkaisuja. Selvityksiä ja ohjeita 2020:22. Oikeushenkilön rangaistusvastuu – nykytila ja kehittämistarpeet.

Rahanpesun selvittelykeskus (Keskusrikospoliisi). Vuosikertomus 2020. https://poliisi.fi/documents/25235045/67733116/2020-Rahanpesun-selvittelykeskus-vuosikertomus-2020.pdf/e340331f-f04c-7eec-2756-111628ae368a/2020-Rahanpesun-selvittelykeskus-vuosikertomus-2020.pdf?t=1617010848853 ., haettu osoitteesta 15.12.2021.

Rahanpesun selvittelykeskus (Keskusrikospoliisi): Puolivuosikatsaus 2021. https://poliisi.fi/documents/25235045/67733116/2021-Rahanpesun-selvittelykeskus-puolivuosikatsaus.pdf/e7c27211-792a-a06c-04cc-4cfd834bf1f1/2021-Rahanpesun-selvittelykeskus-puolivuosikatsaus.pdf?t=1626780902217 .

Sisäministeriön julkaisuja 2019:14. Malkki, Leena – Saarinen, Juha: Jihadistinen liikehdintä Suomessa.

Valtiovarainministeriö (2021). Valtiovarainministeriön julkaisuja - 2021:17, Kansallisen rahanpesun ja terrorismin rahoittamisen riskiarvio 2021. Julkaisun pysyvä osoite on http://urn.fi/URN:ISBN:978-952-367-715-9 .

Valtiovarainministeriö (2021b). Kansallisen rahanpesun ja terrorismin rahoittamisen riskiarvion toimintasuunnitelma 2021-2023. Valtiovarainministeriö. Kansallisen rahanpesun ja terrorismin rahoittamisen riskiarvion 2021 liite.

Valtiovarainministeriö (2022) Valtiovarainministeriön julkaisuja – 2022:18, Selvitys tietojenvaihdon parantamisesta kansallisessa rahanpesun ja terrorismin rahoittamisen estämistoiminnassa. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163966/VM_2022_18.pdf?sequence=1&isAllowed=y .

Verohallinto (2020). Verohallinnon ohje Virtuaalivaluuttojen verotus 22.1.2020 dnr VH/5083/00.01.00/2019. https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojen-verotus3/ .

PeVL 93/2016 vp, Perustuslakivaliokunnan lausunto 20.9.2016.

PeVL 1/2021vp, Perustuslakivaliokunnan lausunto 4.2.2021.

PeVL 34/2021 vp, Perustuslakivaliokunnan lausunto 30.9.2021.

PeVM 25/1994 vp, Perustuslakivaliokunnan mietintö hallituksen esityksestä (HE 309/1993 vp) perustuslakien perusoikeussäännösten muuttamisesta.

SopS 74/2002, Terrorismin rahoituksen torjumista koskeva kansainvälinen yleissopimus.

U 1/2017 vp, Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi (rahanpesurikokset), 2.2.2017.

Eurooppalaiset virallislähteet

European Banking Authority (EBA). EBA Report on competent authorities' approaches to the anti-money laundering and countering the financin of terrorism supervision of banks, EBA/Rep/2020/06.

Euroopan komissio, 2020. Komission tiedonanto. Toimintasuunnitelma rahanpesun ja terrorismin rahoituksen torjuntaa koskevaa kokonaisvaltaista unionin toimintapolitiikkaa varten (2020/C 164/06), Euroopan unionin virallinen lehti, 13.5.2020.

Euroopan komissio, 2021a: Ehdotus, Euroopan parlamentin ja neuvoston asetus; rahanpesun ja terrorismin rahoituksen torjuntaviranomaisen perustamisesta ja asetusten (EU) N:o

1093/2010, (EU) N:o 10924/2010 ja (EU) N:o 10952/2010 muuttamisesta, 20.7.2021, Bryssel. https://eur-lex.europa.eu/resource.html?uri=cellar:ce0c29bb-ead1-11eb-93a8-01aa75ed71a1.0017.02/DOC_1&format=PDF .

Euroopan komissio. 2021b: Ehdotus, Euroopan parlamentin ja neuvoston direktiivi; jäsenvaltioissa käyttöön otettavista mekanismeista rahoitusjärjestelmän käytön estämiseksi rahanpesuun ja terrorismin rahoitukseen ja direktiivin (EU) 2015/849 kumoamisesta, 20.7.2021, Bryssel. https://eur-lex.europa.eu/resource.html?uri=cellar:05758242-ead6-11eb-93a8-01aa75ed71a1.0006.02/DOC_1&format=PDF .

Euroopan parlamentin ja neuvoston asetus (EU) 2015/847, annettu 20 päivänä toukokuuta 2015, varainsiirtojen mukana toimitettavista tiedoista ja asetuksen (EY) N:o 1781/2006 kumoamisesta, 20.5.2015, Bryssel. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32015R0847&from=FI .

Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/843, rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen annetun direktiivin (EU) 2015/849 ja direktiivien 2009/138/EY ja 2013/36/EU muuttamisesta (viides rahanpesudirektiivi). https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32018L0843&qid=1632155580794

Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/849, rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2005/60/EY ja komission direktiivin 2006/70/EY kumoamisesta (neljäs rahanpesudirektiivi). https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32015L0849&qid=1632155746455 .

Euroopan tilintarkastustuomioistuin, Erityiskertomus 13/2021. EU:n toimet rahanpesun torjumiseksi pankkisektorilla ovat hajanaisia ja täytäntöönpano riittämätöntä. https://www.eca.europa.eu/fi/Pages/DocItem.aspx?did=58815 .

Euroopan unionin virallinen lehti (EUVL). Tiedonantoja ja ilmoituksia, 55. vuosikerta, 26. lokakuuta 2012.

Europol (2017). From suspicion to action: Converting financial intelligence into greater operational impact. Haettu osoitteesta https://www.europol.europa.eu/cms/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf

Europol (2018). Internet Organised Crime Threat Assessment 2018. Haettu osoitteesta https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 . 19.12.2021.

Europol (2020). Europol (2021), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg. Haettu osoitteesta https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf , 19.12.2021.

Muut ulkomaiset virallislähteet

FATF (2012-2022), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html

FATF, 2013. National Money Laundering and Terrorist Financing Risk Assesment Guidance. Paris, France 2013. Haettu osoitteesta https://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf .

FATF, 2019. Anti-money laundering and counter-terrorist financing measures Finland Mutual Evalu- ation Report. Pariisi 16.4.2019. Haettu osoitteesta https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Finland-2019.pdf .

FATF, 2021. Virtual assets and virtual asset service providers, Paris. Haettu osoitteesta http://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf .

Internet-lähteet

Committee on Payments and Market Infrastructures and the Bank for International Settlements: ”G7 Working Group on Stablecoins; Investigating the impact of global stablecoins” (October 2019), https://www.bis.org/cpmi/publ/d187.pdf .

Decrypt. New money laundering regulations threaten crypto firms in Europe. 1/2020. https://decrypt.co/16581/new-money-laundering-regulations-threaten-crypto-firms-in-europe , katsottu 11.2.2022.

Eurooppa-neuvosto. Lehdistötiedotteet. Rahanpesun torjunta: neuvosto hyväksyi neuvotteluvaltuutuksen kryptovarojen siirtojen avoimuudesta. https://www.consilium.europa.eu/fi/press/press-releases/2021/12/01/anti-money-laundering-council-agrees-its-negotiating-mandate-on-transparency-of-crypto-asset-transfers/ , katsottu 3.1.2022.

Finanssivalvonta. Lehdistötiedote 22.11.2017. Finanssivalvonnan varoitus: kryptovaluutat ja ICOt (Initial Coin Offering) riskialttiita sijoituskohteita. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2017/finanssivalvonnan-varoitus-kryptovaluutat-ja-icot-initial-coin-offering-riskialttiita-sijoituskohteita/ , katsottu 15.4.2022.

Finanssivalvonta. Mitä tarkoittaa virtuaalivaluutta, kryptovaluutta, kryptovara, ICO tai lompakkopalvelu?, 17.10.2019. https://www.finanssivalvonta.fi/kuluttajansuoja/virtuaalivaluutat/ , katsottu 15.4.2022.

Finanssivalvonta. Rahanpesun estäminen - uutiskooste, 2/202, 2.9.2021. https://www.finanssivalvonta.fi/globalassets/fi/rahanpesun-estaminen/rahanpesun_estaminen_uutiskooste_2_2021.pdf , katsottu 17.12.2021.

Finanssivalvonta.2021. Ylikansallinen riskiarvio. https://www.finanssivalvonta.fi/paaomamarkkinat/rahanpesun-estaminen/riskiarvio/ , katsottu 16.12.2021.

Finanssivalvonta. Kansallinen riskiarvio. https://www.finanssivalvonta.fi/paaomamarkkinat/rahanpesun-estaminen/riskiarvio/ , katsottu 16.12.2021.

Iltalehti. Suomessa yksi maailman suurimmista netin huumetutkinnoista – tuhansia tavallisia ihmisiä epäiltynä, 4.12.2019, https://www.iltalehti.fi/kotimaa/a/1a6056e8-c14a-414a-a41e-7fbedf33c171 , katsottu 4.5.2022.

Ilta-Sanomat. Poliisi takavarikoi F-Securen vpn-palvelun lokitietoja – korkein oikeus totesi KRP:n toiminnan kielletyksi, 6.4.2022, https://www.is.fi/digitoday/tietoturva/art-2000008732480.html , katsottu 15.5.2022.

Ilta-Sanomat. Bitcoinien liikkeet voivat paljastaa Vastaamo-kiristäjän – näin rahan liikkeitä seurataan, 18.11.2020, https://www.is.fi/digitoday/art-2000007626229.html , katsottu 11.4.2022.

Länsiväylä. Espoolaismies tienasi virtuaalivaluuttakaupoilla lähes puoli miljoonaa eikä ilmoittanut tuloja verottajalle – nyt tuli tuomio, 19.10.2021, https://www.lansivayla.fi/paikalliset/4336583 , katsottu 10.4.2022.

Mtv-uutiset. Markkinamanipulaatiosta syytetty Elon Musk sai bitcoinin arvon jälleen pompahtamaan – Tesla-pomo kertoo tämän ehdon bitcoinin huolimiselle, 14.06.2021, https://www.mtvuutiset.fi/artikkeli/markkinamanipulaatiosta-syytetty-elon-musk-sai-bitcoinin-arvon-jalleen-pompahtamaan-tesla-pomo-kertoo-taman-ehdon-bitcoinin-huolimiselle/8170372#gs.lrpw63 , katsottu 15.9.2021.

Mtv-uutiset. Missä on herra Nakamoto? Bitcoinin keksijän lompakossa lepää niin paljon rahaa, että sen realisoiminen voisi kolauttaa maailmantaloutta. 07.11.2021, https://www.mtvuutiset.fi/artikkeli/missa-on-herra-nakamoto-bitcoinin-keksijan-lompakossa-lepaa-niin-paljon-rahaa-etta-sen-realisoiminen-voisi-kolauttaa-maailmantaloutta/8281188 , katsottu 15.3.2022.

Norton. What is a VPN?, 24.2.2022, https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html , katsottu 10.5.2022.

Reuters. American teenager pleads guilty to helping Islamic State, 11.6.2015 https://www.reuters.com/article/us-usa-security-islamicstate-idUSKBN0OR1V520150611 , katsottu 3.10.2021.

Yle-uutiset. Bitcoin teki 28-vuotiaasta miljonäärin – 500 euron sijoituksella 2 miljoonan euron tulot, 1.11.2018. https://yle.fi/uutiset/3-10487285 , katsottu 15.12.2021.

Yle-uutiset. Mies oli päässyt eroon huumeista vuosia sitten ja odotti isäksi tuloa – sitten poliisi soitti, että on aika vastat vanhoista teoista Tor-verkossa, 16.11.2020. https://yle.fi/uutiset/3-11641812?origin=rss , katsottu 16.12.2021.

Yle-uutiset. Tutkimus: Kryptovaluutta bitcoinin louhinta uhkaa Kiinan päästötavoitteita, 8.4.2021. https://yle.fi/uutiset/3-11875578 , katsottu 5.10.2021.

YK (United Nations), Money laundering: https://www.unodc.org/unodc/en/money-laundering/overview.html , katsottu 23.9.2021.

Ulkoministeriö. Terrorismin vastaiset pakotteet. https://um.fi/terrorismin-vastaiset-pakotteet , katsottu 3.11.2021.

Oikeuskäytäntö

KHO 2019:42

KKO 2019:2

KKO 2018:3

Helsingin HO 23.3.2016, nro 16/111925

Turun HO 19.11.2021, 21/149517

Lyhenteet

AMLA	EU:n rahanpesun vastainen toimielin (Anti-Money-Laundering Authority)
EBA	European Banking Authority
EKP	Euroopan keskuspankki
ESMA	Euroopan arvopaperimarkkinaviranomainen
FATF	Financial Action Task Force
ICO	Initial coin offering
IP	internet protocol
IPO	Initial public offering
NFT	Non fungible token
P2P	Peer-to-peer (vertaisverkko)
PoS	Proof-of-stake
PoW	Proof-of-work
PKI	Public key infrastructure
PPP	Public-private partnership

1. Johdanto

1.1 Aluksi

> *”Bitcoin on ensimmäinen esimerkki uudesta elämänmuodosta. Se elää ja hengittää Internetissä. Se elää, koska sillä on kyky maksaa ihmisille hengissä pitämisestään. - - Sitä ei voi muuttaa. Sen kanssa ei voi väitellä. Sitä ei voi peukaloida. Sitä ei voi lahjoa. Sitä ei voi pysäyttää. - - Vaikka ydinsota tuhoaisi puolet planeetastamme, se jatkaisi elämäänsä, vahingoittumattomana.”*
>
> - *Ralph Merkle*[1]

Viime vuosina uutisissa on alkanut vilistä yhä useammin mainintoja virtuaalivaluutoista. Uutisointi liittyi etenkin 2010-luvun alussa hyvin vahvasti virtuaalivaluuttoihin liittyvään rikollisuuteen ja niihin liittyviin erilaisiin huijauksiin. Lainsäädännössä ja oikeustieteellisessä keskustelussa virtuaalivaluuttoihin kiinnitettiin suhteellisen rajatusti huomiota, eikä sääntelytarpeesta ainakaan laajemmin vielä puhuttu. Myöhemmin kansallisiinkin uutisiin alkoi ilmestyä uutisjuttuja muun muassa virtuaalivaluutoilla rikastuneista suomalaisista[2], minkä jälkeen keskustelu virtuaalivaluutoista ja niihin liittyvistä lainsäädännöllisistä ongelmista on lisääntynyt räjähdysmäisesti 2020-luvulle tultaessa.

Tämän tutkielman tarkoituksena on tutkia virtuaalivaluutoista aiheutuvia haasteita rahanpesu- ja terrorismin rahoittamisrikoksissa niiden sääntelyyn liittyvien haasteiden ja rikosten estämisen ja ennaltaehkäisyn näkökulmasta. Virtuaalivaluuttojen käytön jatkuva lisääntyminen on pakottanut lainsäätäjät niin EU:ssa, kuin kansallisestikin päivittämään lainsäädäntöään vastaamaan uusia tarpeita. Rikosten ennaltaehkäisyn näkökulmasta on ollut tärkeää herätä siihen, että virtuaalivaluuttojen toiminnan pohjana olevan lohkoketjuteknologian ominaisuudet ovat avanneet rikollisille uusia väyliä ja mahdollisuuksia rikosten tekemiseen virtuaalivaluuttojen avulla siten, että rikoksia voidaan toteuttaa entistä tehokkaammin, anonyymisti ja valtioiden rajat ylittäen.

---

[1] Gigi, 2020, s. 13.
[2] ks. Yle-uutiset. Bitcoin teki 28-vuotiaasta miljonäärin – 500 euron sijoituksella 3 miljoonan euron tulot, 1.11.2018.

Rahanpesu ja terrorismin rahoittaminen ovat EU:n taloudelle, sen rahoitusjärjestelmien eheydelle ja kansalaisten turvallisuudelle vakavia uhkia. Europolin arvion mukaan 1 % EU:n alueen bruttokansantuotteesta on yhteydessä epäilyttävään liiketoimintaan. Mielenkiintoisena yksityiskohtana voidaan todeta, että jopa yli 65 % näistä epäilyttäviä liiketoimia koskevista ilmoituksista olivat vuonna 2017 peräisin kahdesta (silloisesta) EU-jäsenmaasta; Iso-Britanniasta ja Alankomaista.[3] Euroopan komissio taas ilmoitti vuonna 2019, että rahanpesuun ja terrorismin rahoittamiseen liittyvä rikollinen toiminta on lisääntynyt huomattavasti covid19-pandemian myötä. Tämä on komission mukaan muistutus siitä, että rikolliset toimijat käyttävät aina hyväkseen kaikki tilaisuudet ja mahdolliset yhteiskunnassa vallitsevat heikkoudet ja haavoittuvuudet omaksi edukseen. EU:n on komission mukaan ”määrätietoisesti varmistettava, että rikolliset eivät saa rikoksistaan hyötyä”.[4]

Uudenlainen teknologia on yleensä aina tuonut mukanaan rikollisuutta, jossa rikolliset toimijat omaksuvat teknologian tarjoamat mahdollisuudet nopeasti palvelemaan rikollisia tarkoitusperiään. Lainsäätäjän rooli jää näissä murroskohdissa usein reaktiiviseksi ja uudenlaista lainsäädäntöä herätään aluksi luomaan siltä pohjalta, minkälaisia käyttötapoja rikolliset mahdollisesti keksivät uudelle teknologialle. Tutkielman aihe on ajankohtainen ja uusi, eikä suomalaista tutkimusta aiheesta ole juurikaan tehty. Tutkielman pääasiallisena aineistona on käytetty ulkomaista ja kotimaista oikeuskirjallisuutta, lainvalmisteluaineistoa ja eri viranomaisten antamia ohjeistuksia, raportteja ja selontekoja. Oikeuskirjallisuus koostuu pääasiassa ulkomaisista tieteellisistä artikkeleista ja tutkimuksista. Suomalaista oikeuskirjallisuutta on ollut saatavissa niukasti ja osa olemassa olevasta suhteellisen tuoreestakin kirjallisuudesta vaatisi jo päivittämistä.

1.2 Tutkimuskysymykset ja aiheen rajaus

Tämän tutkielman ydin tiivistyy keskeisimpään tutkimuskysymykseen; ”*Mitä haasteita ja muutostarpeita virtuaalivaluutoista aiheutuu rahanpesu- ja terrorismirikoksiin liittyvälle lainsäädännölle?*”. Kysymys sisältää niin kansalliseen, kuin kansainväliseenkin sääntelyyn liittyvän problematiikan. Rahanpesua ja terrorismin rahoittamista pyritään pääsääntöisesti sääntelemään preventiivisellä lainsäädännöllä, eli kysymykseen kuuluu myös tutkielman otsikossa mainitut ennaltaehkäisy- ja estämistoimet. Ydinkysymyksen lisäksi tutkielmaa ohjaa

[3] Europol, 2017, s. 5.
[4] Euroopan komissio, 2020, s. 1.

pääjaksoittain olennaisimmat apukysymykset. Johdannossa esitellään aihe yleisesti ja käydään läpi tutkielman rakenne, rajaukset ja tutkimusmetodit.

Toisessa pääjaksossa vastataan siihen, *mitä virtuaalivaluutat ovat ja miten niiden taustalla oleva lohkoketjuteknologia toimii*. Tutkielman rajaamiseksi käydään läpi tunnetuimmat ja tämän tutkielman kannalta keskeisimmät virtuaalivaluutat ja niiden oikeudellista asemaa *kotimaisessa lainsäädännössä*, sekä tiettyjä tämän tutkielman kannalta olennaisia virtuaalivaluuttoihin liittyviä ilmiöitä.

Kolmannessa kappaleessa käydään läpi *rahanpesua ja terrorismin rahoittamista yleisesti*, sekä esitellään niiden *nykyinen sääntely kotimaisessa rikoslainsäädännössä*. Tässä vaiheessa vastataan myös hyvin yleisellä tasolla siihen, *miten virtuaalivaluuttoja pyritään käyttämään hyödyksi kyseisissä rikoksissa* erityisesti niiden taustalla olevan lohkoketjuteknologian näkökulmasta. Terrorismin rahoittamisosiossa kuvaillaan, miten terroristirikolliset itse ovat kertoneet virtuaalivaluuttojen käytöstä rikollisuudessa. Lopuksi pohditaan yleisten kriminalisointiperiaatteiden kautta niitä rajoja, joiden puitteissa lainsäädäntöä mahdollisesti voisi muuttaa.

Neljännessä kappaleessa vastataan siihen, *miten rahanpesua ja terrorismin rahoittamista pyritään estämään niin kansallisella, kuin kansainväliselläkin tasolla.,* Rahanpesun ja terrorismin rahoittamisen vastaisia toimia toteutetaan niin monella tasolla ja niin monen tahon toimesta, että tutkielman rajaamiseksi keskitytään niihin toimijoihin ja säädöksiin, joilla on merkitystä nimenomaan virtuaalivaluuttojen näkökulmasta.

Viidennessä kappaleessa käydään tarkemmin läpi *virtuaalivaluuttojen rikoslainsäädännölle aiheuttamia haasteita kansallisessa riskiarviossa.* Valtiovarainministeriö on velvoitettu laatimaan vuosittain rahanpesun ja terrorismin rahoittamisen kansallinen riskiarvio, jonka pohjalta kappaleessa käydään tarkemmin läpi sitä, minkälaisia haasteita virtuaalivaluutat aiheuttavat nimenomaan *suomalaiselle lainsäädännölle ja rikollisuuden estämis- ja ennaltaehkäisytoimille.*

Kuudennessa kappaleessa vastataan siihen, *miten näihin aiemmin esiteltyihin haasteisiin aiotaan viranomaisten toimesta vastata ja mihin suuntaan lainsäädäntöä tulisi lähteä kehittämään*. Kappaleessa annetaan ehdotuksia myös mahdollisista uusista kriminalisoinneista. Lopuksi pohditaan vielä yleisemmin virtuaalivaluuttojen finanssimaailmalle aiheuttamia

muutospaineita ja seitsemännessä ja viimeisessä kappaleessa tutkielman olennaisimmat johtopäätökset ja havainnot vedetään yhteen.

1.3 Metodi ja lähdeaineisto

Lainsäädäntö ei ole yhteiskunnallisista ilmiöistä irrallinen ja erillinen kokonaisuus, vaan ne käyvät jatkuvaa vuorovaikutusta toistensa kanssa ja vaikuttavat toinen toisiinsa. Etenkin uusia yhteiskunnassa olevia ilmiöitä pyritään usein ensin tulkitsemaan ja sovittamaan voimassaolevan lainsäädännön kehykseen ja tulkitsemaan niitä sen hetkisestä lainsäädännöstä käsin. Mikäli voimassa oleva lainsäädäntö ei enää ole riittävää ja tulkinnassa joudutaan menemään kohti kiellettyä analogiaa, joudutaan säätämään uusia tai päivittämään vanhoja lakeja ja vaikutus kääntyy yhteiskunnasta lainsäädännön suuntaan.

Tässä tutkielmassa tutkimusmetodina on lähtökohtaisesti lainoppi, joka painottuu de lege ferenda-tutkimukseen, eli voimassaolevan lainsäädännön ja lain tavalla velvoittavien viranomaisten ohjeistuksen systematisointiin. Oikeusdogmatiikka eli lainoppi on yleensä nähty hyvin perinteisenä oikeustieteen ydinalueena, jonka avulla tutkitaan kullakin hetkellä voimassaolevaa oikeutta ja tuotetaan tieteellistä tietoa oikeusnormeista ja voimassaolevasta oikeudesta. [5] Virtuaalivaluuttoihin liittyvä ongelmakenttä on niin moninainen, kansainvälinen ja useille tieteenaloille ulottuva, että tutkimuksessa on lainopin ohella väistämättä vahva oikeuspoliittinen painotus ja siihen sisältyy myös yhteiskunnallista ja taloustieteellistä pohdintaa. Oikeuspoliittinen näkökulma on välttämätön senkin takia, että virtuaalivaluuttojen sääntelyyn liittyvät lainsäädäntöhankkeet ovat esimerkiksi EU:ssa vasta ehdotusvaiheessa ja ala on edelleen jatkuvassa muutoksessa. Oikeusteoreettista pohdintaa taas joudutaan soveltamaan, kun pohditaan yleisten kriminalisointiperiaatteiden ja perustuslain asettamia rajoja mahdollisille lainsäädännön muutoksille.

Yleisesti tutkimuksen tarkoituksena tulisi olla tuottaa jonkinlaista lisäarvoa, uutta tietoa ja jäsenneltyjä näkökulmia tutkittavana olevaan aiheeseen, eikä esimerkiksi liian tiukka lainopillisessa metodissa pysytteleminen muuttuvaa ja suhteellisen uutta aihetta tutkiessa ole välttämättä hedelmällisin lähtökohta. Aiheesta ei ole kirjoitettu juurikaan ja nykyisen oikeudellisen tilanteen systematisointi ja sen puutteiden ja haasteiden esiin nostaminen on tässä vaiheessa luonteva tapa lähestyä aihetta.

[5] Hirvonen, 2011, s. 17.

Tätä tutkielmaa on sen tekoaikana jo jouduttu päivittämään ja käytännössä jokainen kuukausi on tuonut ja tuo mukanaan uudenlaisia näkökulmia ja myös muutostarpeita aiheeseen liittyen. Tämän lisäksi myös puhtaasti oikeustieteellisten lähteiden vähäisyys suuntaa tutkimuksen painopisteen enemmän yleisellä tasolla olevien säännösten ja periaatteiden tarkasteluun ja annetut lainsäädännön muutosehdotukset lopussa pyrkivät vastaamaan tiettyihin tutkimuksessa esiin nousseisiin ongelmiin. Kehitys on tällä hetkellä vaiheessa, jossa suhtautumistapaa virtuaalivaluuttoihin on alettu pohtimaan ja niiden oikeudellinen arviointikin on monella tapaa kesken. Lainsäätäjällä ei ole varmaa tilannekuvaa siitä, minne virtuaalivaluuttojen ja lohkoketjuteknologian kehitys lopulta etenee ja mikä niiden rooli tulee todellisuudessa tulevaisuudessa olemaan.

Kaarlo Tuori on todennut, että ”tärkeä tehtävä oikeustietelijöiden itseymmärryksen syventämisessä on tehdä heidät tietoisiksi yhteiskuntateoreettisista riippuvuuksistaan”.[6] Oikeustiede on riippuvainen ja myös jatkuvassa vuorovaikutuksessa muiden tieteenalojen kanssa. Lainsäädäntöä ei luoda tyhjiössä, vaan lait heijastelevat käytännössä aina kulloisenkin ajan yhteiskuntaa ja siinä vallitsevia arvoja ja moraalia. Lain soveltajien ja tuomarien ihanteena toimii symbolisestikin side silmillään tuomitseva oikeuden jumalatar, mutta tutkija joutuu väistämättä pohtimaan lainsäädäntöä myös muiden tieteiden kautta ja niiden avustuksella. Tutkielman aihe on vahvassa yhteydessä finanssi- ja sijoitusmaailmaan ja erityisesti internet-lähteitä käytettäessä tulee tästä syystä olla erityisen huolellinen, ettei tutkimukseen pääsisi mukaan sellaisten henkilöiden värittyneitä näkemyksiä tai jopa toiveita, jotka ovat esimerkiksi itse sijoittaneet varallisuuttaan virtuaalivaluuttoihin. Internetistä kerätyt lähteet ovat pääsääntöisesti peräisin viranomaisten verkkosivuilta ja ulkomaiset artikkelit vertaisarvioituja ja haettu yliopiston tietokannoista. Tutkielmassa on tehty myös tietoinen valinta jättää pois virtuaalivaluuttojen tarjoajien näkemykset virtuaalivaluuttojen tulevaisuudesta ja tietoa esimerkiksi näiden toimijoiden verkkosivustoilta on haettu rajatusti.

Tutkielman lähtökohtia esiteltäessä voidaan viitata myös *Tuorin* esille nostamaan ajatukseen oikeustieteen hitaasti muuttuvasta syvärakenteesta ja nopeammin muuttuvasta pintatasosta.[7] *Tuorin* teoriaa mukaillen voidaan todeta, että virtuaalivaluuttoihin liittyvä sääntely on vaikuttanut nimenomaan ensin oikeuden pintatasoon. Suomessa on suhteellisen nopeasti virtuaalivaluuttojen yleistymisen jälkeen säädetty laki virtuaalivaluuttojen tarjoajista. Uudistuksen jälkeen on kuitenkin havaittu, että kyse onkin laajemmasta ongelmasta tai

[6] Tuori, 2000, s. 324.
[7] Ks. Tuori, 1998.

kokonaisuudesta ja sellaisesta teknologian kehityksestä, joka tulee väistämättä vaatimaan muutoksia myös oikeuden syvärakenteeseen ja sen pohjana oleviin fundamentteihin. Tämä tutkielma pyrkii antamaan rikosoikeuden ja rikosten ennaltaehkäisyn näkökulmasta kuvan siitä, minkälaisten haasteiden ja pohdintojen edessä ollaan, kun virtuaalivaluuttoja lähdetään sääntelemään niin kansallisesti, kuin kansainvälisestikin ja samalla myös antamaan vastauksia akuuteimpiin täsmällisempiin lainsäädännöllisiin haasteisiin.

2. Lohkoketjuteknologia ja virtuaalivaluutat

2.1 Lohkoketjuteknologia

> *”Imagine having almost instantaneous access to a permanent record of all digital transactions undertaken across the world. Without revealing precisely who and what is involved in these transactions, this digital database grants you nearly real-time overviews of peer-to-peer exchange within and across national borders.”*[8]

Yllä oleva kuvaus tiivistää lohkoketjuteknologian taustalla olevan perimmäisen ajatuksen. Jotta virtuaalivaluuttoihin liittyviä oikeudellisia ongelmia voisi ymmärtää, on hyvä aluksi esitellä niiden toimintaa ja taustalla olevaa lohkoketjuteknologiaa, jotta perehtymätönkin lukija saisi riittävän laajan kuvan siitä, mitä lohkoketjuteknologia ja virtuaalivaluutat ovat ja miten ne toimivat. Virtuaalivaluuttojen hyödyntäminen rikollisessa toiminnassa perustuu käytännössä täysin niiden pohjalla olevan teknologian ominaisuuksien hyödyntämiseen, joten hyvän kokonaiskuvan saamiseksi aihetta ei voi ohittaa.

Lohkoketjuteknologia ja niiden pohjalle rakentuneet virtuaalivaluutat ovat herättäneet viime vuosina laajaa keskustelua ja joidenkin mielestä lohkoketjut ovat jopa tärkein keksintö sitten internetin syntymisen. [9] Lohkoketjuteknologiaa voidaan yksinkertaisimmillaan kuvata siten, että se on kehittynyt teknologinen versio julkisista rekistereistä, joihin on aiemmin kirjattu kylissä ja kaupungeissa kaikki tärkeä ihmisten syntymätiedoista avioliittoon ja omaisuuden siirtoihin. Sen sijaan, että nämä tiedot kirjattaisiin nykyisin käsin ylös paksuihin muistikirjoihin, lohkoketju käyttää kehittynyttä kryptografiaa ja hajautettua järjestelmää, joiden avulla pystytään luomaan läpinäkyvä, pysyvä ja turvallinen lähdeaineisto, joka myös kestää siihen kohdistuvat hyökkäykset ja manipulaatioyritykset. Lohkoketju on käytännössä perinteistä luotettavampi tilikirja, johon aikajärjestyksessä merkitään tapahtumia.[10] Vaikka lohkoketjuteknologia yhdistetään yleisimmin virtuaalivaluuttoihin ja etenkin bitcoiniin, on sen pohjalle alettu kehitellä yhä kiihtyvällä tahdilla muitakin sovellutuksia, jotka todennäköisesti tulevat laajasti käyttöön useilla aloilla.[11] Tässä esityksessä keskitytään kuitenkin tuomaan

[8] Campbell-Verduy, 2018, s. 1.
[9] Johansson ym., 2019, s. 26. Internet-vertaus on sikäli osuva, että aikoinaan internetin sääntelyyn liittyvät ongelmat olivat hyvin samankaltaisia, kuin nykyisin virtuaalivaluuttojen kanssa. Olennaisin yhdistävä tekijä on molempien hajaantuneisuus ja kansainvälinen sääntelytarve.
[10] Johansson ym., 2019, s.27.
[11] Ks. esim. Garcia-Teruel, R.M, 2020. Tutkimuksessa selvitettiin lohkoketjuteknologian käyttömahdollisuuksia kiinteistönvälityksessä. Lohkoketjuteknologiaan perustuvat älykkäät

lohkoketjuteknologiaa ja sen ominaisuuksia esiin virtuaalivaluuttojen käytön ja toiminnan näkökulmasta.

Ensimmäinen ja alkuperäinen lohkoketju on luotu virtuaalivaluutta bitcoinin luomisen yhteydessä. *Johansson* on kuvaillut bitcoinin taustalla olevaa lohkoketjua vertaamalla sitä jo edellä esitetyn mukaisesti valtavaan tilikirjaan tai Excel-taulukkoon, jonka tiedot muodostuvat kaikista niistä transaktioista ja siirroista, joita bitcoinin käyttäjät tai haltijat ovat aikojen saatossa tehneet. Esimerkkinä; mikäli henkilö A lähettää bitcoinia henkilölle B, jää tästä merkintä bitcoinin lohkoketjuun, jonka perusteella henkilön A tilin saldo vähenee ja B:n kasvaa transaktion mukaisesti.[12] Lohkoketju on siis käytännössä täysin julkinen tietokanta ja siihen merkityt siirrot kaikkien nähtävillä ja saavutettavissa. Lohkoketjun luotettavuus syntyy matemaattisesti siten, että sen luotettavuuden takaamiseksi ei tarvita ihmisten ylläpitämää tai luomaa järjestelmää tai tahoa. [13] Tämä on lohkoketjun ominaisuus, joka luo sille ominaisen luotettavuuden; lohkoketjuihin merkittyjä siirtoja ja transaktioita ei ole mahdollista enää jälkikäteen muokata tai poistaa.

Yleensä virtuaalivaluutoista puhuttaessa korostetaan nimenomaan niiden itsenäisyyttä yhdenkään keskuspankin tai valtion kontrollista. Tämä on seurausta toisesta lohkoketjulle ominaisesta piirteestä, hajautuneisuudesta. Lohkoketju on hajautettu järjestelmä ja sen osaset on jaettu lukuisille eri tietokoneille, jotka yhdessä pitävät yllä tätä järjestelmää. Mikä tahansa tätä järjestelmää ylläpitävä tietokone voi tehdä muutoksia lohkoketjuun tietyillä säännöillä ja ehdoilla. Näitä yhteisiä sääntöjä kutsutaan ”konsensusprotokollaksi”, eli vaikka muutoksia voi tehdä periaatteessa kuka tahansa, jokaisen muutoksen toteuttamiseen vaaditaan kuitenkin kaikkien käyttäjien hyväksyntä. [14] Luonnollisestikaan ei ole kyse siitä, että käyttäjät todellisuudessa tekisivät jonkin tietoisen päätöksen tai toimen näiden muutosten hyväksymiseksi, vaan ne toteutetaan monimutkaisilla matemaattisilla menetelmillä, joita ei ole tarkoituksenmukaista käydä tässä esityksessä tarkemmin läpi.

Yksi merkittävimmistä haasteista nykyisissä julkisissa lohkoketjuissa on se, että ne vaativat suuria määriä laskentatehoa tilikirjan ylläpitämiseksi. Tällä hetkellä lohkoketjut ovatkin

---

sopimukset voisivat nopeuttaa ja tehostaa kiinteistökauppoja, sekä lisätä osapuolten välistä luottamusta. Tutkimuksessa mainittiin myös useita muitakin sopimuksiin pohjautuvia aloja, jotka voivat lohkoketjuteknologian kehityksen mukana ottaa valtavia harppauksia nykyisestä. Muutamina esimerkkeinä mainittiin mm. vakuutusala, julkinen hallinto ja jopa terveydenhuolto.

[12] Johansson ym., 2019, s. 28.

[13] Johansson ym., 2019, s. 28.

[14] Johansson ym., 2019, s. 29.

suhteellisen hitaita prosessoimaan suuria määriä transaktioita verrattuna perinteisiin luottokortteihin. Yritysmaailmassa virtuaalivaluuttojen käyttöönoton suurimmat ongelmat liittyisivät nimenomaan julkisuuteen ja siihen, että mahdolliset kilpailijat voisivat onkia transaktioista itseään hyödyttäviä tietoja. [15]

Sen jälkeen, kun bitcoin on käynnistetty, on luotu muitakin samankaltaisia lohkoketjuja, jotka toimivat periaatteessa samalla tavalla kuin bitcoin, mutta niissä on joitain teknisiä muutoksia, jotka liittyvät esim. lohkojen luomisnopeuteen tai transaktioiden määrään. Vuonna 2015 julkaistiin Ethereum-startup, jonka uudenlainen lohkoketju mahdollisti tietokoneohjelmien suorittamisen ja tallentamisen lohkoketjussa. Nämä tietokoneohjelmat mahdollistavat myös ns. älykkäät sopimukset, joita voidaan muun muassa toteuttaa automaattisesti ilman ihmisten konkreettisia toimia. [16]

2.1.1 Lohkoketjun osat ja keskeiset käsitteet

Seuraavaksi käydään yksityiskohtaisemmin läpi lohkoketjun olennaisimmat osat ja rakennuspalikat, jotta niiden taustalla oleva teknologia avautuisi hieman laajemmin, sillä juuri nämä osaset tarjoavat virtuaalivaluutoille niille ominaiset piirteet, kuten hajautuneisuuden, luotettavuuden ja vahvan salauksen. Huomionarvoista on, että lohkoketjuteknologian taustalla olevat yksittäiset osaset eivät ole mitään uusia keksintöjä ja virtuaalivaluutat perustuvatkin näiden vanhojen teknologioiden innovatiiviseen yhdistelyyn. [17]

1) Hajautettu tilikirja[18]

Hajautettu tilikirja on käytännössä jaettu tietokanta, jota ylläpitää monet itsenäiset osanottajat. Tilikirja on tapahtumarekisteri, johon kaikki tapahtuneet siirrot ja transaktiot ovat tallentuneet, eikä näitä tietoja voida muuttaa, sillä ne tallentuvat kryptografisesti[19] allekirjoitettuun ja salattuun tietokantaan. [20] Tämä ominaisuus takaa hajautettuun järjestelmään perustuville virtuaalivaluutoille niille ominaisen luotettavuuden. Hajautetun tilikirjan toiminta perustuu hajautetussa verkossa (P2P) toimiviin tietokoneisiin.

[15] Johansson ym., 2019, s. 76
[16] Johansson ym., 2019, s. 30.
[17] Johansson ym., 2019, s. 56.
[18] eng. *ledger*.
[19] Kryptografia tarkoittaa tässä yhteydessä salausta, jonka avulla voidaan salata dataa niin, että vain viestin vastaanottajalla on mahdollisuus lukea kyseinen viesti.
[20] Johansson ym., 2019, s. 57.

2) PKI

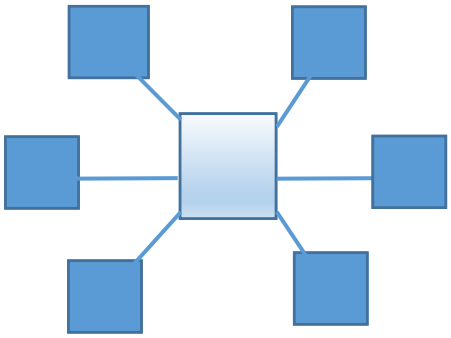
PKI on lyhenne sanoista Public Key Infrastructure ja se tarkoittaa niitä toimintatapoja, joiden tarkoituksena on datan salaaminen.[21] PKI perustuu sille mekanismille, jota käytetään digitaalisten sertifikaattien luomiseen. Nämä sertifikaatit ovat käytännössä digitaalisia versioita fyysisistä henkilökorteista tai esimerkiksi passeista.[22] PKI:n perustana on kaksi avainta, joista toinen on julkinen ja toinen yksityinen. Nämä avaimet muodostetaan aina parina, jotka ovat molemmat saman käyttäjän hallinnassa. Julkinen avain on nimensä mukainen julkinen kaikille ja yksityinen taas vain sen tiedossa, jonka hallinnassa kyseinen avain on, eikä käyttäjä ei saa luovuttaa avainta kenellekään muulle. Julkisella avaimella voidaan purkaa salaus vain sellaisten tietojen osalta, jotka on salattu sen vastinkappaleella, eli jos julkista avainta käytetään salauksen purkamiseen, voidaan olla varmoja, että tiedoston salaaja omistaa avaimen yksityisen vastakappaleen.[23] PKI antaa virtuaalivaluutoille niille ominaisen vahvan salauksen ja anonymiteetin. Ongelmana esimerkiksi bitcoinin kanssa onkin ollut tilanteet, joissa käyttäjä on kadottanut oman salasanansa, eikä tämä ole enää päässyt käsiksi virtuaalivaluuttavarallisuuteensa.

3) P2P

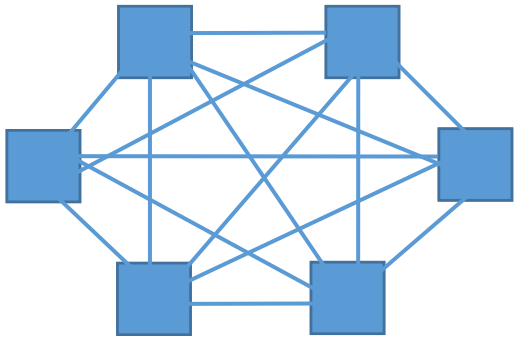
P2P on lyhenne Peer to Peer-verkosta. P2P tarkoittaa vertaisverkolla jaettua sovellusarkkitehtuuria, jossa tehtävät on jaettu monien vertaisten kesken. Vertaiset ovat nimensä mukaisesti tasa-arvoisia ja ne ovat olennainen syy sille, miksi lohkoketjut ovat niin luotettavia. Kaikki käyttäjät tuovat verkkoon jotain ja kaikki käyttäjät myös hyötyvät siitä.[24] Perinteisesti verkoissa on ollut palveluntarjoajat, jotka tarjoavat käyttäjille palveluita ja asetelma on ollut hierarkkinen. Näitä verkkoja kutsutaan serveriverkoiksi. Vertaisverkot ovat poistaneet tarpeen keskuspalvelimille ja verkkojen ”isännille”. [25]

[21] Johansson ym., 2019, s. 58.
[22] Johansson ym., 2019, s. 58.
[23] Johansson ym., 2019, s. 59
[24] Johansson ym., 2019, s. 61.
[25] Johansson ym., 2019, s. 61.

Serveriverkko



Vertaisverkko



4) Konsensus ja konsensusalgoritmi

Hajautettujen järjestelmien suurimpia ongelmia on yleensä se, miten käyttäjien välillä päästään yhteisymmärrykseen vertaisverkkojen toiminnasta, kun järjestelmällä ei ole minkäänlaista ”keskushallintoa” selvittämässä ongelmia ja luomassa yhteisiä pelisääntöjä. Tämä on ratkaistu usein niin sanotulla konsensusalgoritmilla, joka luo yhteisymmärryksen siitä, missä tilassa kukin muuttuja on tieyllä hetkellä. Konsensusalgoritmi ratkaisee luotettavuuden ongelmat matemaattisesti siten, ettei jokaisen toimijan luotettavuutta tarvitse erikseen arvioida.[26] Bitcoinissa käytetään esimerkiksi niin sanottua Proof-of-Work-verkkoa, joka perustuu siihen, että verkon osanottajien suorittaman laskennan määrä on sidottuna siihen käytettyyn aikaan.[27]

5) Älykkäät sopimukset

Älykkäät sopimukset ovat tietokoneohjelmia, jotka on ohjelmoitu toteuttamaan ostajan ja myyjän sopimusehdot ja tahdonilmaisut niin, että ne kirjautuvat automaattisesti hajautettuun tilikirjaan, eikä kenenkään kolmannen osapuolen tarvitse niitä vahvistaa.[28] Lohkoketjuteknologia ratkaisi älykkäissä sopimuksissa aiemmin olleen ongelman, jossa ulkopuolisella oli mahdollisuus muokata sopimuksia ja niiden ehtoja jälkikäteen. Älykkäät sopimukset mahdollistavat rahan tai vaikka osakkeiden vaihdon ilman kolmansia osapuolia ja lisäkustannuksia, luotettavasti ja läpinäkyvästi.[29] Kaikilla lohkoketjuilla ei kuitenkaan ole näitä ominaisuuksia ja esimerkiksi bitcoin mahdollistaa älykkäät sopimukset vain hyvin rajoitetusti.[30]

[26] Johansson ym., 2019, s. 62.
[27] Casey ym., 2018, s. 2.
[28] Casey ym., 2018, s. 4.
[29] Johansson ym., 2019, s. 64.
[30] Casey ym., 2018, s. 5.

6) Dipolit/tokenit

Englannin kielessä puhutaan virtuaalivaluuttojen yhteydessä ns. tokeneista, eli dipoleista. Dipoli on lyhenne sanoista digitaalinen poletti. Poletti ei ole varsinainen valuutta, vaan niiden avulla voidaan lunastaa tiettyjä hyödykkeitä.[31] Esimerkkinä tästä on kasinoilla saatavat poletit, joilla voidaan pelata ja jotka voidaan myöhemmin vaihtaa takaisin rahaksi. Dipolit ovat näistä digitaalinen versio, jotka on sijoitettu lohkoketjuun. Ne toimivat siellä kuvauksena jostain omaisuuserästä tai oikeudesta, kuten vaikkapa osakkeista tai kanta-asiakaspisteistä.[32]

7) Lohko

Lohkoketjun keskeisimpiä osasia ovat siinä olevat lohkot. Lohkot ovat niitä paikkoja, joihin tallennetaan osa tai kaikki viimeisimmät lohkoketjuverkkoon lähetetyt tiedot, joita ei vielä ole sisällytetty aikaisempiin lohkoihin. Lohkot ovat siis aikaisempien esimerkkien mukaisia ”fyysisen maailman tilikirjoja”, joihin kaikki omaisuuden siirrot merkitään. Aina kun lohko on valmis, se siirtyy pysyväksi ketjun osaksi ja uudet tiedot tallennetaan sen tilalle tulleeseen uusimpaan lohkoon. Lohkot muodostavat katkeamattoman ketjun ja jokaisen lohkon tiedot ovat salattuja. Juuri tämä ominaisuus tekee niiden jälkikäteisestä muokkaamisesta käytännössä mahdotonta. [33]

8) Noodi

Noodeiksi kutsutaan niitä laitteita, jotka ovat aktiivisesti mukana luomassa lohkoketjua ja pitämässä yllä sen järjestelmää. Noodit voivat olla niin tietokoneita, kuin puhelimiakin ja niiden tehtävä on tukea verkkoa ja säilyttää siitä kopioita. Noodit mahdollistavat lohkoketjujen hajautuneisuuden ja sen, että niitä ei voi tuhota esimerkiksi hakkerien toimesta.[34]

9) Louhinta ja louhijat

Louhinta on yksinkertaistettuna ja lyhyesti sitä, että noodien omistajat keräävät transaktiokustannuksia ja ansaitsevat palkkioita siitä, että he jakavat laskentaresurssejaan transaktioiden varmentamiseksi ja tallentamiseksi lohkoketjussa.[35] Bitcoinin louhinnasta on ollut laajalti keskustelua mediassa sen valtavan sähkönkulutuksen ja ilmastovaikutusten

[31] Dipolien määritelmä vaihtelee sen mukaan, mistä virtuaalivaluutasta on kyse. Ethereum-lohkoketjussa dipolilla tarkoitetaan esimerkiksi yhtä ether-yksikköä, ks. kappale 2.2.1. Bitcoin ja etheruem.
[32] Johansson ym., 2019, s. 66.
[33] Johansson ym., 2019, s. 67.
[34] Johansson ym., 2019, s. 68.
[35] Johansson ym., 2019, s. 69.

takia.[36] Louhinta tapahtuu nykyisin erittäin tehokkailla tietokoneilla, mutta bitcoin-lohkoketjun alkuvaiheissa louhintaan riitti tavallinen kotitietokone. Bitcoinia louhitaan sen protokollasta, jossa ne ovat olemassa ja johon on määritelty bitcoinien maksimimäärä, 21 miljoonaa yksikköä.[37] Bitcoin-järjestelmässä tämä tapahtuu käytännössä siten, että noodit ratkaisevat monimutkaisia matemaattisia yhtälöitä ja sisällyttävät yhtälöistä saadut vastaukset lohkoihin. Louhinta on siis yleensä välttämätöntä, jotta lohkoihin voidaan lisätä ja tallentaa dataa ja niitä voidaan liittää toisiinsa. On kuitenkin mahdollista luoda myös sellaisia lohkoketjuja, joissa louhinnan sijaan on datan tallentamiseksi valittu jokin toinen menetelmä.[38] Bitcoin-lohkoketjun alkuvaiheissa louhintaa pystyttiin suorittamaan tavallisilla kotitietokoneilla, mutta nykyisin siihen vaaditaan tehokkaita erikoistietokoneita, jotka kuluttavat paljon sähköä.[39]

2.2 Virtuaalivaluutat

Virtuaalivaluuttoja määritellään hieman eri tavalla määrittelijästä ja kontekstista riippuen. Bitcoin-lohkoketjun perustaja *Satoshi Nakamoto*[40] on määritellyt virtuaalivaluutat seuraavasti;

> *”Kryptovaluutat*[41] *ovat lohkoketjuissa sijaitsevaa salattua valuuttaa. Toisin kuin setelit ja paperiraha, niitä on lähes mahdotonta väärentää. Ne eivät tarvitse toimiakseen keskusauktoriteettia, ja niitä suojelee, säännöstelee ja luo sarja monimutkaisia algoritmeja. Kryptovaluutat poistavat monet sähköisen varojen siirron haitoista ja heikkouksista, kuten - - päivittäisen siirtorajan. Siirrettävien varojen määrälle ei ole rajoitteita. Tilejä ei voi hakkeroida, koska niillä ei ole keskitettyä*

[36] Ks. Yle-uutiset. Tutkimus: Kryptovaluutta bitcoinin louhinta uhkaa Kiinan päästötavoitteita, 8.4.2021.
[37] Rantala, 2018, s. 45. Vuonna 2017 21 miljoonasta kolikosta oli louhittu jo 16 miljoonaa, mutta louhinnan vaikeutuessa viimeisten kolikkojen ennustetaan louhittavan noin vuonna 2040.
[38] Johansson ym., 2019, s. 69.
[39] Ks. Wang ym. 2022. Tutkimuksessa on selvitetty virtuaalivaluuttojen ympäristö- ja ilmastovaikutuksia, jotka liittyvät niiden käyttöön liittyvään suureen energian tarpeeseen ja etenkin louhimisesta aiheutuviin päästöihin. Tutkimuksessa on luotu ns. ICEA-indeksi (index of cryptocurrency environmental attention), jonka avulla voidaan arvioida esimerkiksi sitä, miten virtuaalivaluuttojen ympäristövaikutukset voivat lopulta vaikuttaa sen vakauteen ja miten sitä tulisi jatkossa kehittää huomioiden riittävästi myös ympäristönäkökulma.
[40] Ks. kappale 2.2.1.
[41] Sanat virtuaalivaluutta ja kryptovaluutta tarkoittavat tarkasti määriteltynä hieman erilaisia asioita. Virtuaalivaluutta on yleiskäsite niin hajautetuille, kuin hajautumattomillekin virtuaalivaluutoille ja kryptovaluutoilla taas viitataan bitcoinin kaltaisiin hajautuneisiin ja julkisiin järjestelmiin perustuviin virtuaalivaluuttoihin, joissa keskeistä on myös käyttäjän anonymiteetti. Lainsäädännössä virtuaalivaluutan käsitteellä tulee kuitenkin kattaa kaikenlaiset virtuaalivaluutat, vaikka suurimmat ongelmat liittyvätkin hajautuneisiin järjestelmiin perustuviin kryptovaluuttoihin. Tässä tutkielmassa käytetään pääsääntöisesti yleisnimitystä virtuaalivaluutta, vaikka esimerkiksi anonyymiyden ongelmista puhuttaessa viitataan tarkemmin kryptovaluuttoihin.

tietokeskusta ja työtodenteellinen hajautettu tilikirja takaa tietojen eheyden." [42]

Vaikka virtuaalivaluuttoja on suomalaisessakin lainsäädännössä määritelty, oleellista on ymmärtää se, mitä virtuaalivaluutta on tai voi olla. Sitä valuuttaa, jota me käytämme normaalissa jokapäiväisessä elämässämme, kutsutaan yleisesti fiat-valuutaksi.[43] Sen arvo perustuu lainsäädäntöön ja käytännössä siihen, että ihmiset uskovat sillä olevan arvoa. Fiat-valuutta eroaa virtuaalivaluutoista myös siinä, että sitä voidaan käytännössä valtioiden käskystä ja/tai keskuspankkien toimesta painaa aina lisää. Bitcoineja taas on lohkoketjuun perustuvan teknologian ansiosta olemassa vain rajallinen määrä. Tästä syystä virtuaalivaluuttoja ja etenkin bitcoinia kuvaillaan joskus "virtuaaliseksi kullaksi", sillä se on kullan tavoin rajoitettu hyödyke.[44] Täytyy kuitenkin selvyyden vuoksi todeta, että rajattu määrä ei automaattisesti tarkoita sitä, että valuutan arvo tulisi kasvamaan tai että sillä välttämättä edes olisi mitään arvoa tulevaisuudessa. Kriitikot arvelevatkin bitcoinin olevan ainoastaan kupla, joka jossain vaiheessa puhkeaa.[45]

Rikollisuuden torjunnan ja rikosoikeudellisen vastuun toteuttamisen näkökulmasta suurimmat virtuaalivaluuttoihin liittyvät ongelmat ovat liittyneet pääasiassa niihin liittyvään anonymiteettiin ja hajautetun järjestelmän ominaisuuksiin. Anonymiteetti on vaihdellut anonymiteetistä pseudo-anonymiteettiin, mikä on mahdollistanut esimerkiksi laittomat varainsiirrot ja estänyt virtuaalivaluuttojen siirtojen riittävän valvonnan. Tämän seurauksena esimerkiksi rahanpesussa rikollisilla ja rikollisjärjestöillä on ollut helpompaa päästä suoraan käsiksi rikoksella hankittuun "likaiseen rahaan" ja kiinnijäämisen riski on ollut vähäinen. Anonymiteetti on ollut olennainen osa myös virtuaalivaluuttojen avulla suoritettavaa veronkiertoa.[46] Kun verotuksen alaisten transaktioiden tekijät ovat jääneet veroviranomaiselle hämärän peittoon, tehdyistä rikoksista ei myöskään ole voitu välttämättä antaa mitään sanktioita.[47] Lohkoketjuteknologialle ja virtuaalivaluutoille ominainen hajautettu luonne

[42] Quinones – Nakamoto, 2021, s. 29.
[43] Hautamäki ym., 2019, s. 4.
[44] Hautamäki ym., 2019, s. 5.
[45] Ks. Diniz ym., 2022. Tutkimuksessa bitcoinin ja ethereumin arvostuksessa olevaa mahdollista kuplaa on pyritty tutkimaan niin sanottua taloustieteessä käytössä olevaa GSDAF (generalized supremum augmented Dickey-Fuller)-testiä apuna käyttäen ja sen mukaan molemmissa virtuaalivaluutoissa on havaittavissa testin asteikolla erittäin kohonnut kuplan riski. Tutkimus on julkaistu maaliskuussa 2022.
[46] Nykyisin virtuaalivaluuttojen tarjoajat on velvoitettu tunnistamaan asiakkaansa ja ilmoittamaan verottajalle virtuaalivaluutoista saadut tuotot. Vuonna 2021 Länsi-Uudenmaan käräjäoikeus tuomitsi espoolaismiehen törkeästä veropetoksesta hänen jätettyä ilmoittamatta vuosina 2015 ja 2016 noin 500 000 euron suuruiset tulot, jotka olivat peräisin virtuaalivaluuttakaupoista, ks. Länsiväylä, 19.10.2021.
[47] Johansson, 2019, s. 212.

tarkoittaa sitä, että tehokasta lainsäädäntöä ei voida käytännössä luoda vain yhden valtion toimesta, vaan sitä tulisi säädellä kansainvälisesti. Louhinta itsessään voi myös toimia tehokkaana rahanpesumenetelmänä, jos ”likaisen” rahan käyttäisi bitcoinien louhimiseen ja mikäli virtuaalivaluutta kävisi suoraan maksuvälineen kulutushyödykkeisiin.

2.2.1 Bitcoin ja ethereum

Luultavasti kaikkein tunnetuin virtuaalivaluutta luotiin vuonna 2009. Sen alkuperäinen kehittäjä ja liikkeellelaskija on *Satoshi Nakamoto*, mikä on peitenimi ja kuuluu jollekin anonyyminä pysyttelevälle henkilölle tai ryhmälle. *Nakamoton* henkilöllisyyttä on pyritty selvittämään vuosien ajan ja jäljet ovat jossain vaiheessa johtaneet Suomeenkin, mutta useista ponnisteluista huolimatta *Nakamoton* henkilöllisyyttä tai henkilöllisyyksiä ei ole kyetty selvittämään.[48]

Bitcoinin perustuessa jo edellä esiteltyyn avoimeen lähdekoodiin sekä hajautettuun lohkoketjuteknologiaan, ei millään valtiolla tai keskuspankilla ole siihen valtaa, eivätkä ne voi hallita sitä. Bitcoinin käyttöön ei tarvita myöskään mitään erillisiä lupia, eikä kukaan ole voinut ainakaan teknologisesti puuttua bitcoin-siirtoihin.[49] Väitetään, että bitcoin on perustettukin tarkoituksin vähentää valtioiden ja pankkien valtaa talous- ja rahapolitiikassa ja samaan aikaan vastustaa niiden harjoittamaa finanssipolitiikkaa ja tämän myös *Satoshi Nakamoto* on omissa viesteissään vahvistanut. [50]

Bitcoinin arvo perustuu täysin kysynnälle ja tarjonnalle, eikä sen arvoa ole sidottu esimerkiksi minkään valtion valuuttaan tai kultakantaan. Valuuttana bitcoin on saanut osakseen arvostelua myös sen takia, että sen määrää on rajoitettu. Nykyistä kapitalistista järjestelmää suojaa maltillinen inflaatio, minkä ansiosta rahan arvo ei kasva kasvamistaan ja toimijoilla on kannustin tehdä investointeja heti, eikä lykätä niitä odottamaan rahan arvon nousua. [51] Bitcoinin ja yleisemminkin lohkoketjun vaikutuksista kapitalistiseen järjestelmään pidemmällä tähtäimellä on myös tehty tutkimusta ja osa ennustaa, että mikäli lohkoketjuteknologia omaksutaan laajemmin käyttöön, tulisi se myös vähentämään tarvetta talouspolitiikalle ja

[48] Ks. Mtv-uutiset, 7.11.2021.Nakamoton nimissä on virtuaalivaluuttalompakko, jossa on arvioitu olevan yli miljoona bitcoinia. Mikäli nämä varat vapautettaisiin, voisi sillä olla yllättävänkin laajoja vaikutuksia koko maailmantalouteen.
[49] Hautamäki ym., 2019, s. 3.
[50] Frisby, 2014, prologi.
[51] Hautamäki ym., 2019, s. 6.

valtion finanssipoliittisille toimille.[52] Tällä hetkellä bitcoin nähdään yleisimmin lähinnä spekulatiivisena sijoituskohteena, eikä merkkejä ole siitä, että sen käyttöä oltaisiin ainakaan viranomaisten toimesta laajentamassa. Mikäli bitcoin nousisi yleisesti käytettäväksi valuutaksi, tulisi sitä ennen ratkoa monta ongelmaa, kuten louhimisen aiheuttamat negatiiviset ilmastovaikutukset, bitcoinien rajattu määrä sekä ylipäätään se, että useimmilla ihmisillä tulisi hyväksyä ja omaksua bitcoin omaan käyttöönsä.[53]

Bitcoin oli ensimmäinen lohkoketjuteknologiaa hyödyntävä sovellutus ja se määritteli käytännössä koko virtuaalivaluuttakentän lähtökohdan. Vuonna 2013 Vitalik Buterin[54] julkaisi artikkelin, jossa hän esitteli uuden, toimivamman lohkoketjusovellutuksen; ethereumin. Julkaisun jälkeen joukko sijoittajia lähti mukaan luomaan ethereumia. Ethereumia ei luotu pelkästään virtuaalivaluutaksi, vaan alun perin sen tarkoituksena oli toimia alustana jo edellä mainituille älykkäille sopimuksille.[55] Ethereum on siis lyhyesti avoimeen lähdekoodiin ja hajautettuun järjestelmään perustuva tietojenkäsittely-ympäristö.[56]

Vaikka ethereum onkin pohjimmiltaan palvelualusta, jonka avulla mahdollistetaan lohkoketjuteknologian avulla esimerkiksi algoritmien suorittaminen ja kehittäminen, tarvitsee se kuitenkin resurssikseen virtuaalivaluutan, etherin (ETH).[57] Virtuaalivaluutta on välttämätön, jotta käyttäjillä olisi kannuste ylläpitää ethereumin taustalla olevaa lohkoketjua, mutta se ei ole ethereumin tarkoitus, vaan lähinnä sisäinen resurssi.[58] Tällä hetkellä ethereumia käytetään enimmäkseen sijoitusvarallisuutena, mutta sen pohjalle ollaan jatkuvasti kehittelemässä uusia teknologioita ja innovaatioita, uusimpana tulokkaana niin sanotut NFT:t. [59]

Koronaviruspandemian vaikutuksia bitcoinin ja ethereumin arvoon on tutkittu ja tultu sen kaltaisiin lopputuloksiin, että niiden kurssit eivät olleet niin herkkiä pandemian eri vaiheille,

[52] Ks. lisää Berg ym., 2020. Tutkimuksen ennuste oli, että lohkoketjujen omaksuminen voi aiheuttaa taloudellisen järjestelmämme muutoksen vähemmän hierarkkiseksi, kun valuutat toimivat keskitetyn järjestelmän sijaan tasavertaisissa, hajautuneissa järjestelmissä.
[53] Hautamäki ym., 2019, s. 7.
[54] Vitalik Buter on 27-vuotias kanadalais-venäläinen ohjelmoija, joka oli Ethereumin lisäksi perustamassa myös Bitcoin Magazine-lehteä.
[55] Rantala, 2018, s. 49.
[56] Rantala, 2018, s. 49.
[57] Rantala, 2018, s. 49.
[58] Rantala, 2018, s. 49.
[59] Ethereum-ympäsristössä toimiviin älykkäisiin sopimuksiin pohjautuu esim. vuonna 2021 pinnalle nousseet NFT:t (Non-Fungible-Token), joiden avulla voidaan todentaa jonkin digitaalisen rahakkeen tai vaikka taideteoksen omistaja. NFT:t on julkisessa keskustelussa nähty ainakin toistaiseksi lähinnä spekulatiivisena sijoituskohteena, ks. lisää Wang ym., 2021.

kuin esimerkiksi eri valtioiden indeksit olivat. Huomattiin myös, että bitcoinin kurssi ennusti vahvasti muiden virtuaalivaluuttojen, kuten ethereumin arvonmuutoksia.[60] Rikollisten toimijoiden ja myös tämän tutkimuksen kannalta bitcoin ja ethereum ovat olennaisimmat yleisesti käytössä olevat virtuaalivaluutat, sillä niiden vaihdanta- ja käyttökelpoisuus on ainakin vielä toistaiseksi paras verrattuna muihin virtuaalivaluuttoihin.[61]

2.2.2 Proof-of-Work ja Proof-of-Stake

Aikaisemmin on konsensusprotokollista puhuttaessa jo avattu niiden toimintaa. Bitcoin ja ethereum valikoituivat tutkielmassa käsiteltäviksi virtuaalivaluutoiksi myös siksi, että niiden taustalla olevat teknologiat perustuvat kahdelle hieman erilaiselle tekniikalle tai käyttötarkoitukselle. Proof-of-Work (PoW) on konsensusprotokolla, jossa lohkoketjun ylläpito vaatii varmentamista, jossa hajautetun verkoston koneet hyväksyvät kollektiivisesti muutoksia lohkoketjun tietokantaan tai tilikirjaan. [62] PoW-verkkoa on arvosteltu sen kuluttamasta energiamäärästä ja hitaudesta.

Toinen käytössä oleva konsensusprotokolla on ns. Proof-of-Stake-protokolla (PoS), joka toimii ethereumissa varmennusprosessina, jossa käyttäjät voivat ”äänestää” seuraavasta ketjuun tulevasta lohkosta ja kunkin äänen painoarvo on riippuvainen kyseisenen äänen resurssitalletuksesta.[63] Ethereumissa tämä resurssitalletus on ether ja jokaisella ethereitä omistavalla on mahdollisuus luoda lohkoketjussa transaktio, jossa tietty määrä ethereitä vahvistaa jonkin tiedon tallentamisen pysyvästi lohkoketjuun.[64] PoS on PoWiin verrattuna huomattavasti energiatehokkaampi, eikä se ole myöskään niin altis väärinkäytöksille. PoS-protokollan ajatellaankin yleisesti tulevan olemaan valtavirtaa etenkin uusia virtuaaluvaluuttoja kehitettäessä.

2.2.3 Initial coin offering (ICO)

ICO:lla (Initial coin offering) tarkoitetaan sitä, kun esimerkiksi start-up-yrittäjä tarjoaa uutta virtuaalivaluuttaa vastineeksi siitä rahoituksesta, jota lähdetään hakemaan muilta kuluttajilta ja

60 Ks. laajemmin; Marobhe, M.I. (2021), Cryptocurrency as a safe haven for investment portfolios amid COVID-19 panic cases of Bitcoin, Ethereum and Litecoin.
61 Diaz ym., 2022, s. 1.
62 Rantala, 2018, s. 45.
63 Rantala, 2018, s. 51.
64 Rantala, 2018, s. 51.

yrityksiltä. ICO:a voidaankin pitää vastineena perinteisille pääomasijoituksille.[65] Lohkoketjuteknologian hajautuneen luonteen seurauksena rahoitusta voidaan kerätä nopeasti ja helposti ympäri maailmaa.[66] ICO:n kautta liikkeelle lasketuille virtuaalivaluutoille on ominaista, että niiden ominaisuudet voivat vaihdella, mutta karkeasti ne voidaan jakaa kolmeen tyyppiin, joita ovat maksuvälineen kaltaiset virtuaalivaluutat, tietyn hyödykkeen maksamiseen käyvät virtuaalivaluutat (utility coin) ja rahoitusvälineiksi luettavat virtuaalivaluutat.[67] Edellä esitellyt bitcoin ja ethereum luetaan maksuvälineen kaltaisiin virtuaalivaluuttoihin. ICO:n on ajateltu olevan tietynlainen seuraava askel perinteisestä IPO:sta (Initial public offering), eli yritysten järjestämistä listautumisanneista.[68] Tässä vertauksessa on nähtävissä tietynlaista samankaltaisuutta, kuin virtuaalivaluutoista ja fiat-valuutoista puhuttaessa. Suomessa kuitenkin esimerkiksi Finanssivalvonta on varoittanut yleisesti niin kryptovaluuttojen, kuin ICOjenkin olevan riskialttiita sijoituskohteita niiden sääntelemättömyyden, pääoman menettämisriskin, voimakkaan hinnanvaihtelun[69], riittämättömän informoinnin ja teknologiariskin takia.[70] Finanssivalvonnan suositus perustuu suoraan Euroopan arvopaperimarkkinaviranomaisen ESMAn vuonna 2017 julkaisemaan lehdistötiedotteeseen.[71]

2.2.4 Mixer-palvelut anonymiteetin vahvistajana

Virtuaalivaluuttojen rikollisen käyttöpotentiaalin näkökulmasta olennainen ilmiö on ns. mixer-palvelut. Bitcoinin siirroista ja liikkeistä jää aina pysyviä jälkiä lohkoketjuun ja teknologian kehittyessä myös viranomaisilla on ollut mahdollisuus purkaa virtuaalivaluuttojen käyttäjän anonymiteettiä seuraamalla näitä liikkeitä esimerkiksi jonkin rinnakkaisen tietokannan avulla.[72] Mixer- tai sekoitinpalvelut pyrkivät poistamaan tämän ongelman siten, että virtuaalivaluutan käyttäjä maksaa pienen summan siitä, että sekoitinpalvelun ylläpitäjä ”sekoittaa” useiden käyttäjien virtuaalivaluuttakolikkoja ja palauttaa palvelun käyttäjälle valuuttaa, joka alun perin

[65] Howell ym., 2019, s. 1.
[66] Brochado – Troilo, 2021, s. 113.
[67] Finanssivalvonta. Mitä tarkoittaa virtuaalivaluutta, kryptovaluutta, kryptovara, ICO tai lompakkopalvelu?, 17.10.2019.
[68] Mohammad ym., 2020, s. 762.
[69] Virtuaalivaluuttojen voimakkaan arvonvaihtelun vastapainoksi on luotu myös ns. stablecoineja, eli virtuaalivaluuttoja, joiden arvo on sidottu aina johonkin tiettyyn kohteeseen, kuten kiinteään omaisuuteen tai fiat-valuuttaan, ks. Finanssivalvonta. Mitä tarkoittaa virtuaalivaluutta, kryptovaluutta, kryptovara, ICO tai lompakkopalvelu? , 17.10.2019.
[70] Finanssivalvonta, lehdistötiedote 22.11.2017. Finanssivalvonnan varoitus: kryptovaluutat ja ICO:t (Initial Coin Offering) riskialttiita sijoituskohteita.
[71] Ks. European Securities and Markets Authority, Press release, 13.11.2017. ESMA highlights ICO risks for investors and firms.
[72] Ks. esim. Silkkitie, kappale 2.3.2.

on kuulunut toiselle henkilölle.[73] Mixer-palvelut eivät ole niiden käyttäjillekään täysin riskittömiä ja onkin jo ilmennyt useita tapauksia, joissa sekoitinpalvelun tarjoaja on vain yksinkertaisesti jättänyt palauttamatta virtuaalivaroja käyttäjille ja kadonneet jäljettömiin.[74]

On ilmeistä, että mixer-palveluiden tarkoituksena on häivyttää varojen alkuperää ja niitä käytetään niin rahanpesuun, kuin muuhunkin rikolliseen toimintaan. Suomessa esimerkiksi julkisuudessa olleessa *Vastaamon tietovuototapauksessa* rikolliset kiristivät uhreja ja pyysivät lähettämään lunnasrahat heille bitcoineina. Viranomaiset ovat päässeet tekijöiden jäljille seuraamalla bitcoinien liikkeitä, mutta törmänneet siihen, että kiristäjät ovat häivyttäneet varoja mixer-palveluiden avulla. Ainakaan toistaiseksi tekijöitä ei ole saatu kiinni.[75] Kansainvälisesti ja myös Suomessa mixer-palvelut on tunnistettu rahanpesun ja terrorismin rahoittamisen näkökulmasta hyvin riskialtteiksi palveluiksi, josta jäljempänä lisää.

2.3. Virtuaalivaluuttojen nykyinen oikeudellinen asema

Lohkoketjuteknologian ja virtuaalivaluuttojen hyödyntämistä laajemmin pohdittaessa yksi keskeisimpiä ratkaistavia ongelmia on niiden mukanaan tuomat sääntelyyn liittyvät haasteet. Lohkoketjuteknologia kehittyy huimaa vauhtia ja uusia virtuaalivaluuttoja ja myös niiden käyttökohteita tulee jatkuvasti uusia. Lainsäädännöllä taas on tapana laahata hieman teknologian kehityksestä jäljessä ja lainsäätäjän kannalta on haastavaa, jos vasta valmisteilla olevat hankkeet vaatisivat jo päivittämistä. Lohkoketjuteknologiaa on tämän lisäksi haastava ymmärtää, mikä tekee lainsäädäntöhankkeiden läpiviemisestä entistä hankalampaa. Useat valtiot ovat vasta viime aikoina heränneet virtuaalivaluuttojen ja sen taustalla olevan lohkoketjuteknologian sääntelytarpeisiin.

Pelkona lohkoketjuteknologiaa rehelliseen liiketoimintaan ja tuotekehitykseen käyttävillä toimijoilla on se, että asiasta vielä tietämättömät päättäjät luovat lainsäädäntöä, mikä hankaloittaa teknologian ja uusien innovaatioiden kehittymistä. Esimerkkinä tästä on Suomessa Verohallinto, joka muutama vuosi sitten linjasi, että virtuaalivaluutoilla tehdyt tuotot ovat verotettavaa tuloa, mutta mahdollisesti syntyviä tappioita taas ei ollut mahdollista vähentää verotuksessa.[76] Pian tämän jälkeen huomattiin, että kyse oli ainoastaan yhden viranomaisen

[73] Wronka, 2022, s. 87.
[74] Wronka, 2022, s. 87.
[75] Ilta-Sanomat, 18.11.2020. Bitcoinien liikkeet voivat paljastaa Vastaamo-kiristäjän – näin rahan liikkeitä seurataan.
[76] Verohallinto vertasi vanhassa ohjeessaan Virtuaalivaluuttojen tuloverotuksesta A83/200/2013 virtuaalivaluutoista aiheutuneita tappioita pelaamisessa menetettyihin varoihin, joita voidaan pitää

näkemyksestä ja korkein hallinto-oikeus linjasikin päätöksessään KHO 2019:42, että virtuaalivaluutan myynnistä saatava voitto on katsottava omaisuuden luovutusvoitoksi ja kumosi keskusverolautakunnan päätöksen.[77] Verohallinnon näkemys asiasta siis oli väärä ja luovutustappiot ovat tämän hetken voimassa olevan oikeuden mukaan vähennyskelpoisia. [78] Suomessa virtuaalivaluuttojen sääntelyssä lähdettiin liikkeelle tuomalla virtuaalivaluuttojen tarjoajat samojen sääntöjen ja velvoitteiden piiriin, kuin muutkin finanssialan toimijat. Lakia on jo sen uutuudesta huolimatta jouduttu muutamaan otteeseen päivittämään, kun EU-tasolla on yhä vahvemmin haluttu lähteä harmonisoimaan jäsenvaltioiden lainsäädäntöjä virtuaalivaluuttoihin liittyen.

2.3.1. Laki virtuaalivaluutan tarjoajista

Laki virtuaalivaluutan tarjoajista (572/2019) (jäljempänä virtuaalivaluuttalaki) säädettiin Suomessa 26. huhtikuuta vuonna 2019. Lakia sovelletaan sen 1 §:n mukaan virtuaalivaluutan tarjoajien harjoittamaan liiketoimintaan. Lain taustalla on Euroopan unionin kesäkuussa 2018 julkaisema viides rahanpesudirektiivi, jonka yhtenä tarkoituksena oli estää virtuaalivaluuttojen avulla toteutettavaa rahanpesua ja terrorismin rahoittamista EU:n alueella.

Virtuaalivaluuttalaki ei sääntele tarkemmin itse virtuaalivaluuttoja, vaan siinä säännellään nimensä mukaisesti virtuaalivaluutan tarjoajia ja heidän harjoittamaansa virtuaalivaluuttatoimintaa. Suomessa kaikilla virtuaalivaluutan tarjoajilla on rekisteröidyttävä Finanssivalvonnan ylläpitämään rekisteriin. Tällä hetkellä rekisterissä on 6 virtuaalivaluutan tarjoajaa.[79]

Virtuaalivaluuttojen moninaisuuden vuoksi niiden määritteleminen lainsäädännössä on ollut jokseenkin haastava tehtävä. Virtuaalivaluuttalaissa olevasta virtuaalivaluutan määritelmästä

---

harrastustoimintaan liittyvinä elantomenoina, eivätkä ne siis olisi TVL 31 §:n 4 momentin mukaan verotuksessa vähennyskelpoisia.

[77] KHO:n tapauksessa oli kyse ethereum-virtuaalivaluutan verotuksesta ja päätöksen perusteluissa todetaan, että ”Ether-virtuaalivaluutta ei ole virallista valuuttaa. Ether-virtuaalivaluutalla on kuitenkin rahassa mitattavaa arvoa ja virtuaalivaluutta on siten sellaista varallisuutta, jota varallisuusverolain nolaja olisi voitu pitää verotettavana varallisuutena ja jota ei siten ole jätettävä tuloverolaissa tarkoitetun omaisuuden alan ulkopuolelle.”

[78] Ks. Verohallinnon ohje Virtuaalivaluuttojen verotus 22.1.2020 dnr VH/5083/00.01.00/2019.

[79] Rekisteröityneet virtuaalivaluutan tarjoajat voi tarkastaa osoitteesta https://www.finanssivalvonta.fi/rekisterit/valvottavaluettelo/ . 17.12.2021 katsottuna rekisteröityneet yhtiöt ovat Coinmotion Oy, LocalBitcoins Oy, NordXE Oy, Northcrypto Oy, Prasos Cash Management Oy ja Tesseract Group Oy.

käy ilmi se, miten lainsäädäntömme suhtautuu virtuaalivaluuttoihin ja minkälaisena hyödykkeenä sitä pidetään. Virtuaalivaluuttalain 2 §:n 1 momentin mukaan;

> *virtuaalivaluutalla tarkoitetaan digitaalisessa muodossa olevaa arvoa,*
> *a) jota keskuspankki tai muu viranomainen ei ole laskenut liikkeeseen ja joka ei ole laillinen maksuväline,*
> *b) jota henkilö voi käyttää maksuvälineenä ja*
> *c) joka voidaan siirtää, tallentaa ja vaihtaa sähköisesti.*

Kyseisestä määritelmästä käy ensimmäiseksi ilmi se, että virtuaalivaluuttaa ei tämän lain soveltamisalalla voi siis olla mikään keskuspankin tai muun viranomaisen liikkeelle laskema virtuaalivaluutta.[80] Tämä on lain soveltamisalalle merkittävä rajaus huomioon ottaen, että useat valtiot ja keskuspankit ovat jo alkaneet valmistella ja kehittää omia virtuaalivaluuttojaan.[81]

Toinen huomionarvoinen asia määritelmässä on se, että virtuaalivaluuttaa ei pidetä laillisena maksuvälineenä.[82] Virtuaalivaluuttalain hallituksen esityksen HE 167/2018 mukaan laillisella *maksuvälineellä tarkoitetaan maksuvälinettä, joka velkojan on vastaanotettava, jos maksuvälineestä ei ole velkojan ja velallisen välillä muuta sovittu*. Hallituksen esityksessä todetaan myös, että Euroopan unionin toiminnasta tehdyn sopimuksen 128 artiklan mukaisesti ainoastaan EKP:n ja kansallisten keskuspankkien liikkeeseen laskemat setelit ovat laillisina maksuvälineinä kelpaavia seteleitä unionissa.[83] Jäsenvaltiot voivat laskea liikkeeseen eurometallirahoja, kun ovat ensin saaneet siihen EKP:ltä hyväksynnän. Virtuaalivaluutta on hallituksen esityksen mukaisesti luonteeltaan hyödyke.[84]

Kolmantena määritelmän osana on mainittu se, että ollakseen virtuaalivaluuttaa, tulisi sitä voida käyttää maksuvälineenä. Toisen ja kolmannen määritelmän välillä on selkeästi ristiriitaa, kun virtuaalivaluutalta edellytetään samaan aikaan kykyä toimia maksuvälineenä, mutta samaan aikaan se ei saa olla laillinen sellainen. Esimerkkejä virtuaalivaluutan käytöstä maksuvälineenä kuitenkin jo on, kun esimerkiksi autovalmistaja Tesla hyväksyi bitcoinit maksuvälineeksi keväällä 2021, joskin tilanne on tuon jälkeen ollut hieman epäselvä. [85]

[80] Hautamäki, 2019, s. 32.
[81] Alkuinnostuksen laantumisen jälkeen vaikuttaa siltä, että valtioiden mahdolliset omat virtuaalivaluutat tulisivat olemaan käytännössä kuin fiat-valuuttaa, mutta vain digitaalisessa muodossa.
[82] Hautamäki, 2019, s. 32.
[83] EUVL, N:o C 326/47, 26.10.2012.
[84] Hautamäki, 2019, s. 32.
[85] Kesällä 2021 Tesla kertoi hyväksyvänsä bitcoinit maksuvälineeksi uudestaan sen jälkeen, kun niiden louhinta on muuttunut ympäristöystävällisemmäksi, ks. Mtv-uutiset, 14.06.2021.

Neljäntenä ehtona se, että virtuaalivaluuttaa tulee voida siirtää, tallentaa ja vaihtaa sähköisesti. Tämä siis tarkoittaa sitä, että virtuaalivaluutan ollessa digitaalisessa muodossa oleva hyödyke, voidaan sitä sähköisesti siirtää, vaihtaa ja tallentaa. Tässä tapauksessa myös esimerkiksi virtuaalivaluutan vaihtaminen kultaan kuuluisi lain soveltamisalaan. Virtuaalivaluuttalain hallituksen esityksessä todetaan, että kansallisen rahanpesun ja terrorismin rahoittamisen torjunnan riskiarvion mukaan virtuaalivaluuttoihin liittyy Suomessa korkea rahanpesun ja terrorismin rahoittamisen riski, joten sitä kannattaa pyrkiä estämään laajentamalla määritelmä mahdollisimman monenlaisiin palveluihin. [86]

Virtuaalivaluuttalain tarpeellisuutta perusteltiin sen hallituksen esityksessä HE 167/2018 virtuaalivaluuttoihin liittyvillä riskeillä. Näitä riskejä ovat mm. valuutan arvojen voimakkaat heilahtelut, henkilöllisyyden väärinkäytökset ja valuuttaan kohdistuvat varkaudet. Tämän lisäksi virtuaalivaluutan käyttöön liittyy vahvasti jo edellä mainittu riski valuutan käytöstä rahanpesuun tai terrorismin rahoittamiseen sekä riski siitä, että koko virtuaalivaluuttojen alustan tarjonnut yritys tai yhteisö katoaa ja vie käyttäjien rahat mukanaan. Virtuaalivaluuttojen arvo on myös hallituksen esityksen mukaan altis manipulaatiolle. [87]

Edellä on jo sivuttu syitä sille, miksi EU:ssa ja kansainvälisesti laajemminkin on haluttu lähteä sääntelemään virtuaalivaluuttoja ja niiden käyttöä. Lainsäädännöllä pyritään yleisesti luomaan vakautta ja varmuutta yhteiskuntaan ja myös finanssimarkkinoille. Sääntely vähentää yritysten transaktiokustannuksia, kun ne voivat luottaa muiden toimivan lainsäädännön edellyttämällä tavalla.[88] Virtuaalivaluuttojen kohdalla tämä tarkoittaa sitä, että toimittajat voivat esimerkiksi luottaa siihen, että virtuaalivaluutan tarjoajat täyttävät ne toiminnan vähimmäisvaatimukset, joista on laissa säädetty. Virtuaalivaluuttalailla pyritään myös erityisesti estämään rahanpesua ja terrorismin rahoittamista. Kaikkien joutuessa noudattamaan samoja sääntöjä, palveluntarjoajilla ei myöskään ole houkutusta pyrkiä saamaan kilpailuetua toimimalla moitittavaksi katsottavalla tavalla. Sääntelyn puute voi pahimmillaan mahdollistaa vapaasti sellaisen toiminnan harjoittamisen, mikä normaalisti katsottaisiin rikolliseksi. [89]

[86] HE 167/2018, s. 84.
[87] HE 167/2018, s. 44-45.
[88] Hautamäki, 2019, s. 13.
[89] Suomessa esim. Verohallinto on linjannut, että virtuaalivaluuttoina pidetään kaikkia sellaisia virtuaalivaluuttalain määritelmän täyttäviä virtuaalivaluuttoja, joilla ei ole virallisen valuutan asemaa. Tähän ei vaikuta se, onko esimerkiksi virtuaalivaluutan arvo sidottu johonkin viralliseen valuuttaan. Ks, Verohallinto, 2020, 1.1. Yleistä virtuaalivaluuttojen luonteesta.

Virtuaalivaluuttalain tarkoituksena ei ole ollut pyrkiä estämään virtuaalivaluuttojen käyttöä tai rampauttamaan niitä, vaan lisäämään niitä käyttävien henkilöiden oikeussuojaa ja ehkäistä talousrikoksia ja niihin liittyviä riskejä. Lait tuovat uudelle alalle myös tietynlaista uskottavuutta ja se on myös virtuaalivaluuttojen tarjoajien etu, kun käyttäjäkunta tämän myötä laajenee.[90]

2.3.2. Suomalaista oikeuskäytäntöä – Postihuumetapaukset ja Silkkitie-takavarikko

Virtuaalivaluutoista ei vielä 2010-luvun lopulla ollut olemassa paljoakaan suomalaista oikeuskäytäntöä tai korkeimman oikeuden ennakkopäätöksiä. Ensimmäiset KKO:n antamat päätökset olivat ns. postihuumetapauksia, joissa vastaajat olivat virtuaalivaluuttaa käyttäen tilanneet huumausaineita TOR-verkossa olevasta Silkkitie-kauppapaikasta. Silkkitie toimi vuodesta 2013 lähtien ns. pimeässä verkossa ja kauppaa siellä tehtiin nimimerkkien avulla. Kun Tulli takavarikoi Silkkitie-palvelimen vuonna 2019[91], tuli esitutkintaan tuhansia epäilyjä huumausainerikoksista, joissa maksuna oltiin käytetty virtuaalivaluuttoja, lähinnä bitcoineja. [92]

Edellä mainitut postihuumetapaukset ovat vuosilta 2019 ja 2018 (KKO 2019:2 ja KKO 2018:3) ja niissä on arvioitu muun muassa sitä, voidaanko virtuaalivaluutan hankkimista yhdistää arviointiin epäillyn syyllisyyden todennäköisyydestä. Virtuaalivaluutat ja niiden käyttö on yleensä yhdistetty vahvasti rikolliseen toimintaan ja yksinään niiden hankintaa on joidenkin mielissä voitu pitää epäilyttävänä toimintana. Näin on osittain tapahtunut myös mainituissa korkeimman oikeuden ennakkoratkaisuissa. Toisessa ratkaisussa KKO 2018:3 syyte hylättiin, sillä järkevää epäilyä postilähetyksen vastaanottajan syyllistymisestä huumausainerikokseen ei voitu sulkea pois. Molemmissa tapauksissa vastaajien omien kertomusten arviointi on ollut keskeisessä roolissa.[93]

---

[90] Hautamäki, 2019, s. 15.
[91] Ks. Iltalehti, 4.12.2019.
[92] Yle-uutiset, 16.11.2020. Poliisi oli eritellyt palvelimelta yli 7500 suomalaisille henkilöille kuuluvaa nimimerkkiä, joilla oltiin tilattu huumausaineita Silkkitieltä. KRP:n mukaan asiassa kirjattiin lopulta noin 3000 rikosilmoitusta, joista noin 2000 päätyi syyteharkintaan. Ylen uutisessa kerrotaan, että epäiltynä on henkilöitä koko Suomen alueelta ja eri koulutus- ja ammattitaustoista. Syrjäseuduilla huumeita voi myös olla hankalaa saada haltuun perinteisin keinoin ja internet on koettu siellä tehokkaaksi kanavaksi huumeostoihin. Anonyymi, nimimerkin takaa suoritettu tilaus on myös voitu kokea houkuttavaksi tavaksi kokeilla huumausaineita, vaikka niitä ei muuten olisi ehkä tullut hankittua.
[93] Riekkinen, 2020, s. 998.

Tapauksessa KKO 2019:2 A:ta syytettiin käräjäoikeudessa huumausaineen käyttörikoksesta, sekä huumausainerikoksesta sillä perusteella, että hän oli tuonut maahan huumausainetta. Hänen kotiosoitteeseensa oli tullut kirjelähetys ulkomailta, joka oli sisältänyt 250 kappaletta 25C- NBOMe-huumausainetta sisältäviä lappuja. A kiisti tilanneensa kyseistä lähetystä tai edes tietävänsä siitä mitään. Käräjäoikeuden mukaan oikeuskäytännössä on pidetty yleisesti epäuskottavana sitä, että henkilö tekisi huumausainetilauksen omalla nimellään omaan kotiosoitteensa ilman, että olisi tästä lainkaan tietoinen. Käräjäoikeus ei myöskään pitänyt A:n omaa kertomusta ylipäätään uskottavana.

Käräjäoikeuden perusteluissa todettiin, että A:n harjoittama maksuliikenne virtuaalivaluuttaa välittävän yhtiön kanssa tuki syytettä. Myös A:n myöntämä huumausaineen käyttörikos kolme kuukautta huumausainelappujen maahantuonnin jälkeen tuki sitä, että A on itse tilannut huumausaineet internetistä. A:n syyllisyydestä ei näin käräjäoikeuden mukaan jäänyt varteenotettavaa epäilyä, joten A:n katsottiin syyllistyneen huumausainerikokseen. A valitti hovioikeuteen, mutta hovioikeus hylkäsi valituksen.[94]

A valitti hovioikeuden päätöksen jälkeen vielä korkeimpaan oikeuteen, jossa siis oli kyse siitä, onko A:n näytetty tuoneen maahan huumausainetta tilaamalla postitse jo edellä mainittuja huumausainelappuja. Päätöksen perustelujen 9. kohdassa KKO toteaa, että se on ennakkopäätöksessään KKO 2018:3 katsonut, että postilähetyksen vastaanottajamerkinnällä on merkittävä näyttöarvo sen osoittamisessa, kuka lähetyksen on tilannut. Lähtökohtaiseen todennäköisyyteen nojautuva näyttö ei kuitenkaan KKO:n mukaan voi riittää yksinään osoittamaan henkilön syyllistyneen kiellettyjen aineiden maahantuontiin. Syyttäjän on tästä syystä kyettävä esittämään myös muita todisteita syyllisyydestä.

Ratkaisun kohdassa 12 KKO toteaa, että asiassa esitetty selvitys postilähetyksen vastaanottajan tiedoista ja vastaanottajan olosuhteista muodostaa sellaisen vahvan näytön, joka antaa perusteen edellyttää vastaajan konkretisoivan kiistämisen perusteet ja kertovan postilähetykseen liittyvistä olosuhteista. Ratkaisun kohdassa 13 KKO toteaa, että on ollut selvää ja riidatonta, että A:n pankkitilin ja virtuaalivaluuttaa välittävän yhtiön tilin välillä on ollut rahansiirtoja. 160 euron siirto on tehty kolme päivää ennen huumausaineen postittamista

[94] Käräjäoikeudessa näyttöä on arvioitu yllättävänkin ankarasti. Huomionarvoista on se, että käräjäoikeuden mukaan maksuliikenne virtuaalivaluuttaa välittävän yhtiön kanssa on tukenut syytettä, vaikka konkreettisia todisteita virtuaalivaluutan käytöstä rikoksessa ei suoranaisesti ollut.

Espanjasta. Tämä summa olisi KKO:n mukaan riidattomasti riittänyt kyseisen huumausaine-erän maksamiseen.

Perustelujen kohdassa 14 KKO toteaa, että on yleisesti tiedossa, että virtuaalivaluuttaa käytetään huumeiden hankkimiseen internetin kautta. Virtuaalivaluuttaa voidaan kuitenkin käyttää moniin muihinkin tarkoituksiin. Tällöin on selvää, ettei sitä yksinään voida käyttää todisteena rikokseen syyllistymiseen. Kun kuitenkin otetaan huomioon tilatun huumaisaine-erän arvo ja tilausajankohta, KKO katsoi, että virtuaalivaluutan käytöllä on syytettä tukeva merkitys näyttönä. Virtuaalivaluutan käyttämisen osalta KKO on käräjäoikeuden tuomion kanssa samoilla linjoilla.

A vetosi puolustuksessaan siihen, että rahojen säilyttäminen virtuaalivaluuttana oli kannattavampaa, kuin niiden pitäminen tavallisella tilillä. A:lla ei myöskään ollut enää tallessa tarkempia tietoja virtuaalivaluuttatilin käytöstä, sillä ne olivat hävinneet puhelimen vaihdon yhteydessä. KKO:n perustelujen mukaan tarina varojen kannattavammasta säilyttämisestä virtuaalivaluuttana ei ollut uskottava muun muassa siksi, että tilisiirrot kyseiselle yhtiölle ovat olleet melko vähäisiä.

Tapausta virtuaalivaluuttojen käytön näkökulmasta arvioitaessa on otettava huomioon, että virtuaalivaluuttalaki astui voimaan vasta päätöksen antamisen jälkeen. KKO ei ole ottanut tarkemmin kantaa virtuaalivaluuttojen kehitykseen tai yleistymiseen, mutta on selvää, että tällä hetkellä virtuaalivaluutan hankintaa tuskin enää voitaisi pitää yhtä vahvasti merkkinä liitynnästä rikolliseen toimintaan. Vaikka KKO ei ole perustanut tuomiotaan yksin virtuaalivaluutan hankkimiselle, on se kuitenkin ollut suhteellisen merkittävä osa syyllisyyttä arvioitaessa.

Jo edellä mainitusti kyseiseen tapaukseen liittyy olennaisesti myös toinen postihuumetapaus KKO 2018:3, jossa vastaaja vapautettiin syytteistä. Tapaukset ovat hyvin samankaltaisia ja merkittävimpänä erona voidaan todeta olevan juuri virtuaalivaluutan käyttöä koskeva näyttö.[95] Vaikka KKO:n ja käräjäoikeuden perusteluissa ei sitä suoraan ilmaista, voidaan näytön virtuaalivaluutan käytöstä kuitenkin todeta olleen merkittävässä asemassa, kun lopullista tuomiota on annettu. Tämän puolesta puhuu lähes muuten identtisessä tapauksessa annettu vapauttava päätös.

[95] Riekkinen, 2020, s. 1009.

Huomionarvoista on etenkin se, että KKO ei pitänyt uskottavana sitä, että A olisi hankkinut virtuaalivaluuttaa sijoitustarkoituksiin. Tällä hetkellä juuri sijoittaminen on yleisin syy hankkia virtuaalivaluuttaa. Tulevissa ennakkopäätöksissä KKO joutuu varmasti pohtimaan uudestaan virtuaalivaluutan käytön näyttöarvoa ja huomioimaan sen käytön ja omistamisen räjähdysmäisen kasvun viime vuosina. KKO:n päätöksillä on kuitenkin varmasti merkitystä esimerkiksi alun Silkkitie-tapauksia arvioitaessa. Syyte- ja tuomitsemiskynnys ylittyy yleensä, mikäli virtuaalivaluuttojen hankinta ja huumausaineiden ostot voidaan yhdistää epäiltyyn esimerkiksi osoitteen, puhelinnumeron tai vastaavan henkilötiedon avulla.[96]

[96] Allekirjoittanut on työskennellyt Syyttäjälaitoksella purkamassa mainittua Silkkitie-tapausten sumaa. Syytekynnyksen katsottiin vakiintuneesti ylittyvän, mikäli tietyillä virtuaalivaluutta-kolikoilla tehdyt ostot voitiin yksilöidä epäiltyyn ja siirrot ajallisesti sopivat tehtyihin huumausainetilauksiin. Mielenkiintoista oli se, että ”anonyymi” virtuaalivaluutan omistaja oltiin poliisin toimesta suoritetun esitutkinnan avulla saatu selvitettyä. Tiettyä bitcoin-erää oli mahdollista seurata sen mukana kulkevan kirjain-/numeroyhdistelmän avulla ja syyllisyyden osoittaminen vaati, että tekijä oli jossain vaiheessa tehnyt rahansiirtoja esimerkiksi omalta pankkitililtään tai ilmoittanut nimimerkin yhteydessä osoitteensa tai puhelinnumeronsa. ”Perinteisiin” huumausainerikoksiin verrattuna erikoista on, että itse huumausaineesta ei saatu muuta selvitystä, kuin Silkkitiellä toimivien myyjien myynti-ilmoituksissa mainitut tiedot tilatuista huumausaine-eristä. Keskustelua Syyttäjälaitoksella käytiin muun muassa siitä, kuinka luotettavana voidaan pitää esimerkiksi myyjän ilmoittamaa tietoa ”erittäin vahvasta amfetamiinista”. Yleinen näkemys oli, että syyllisyys huumausaineen tilaamiseen ja hallussapitoon täyttyy siinä vaiheessa, kun tekijä päättää tilata ilmoituksen mukaista tuotetta Silkkitieltä ja maksaa tilauksen odotuksin, että se toimitetaan hänelle. Syyttäjän vastuulla ei siis olisi tämän jälkeen todistaa esimerkiksi huumausaineen todellisia pitoisuuksia. Huumausaineiden lisäksi Silkkitieltä oltiin tilattu mm. dopingaineita, lääkkeitä ja aseita.

3. Rahanpesu ja terrorismin rahoittaminen

3.1 Kansainväliset sopimukset kriminalisointien taustalla

YK on ollut rahanpesun kansainvälisessä kriminalisoinnissa merkittävässä roolissa. Rahanpesun estäminen nousi kansainvälisen huomion keskipisteeseen vuonna 1988, kun YK laati ns. Wienin yleissopimuksen, jolla pyrittiin estämään huumausaineiden ja psykotrooppisten aineiden laitonta kauppaa. Tämä kehitys sai alkunsa Yhdysvalloista, jossa käytiin 80-luvulla ”sotaa huumausaineita vastaan”. [97] Kyseinen kansainvälinen sopimus oli ensimmäinen laatuaan, jossa määriteltiin rahanpesurikoksen tekomuodot ja velvoitettiin allekirjoittajamaita kriminalisoimaan rahanpesu sopimuksen edellyttämällä tavalla. [98] Wienin sopimus on ollut perustana sille, miten rahanpesua on sen jälkeen lähdetty määrittelemään niin kansainvälisessä, kuin kansallisessakin oikeudessa. Ensimmäinen eurooppalainen sopimus, jossa velvoitettiin sopimuksen jäsenvaltioita kriminalisoimaan rahanpesu, oli Euroopan neuvoston niin sanottu Strasbourgin konfiskaatiosopimus vuodelta 1990. Siinä myös määriteltiin ensimmäistä kertaa, EU-tasolla, minkälaisia tekoja voidaan pitää rahanpesuna. [99]

Vuonna 2000 YK:ssa laadittiin Kansainvälisen järjestäytyneen rikollisuuden vastainen sopimus, eli niin sanottu Palermon yleissopimus. Rahanpesun osalta sopimus eroaa Wienin yleissopimuksesta siinä, että se tunnisti rahanpesun omana rikostyyppinään, eikä edellyttänyt esirikoksena tehtävää huumausainerikosta. [100] Sopimusten joukkoon lisättiin New Yorkissa vuonna 1999 terrorismin rahoittamista koskeva yleissopimus. [101] Sopimuksessa kielletään varojen antaminen tai kerääminen siinä tarkoituksessa tai tietoisena siitä, että varoja käytetään joko kokonaan tai osittain sopimuksen soveltamisalaan kuuluvan terroristisen rikoksen tekemiseen. [102] Sopimuksen liitteessä on määritelty ne teot, joita voidaan pitää terrorismin rahoittamisena. Vuonna 2005 Euroopan neuvostossa hyväksyttiin uusi rikoshyötyihin kohdistuvaa rahanpesua, etsintää, takavarikointia ja konfiskaatiota koskeva sopimus. Tähän sopimukseen otettiin myöhemmin mukaan myös terrorismin rahoittaminen, mitä joudutti syyskuun 11. päivän terroriteot.[103]

[97] Ks. lisää, Sahavirta, 2008, s. 19-24.
[98] Hyttinen, 2021. s. 35.
[99] Hyttinen, 2021, s. 42.
[100] Hyttinen, 2021, s. 37.
[101] SopS 74/2002.
[102] Kimpimäki, 2015, s. 266.
[103] Kimpimäki, 2015, s. 340.

Rahoittamiskiellon soveltumisen ehtona on, että väkivallanteon tulee olla luonteeltaan ja asiayhteydeltään sellainen, että sen tarkoituksena on pelon aiheuttaminen väestön keskuudessa tai vaihtoehtoisesti hallituksen tai kansainvälisen järjestön pakottaminen johonkin tiettyyn toimenpiteeseen tai pidättäytyminen jostain toimenpiteestä.[104] Rahoittamisrikoksen täyttyminen edellyttää siis sitä, että varojen antamisen tai niiden keräämisen tarkoituksena on nimenomaisesti suorittaa jokin sopimuksessa mainittu terrorismirikos tai vähintään, että rahojen antaja tai kerääjä tiedostaa varojen menevän joko kokonaan tai osittain terrorismirikoksen tekemiseen. Sopimuksessa ei edellytetä sitä, että rikos olisi todellisuudessa ehtinyt toteutua, vaan jo valmistelutarkoitus riittää. Tätä yhteyttä teon ja tarkoituksen välillä on todellisuudessa usein hyvin hankala selvittää, sillä terroristijärjestöt usein saavat varoja monien välikäsien kautta ja niillä voi olla rikollisuuden lisäksi muitakin yhteiskunnallisia tavoitteita ja päämääriä.[105] Yhdysvalloissa esimerkiksi on käynyt ilmi tapaus, jossa rahoja välitettiinkin hyväntekeväisyysjärjestöjen sijaan terroristijärjestö Hamasille. [106]

Tämän tutkielman kannalta on olennaista, että Palermon yleissopimuksessa on kiinnitetty erityistä huomiota niihin varoihin, joita rikoksen tekemiseen käytetään ja niihin liittyviin varainsiirtoihin. Sopimus velvoittaa rahoituslaitokset ja muut varainsiirtojen kanssa tekemisissä olevat toimijat ryhtymään tehokkaisiin toimenpiteisiin asiakkaidensa tunnistamiseksi, epäilyttävien rahansiirtojen havaitsemiseksi ja niistä ilmoittamiseksi. Tämän lisäksi sopimus velvoittaa valtiot ryhtymään toimiin, jotta terrorismin rahoittamisrikoksen tekemiseen käytetyt tai osoitetut varat voidaan tunnistaa, havaita ja jäädyttää, jotta varojen takavarikointi ja menetetyksi tuomitseminen olisi mahdollista. Valtioiden tulee myös mm. harkita maksuja välittävien yhtiöiden valvontaan liittyviä toimenpiteitä, sillä pankkisektoriin kohdistuvat velvoitteet ovat hyödyttömiä, mikäli muita, epävirallisia, pankkitoimintoja on mahdollista harjoittaa ilman valvontaa. [107]

3.2 Rahanpesu

Rahanpesulla tarkoitetaan yksinkertaisimmillaan sitä tekoa tai tekokokonaisuutta, minkä tarkoituksena on peittää tai häivyttää rikoksen tuottaman hyödyn tai omaisuuden alkuperä. [108] Rahanpesulla rikolliset pyrkivät varmistamaan, että rikos todella kannattaa. Rahanpesua on

[104] Kimpimäki, 2015, 2. 266-267.
[105] Kimpimäki, 2015, s. 267.
[106] Ks. lisää, Kimpimäki, 2015, s.267-268.
[107] Kimpimäki, 2015, s.268-269.
[108] Hyttinen, 2021, s. 24.

todennäköisesti harjoitettu niin kauan, kun on ollut olemassa rikoksia, joista on saanut taloudellista hyötyä.[109] Suomessa rahanpesu on säädetty rangaistavaksi rikoslain 32 luvun 6 §:ssä. Sen mukaan, joka;

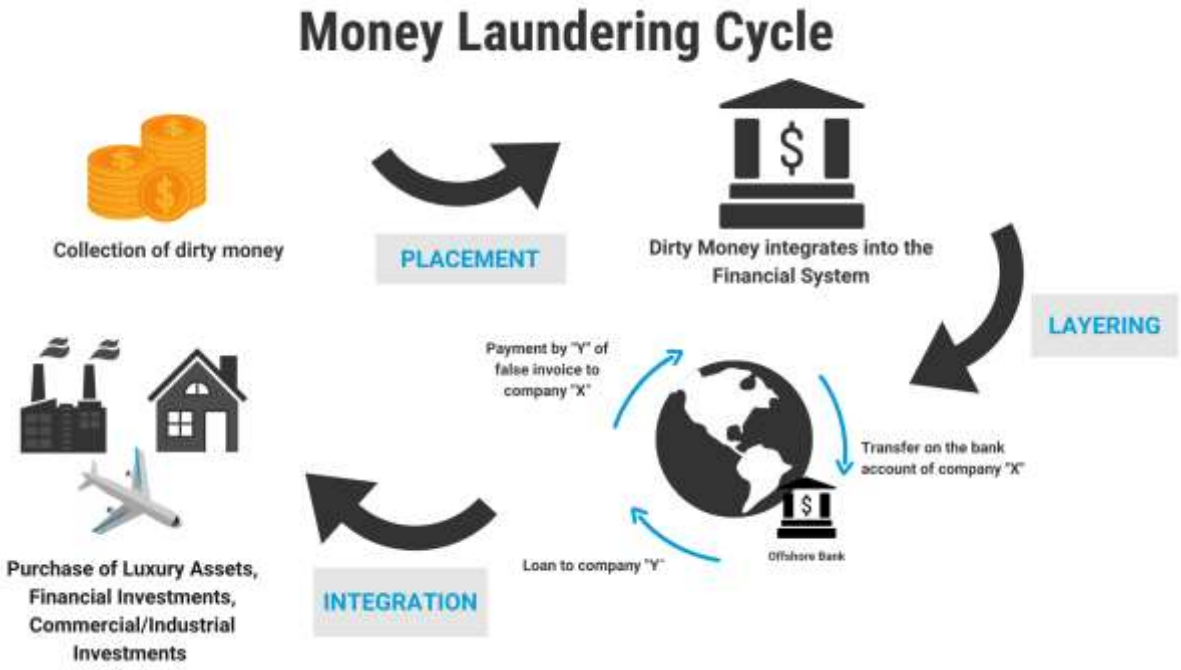
> *1) ottaa vastaan, käyttää, muuntaa, luovuttaa, siirtää, välittää tai pitää hallussaan rikoksella hankittua omaisuutta, rikoksen tuottamaa hyötyä tai näiden tilalle tullutta omaisuutta hankkiakseen itselleen tai toiselle hyötyä tai peittääkseen tai häivyttääkseen hyödyn tai omaisuuden laittoman alkuperän tai avustaakseen rikoksentekijää välttämään rikoksen oikeudelliset seuraamukset, taikka*
>
> *2) peittää tai häivyttää rikoksella hankitun omaisuuden, rikoksen tuottaman hyödyn taikka näiden tilalle tulleen omaisuuden todellisen luonteen, alkuperän, sijainnin tai siihen kohdistuvat määräämistoimet tai oikeudet taikka avustaa toista tällaisessa peittämisessä tai häivyttämisessä, on tuomittava rahanpesusta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.*
>
> *Yritys on rangaistava.*

Törkeässä tekomuodossa vaaditaan, että rikoksen kautta saatu omaisuus on ollut erittäin arvokas tai että rikos on tehty erityisen suunnitelmallisesti. Suomalaisen rikoslainsäädännön mukaan rahanpesemisellä siis tarkoitetaan niitä toimia, joiden tarkoituksena on rikoksella hankitun omaisuuden tai rikoksen tuottaman hyödyn siirtäminen lailliseen talousjärjestelmään siten, että varallisuus saadaan erotetuksi rikollisesta alkuperästä ja saadun varallisuuden saanto pystytään ainakin näennäisesti legitimoimaan.[110] Laajasti määriteltynä rahanpesemiseksi on voitu joskus lukea myös laillisesti hankitun omaisuuden laiton käyttö. Yleisimmin käytetään kuitenkin Wienin sopimuksen määritelmää, jonka mukaan rahan peseminen on omaisuuden muuntamista tai siirtämistä, joka tehdään tarkoituksin salata tai peittää omaisuuden laiton alkuperä tai avustaa esirikokseen syyllistynyttä välttämään tekojensa oikeudelliset seuraamukset. [111]

Rahanpesu on oikeustieteessä useimmiten nähty prosessina, jossa on kolme vaihetta. Ensimmäisessä vaiheessa likainen raha sijoitetaan lailliseen talousjärjestelmään (placement), toisessa vaiheessa likainen raha peitetään tai hävitetään (layering) ja kolmannessa vaiheessa puhdistettu raha integroidaan osaksi laillista taloutta (integration).[112] Koko prosessin tavoitteena on se, että rikoksen tekijä voi käyttää vapaasti sitä varallisuutta, jonka on ansainnut

[109] Hyttinen, 2021, s. 24.
[110] Sahavirta, 2008, s. 21.
[111] Sahavirta, 2008, s. 22.
[112] Ks. laajemmin, Sahavirta, 2008, s. 24-36.

esirikoksen tekemisellä. Rahanpesu on rikosoikeudellisesti kiinnostava rikos, sillä sen toteuttaminen vaatii aina myös esirikoksen toteuttamista. Rahanpesua on havainnollistettu YK:n internet-sivuilla seuraavalla kuviolla.



Rahanpesun vaiheet.[113]

Rahanpesun kriittisin vaihe on yleensä sijoittamisvaihe (placement), jossa tekijä joutuu tuomaan rikoksella ansaitut rahat laillisen talousjärjestelmän piiriin. Tämän johdosta rahanpesun sääntelyssä on aina pyritty erityisesti panostamaan preventiiviseen lainsäädäntöön, sillä se ehkäisee näitä rikoksia tehokkaimmin.[114] Yleisimpiä ja myös tehokkaimpia keinoja tässä ovat muun muassa pankkien velvollisuus tuntea asiakkaansa, sekä niiden velvollisuus tehdä tarvittaessa ilmoitus epäilyttävistä rahan liikkeistä. Nykyisin nämä rahanpesun ennaltaehkäisyyn pyrkivät säännökset velvoittavat monenlaisia toimijoita, kuten liikkeen- ja ammatinharjoittajia. [115]

Rahanpesun tarkoituksena on siis se, että rikollisilla toimilla ansaittua rahaa voitaisiin käyttää huoletta ilman pelkoa kiinnijäämisestä. Ennen rahanpesutoimia rikollisella toiminnalla saatujen rahojen arvo on reaalisesti vähäisempi kuin puhtaan rahan arvo, sillä sitä on vaikea sijoittaa

[113] United Nations, Office on Drugs and Crime. Money Laundering, https://www.unodc.org/unodc/en/money-laundering/overview.html .
[114] Hyttinen, 2021, s. 25.
[115] Hyttinen, 2021, s. 25.

tuottavasti tai tehdä sillä suuria hankintoja. Mikäli tavallinen palkansaaja omistaa esimerkiksi useita kalliita asuntoja, voi se herättää viranomaisten epätoivotun kiinnostuksen. [116]

Suomalainen rahanpesun rikosoikeudellinen sääntely perustuu jo edelläkin todetusti vahvasti kansainvälisiin velvoitteisiin. Rahanpesun on todettu olevan kansainvälisesti niin suuri uhka, että sitä on haluttu säädellä ylikansallisilla sopimuksilla. Etenkin järjestäytyneiden rikollisryhmien tekemistä rahanpesurikoksista on todettu olevan huomattavaa haittaa valtioiden lailliselle taloudelle, turvallisuudelle ja poliittisen järjestelmän toimivuudelle. [117] Rikollisella toiminnalla ansaitun rahan käyttämistä pyritäänkin jatkuvasti hankaloittamaan ja estämään niin lainsäädännöllisin, kuin yhteiskunnallisinkin keinoin. Fyysisen valuutan käytön väheneminen on helpottanut tätä työtä, sillä yksittäisten kolikoiden ja seteleiden alkuperää on hyvin hankala selvittää. Tilisiirroista ja vastaavista sähköisistä toimista jää aina jälki, joka on poliisilla jälkeenpäin helpommin selvitettävissä. Vaikka rahan käyttö on sähköistynyt merkittävästi, se ei ole kuitenkaan kyennyt estämään rahanpesua. Rikolliset ovatkin onnistuneet löytämään uusia keinoja, joista yksi on fyysisen rahan korvaaminen virtuaalivaluutoilla.[118]

YK:n alaisuudessa toimii huumeiden ja rikollisuuden torjunnasta vastaava toimisto (United Nations Office on Drugs and Crimes), joka tekee arvioita siitä, mikä on vuosittainen rikoshyödyn määrä maailmassa. Viimeisin tieto on, että vuosittaisesta kaikkien valtioiden yhteisestä bruttokansantuotteesta noin 2-5% on ansaittu rikollisella toiminnalla.[119] Rikoshyötyä on siis maailman vuosittaisessa talouskierrossa noin 1700-4300 miljardin dollarin edestä, mikä vastaa esimerkiksi Ranskan vuosittaista bruttokansantuotetta.[120]

Rahanpesurikoksen rangaistavuuden alaan tehtiin vuonna 2020 muutoksia itsepesun osalta. Itsepesulla tarkoitetaan sellaista rahanpesua, jonka kohteena olevat varat on hankittu omalla rikollisella toiminnalla. Vakiintunut lähtökohta on ollut, että mikäli rahanpesijä on osallinen esirikokseen, ei häntä erikseen enää rangaista rahanpesusta. Rahanpesu on näissä tilanteissa siis vain esirikoksen jälkiteko, jonka katsotaan tulevan riittävissä määrin arvostelluksi esirikoksesta rangaistaessa.[121] Vuonna 2020 rikoslakiin kuitenkin tehtiin muutoksia, jotta ne vastaisivat EU:n viidennen rahanpesudirektiivin vaatimuksia ja tämän myötä myös itsepesusta voidaan tuomita

[116] Hyttinen, 2021, s. 1.
[117] Sahavirta, 2008, s. 43.
[118] Hyttinen, 2021, s. 2.
[119] https://www.unodc.org/unodc/en/money-laundering/overview.html , katsottu 23.9.2021
[120] Hyttinen, 2021, s. 2.
[121] HE 183/2020 vp, s. 5.

laajemmin. Alustavien arvioiden mukaan nämä muutokset voivat lisätä rahanpesurikostuomioiden määrää vuodessa 100-200 tuomiolla.[122]

3.2.1 Rahanpesu ja virtuaalivaluutat – minkälaisia haasteita virtuaalivaluutat aiheuttavat rahanpesusääntelylle?

Kun laittomasta rahasta pyritään tekemään laillista, kyseessä ei yleensä ole suoraviivainen tai selvästi todennettavissa oleva yksittäinen toimi. Tämä tekee rahanpesun estämisestä haastavaa ja syyllisyyttä ei välttämättä tuomioistuimissa kyetä osoittamaan riittävällä tavalla.[123]

Bitcoin ja muut virtuaalivaluutat ovat mullistaneet finanssimaailman luomalla valuutan, jonka taustalla ei ole, eikä sitä ohjaa yksikään valtio tai keskuspankki. Virtuaalivaluutat ovat mahdollistaneet *anonyymit ja salatut varojen siirrot*. Tämä anonymiteetti on avannut rikollisille aivan uudenlaisia mahdollisuuksia, kun yksityiset henkilöt ovat voineet tehdä laittomia rahansiirtoja ilman, että näiden siirtojen tekijää ei ole pystytty jäljittämään. [124] Rahanpesun ennaltaehkäisyssä ja estämisessä keskeisessä roolissa ovat ilmoitusvelvolliset ja heitä velvoittavat asiakkaan tuntemismenettelyt, joten kyse on merkittävästä riskistä.

Virtuaalivaluuttojen omistajilla ja käyttäjillä ei ole käytössään perinteisiä tilejä varoilleen, vaan varoja säilytetään usein virtuaalivaluuttalompakoissa. Virtuaalivaluuttajärjestelmässä jokainen yksikkö tai kolikko voidaan jäljittää lohkoketjussa useiden avainten kautta, joiden avulla on mahdollista jäljittää yhden kolikon liikkeitä ja sitä, minne se siirtyy. Kolikon haltija saa haltuunsa yksityisen avaimen, joka sitten todistaa avaimen haltijan kyseisen kolikon omistajaksi. Virtuaalivaluuttojen käyttäjien ei ole periaatteessa välttämätöntä antaa itsestään mitään henkilötietoja[125] hankkiakseen tai omistaakseen virtuaalivaluuttoja.[126]

Perinteisesti rahanpesun suorittamiseksi tekijöiden on ollut välttämätöntä jossain tekovaiheessa siirtää rahat keskuspankkijärjestelmän valvonnan piiriin ja näin alttiiksi viranomaisten interventioille.[127] Valtiot myös pystyivät puuttumaan rahanpesuun huomattavasti helpommin

[122] HE 183/2020 vp, s. 33.
[123] McDowell, 2001, s. 6.
[124] Albrecht, 2019, s. 211.
[125] Virtuaalivaluuttalain päivittämisellä ja esimerkiksi EU:n maksajan tiedot-asetuksella on pyritty puuttumaan virtuaalivaluuttojen anonymiteetin aiheuttamiin haasteisiin.
[126] Albrecht, 2019, s. 214.
[127] Rahanpesun vaikuttavimmat ennaltaehkäisytoimet ovat perinteisesti pyrkineet havaitsemaan rikollisen toiminnan tässä erityisesti tässä ns. placement-vaiheessa mm. velvoittamalla pankkeja ja muita finanssimaailman toimijoita havainnoimaan ja ilmoittamaan epäilyttävistä toimista.

mm. asettamalla säännöksiä tai uhkasakkoja sellaisille pankeille, jotka tekivät rahanpesusta rikollisille helpompaa.[128] Esimerkiksi bitcoinilla taas ei ole mitään keskitettyä hallintoa tai järjestelmää, vaan varat liikkuvat tarvittaessa nopeastikin lohkoketjussa niin, että siirtoja ei valvo kukaan. *Hajautunut ja keskusjohtoa vailla oleva järjestelmä* luo merkittäviä haasteita rikollisten kiinni saamiselle ja rikollisuuden ennaltaehkäisemiselle perinteisin valvonnan keinoin.

Kuten aiemmin on jo tuotu esiin, virtuaalivaluuttojen käytöstä jää aina jälkiä, jotka ovat avoimeen lohkoketjuteknologiaan perustuvissa virtuaalivaluutoissa käytännössä kenen tahansa siihen kykenevän selvitettävissä. Pankkien tileillä olevien varojen määrä ja alkuperä taas kuuluvat lähtökohtaisesti ainoastaan asiakkaalle itselleen. Tämä luo merkittäviä haasteita *yksityisyydensuojan ja tietosuojan* näkökulmasta, mikäli esimerkiksi rikollisilla toimijoilla tulevaisuudessa olisi mahdollisuus purkaa käyttäjien anonymiteettiä suojeleva vahva salaus.

Virtuaalivaluuttojen tullessa yhä yleisemmäksi, useat yritykset ovat viime aikoina ilmoittaneet hyväksyvänsä virtuaalivaluutat maksuvälineenä. Tämä avaa rikollisille lisää mahdollisuuksia käyttää virtuaalivaluuttoja rahanpesussa, sillä varoja ei välttämättä koskaan tarvitse siirtää keskuspankkijärjestelmän piirin ja valvonnan alaiseksi tai vaihtaa niitä fiat-valuutaksi. Virtuaalivaluutoilla voi näin hankkia suoraan arvokkaitakin hyödykkeitä. [129]

Seuraava merkittävä riski on se, että *virtuaalivaluuttaa voidaan helposti ja nopeasti siirtää valtiosta toiseen*. Tämän ominaisuuden ansiosta rikolliset voivat hyvinkin nopealla aikataululla ja anonyymisti siirtää rikollisella toiminnalla ansaitut varat kokonaan toisen oikeusjärjestelmän piiriin. Hyödyt ovat ilmeiset, sillä varojen siirtoon riittää pelkkä toimiva internet-yhteys. Lohkoketjuteknologian toimiessa hajautetusti kokonaisuutena sitä ei myöskään voida sulkea yhdestä pisteestä tai yhdestä valtiosta käsin. Järjestelmän kaatuminen vaatisi sitä, että kaikki yhteyspisteet kaadettaisiin samanaikaisesti, mikä on käytännössä mahdotonta, sillä lohkoketjun kaataminen edellyttäisi koko internetin kaatamista.[130] Mikäli valtioiden lainsäädännöt ovat keskenään hyvin erilaisia, voivat rikolliset etsiä ja käyttää hyväkseen näitä löytämiään aukkoja ja ohjata varoja nopeasti otollisimpiin kohteisiin. Erityisesti tällä on perusteltu esim. EU:ssa jäsenvaltioiden rikoslainsäädäntöjen harmonisointitarpeita.

[128] Albrecht, 2019, s. 213.
[129] Albrecht, 2019, s. 213.
[130] Albrecht, 2019, s. 213.

Näiden edellä esitettyjen riskien seurauksena monessa valtiossa on pyritty säätämään lakeja virtuaalivaluuttojen käytön estämiseksi. Näin on tehty vaikkapa Kiinassa ja Intiassa. Toisaalta taas esimerkiksi Japani on luonut lainsäädäntöä, jolla pyritään mahdollistamaan virtuaalivaluuttojen käyttö laillisena maksuvälineenä. [131] Useimmat valtiot ovat kuitenkin vasta olleet käynnistelemässä keskustelua siitä, miten näiden uudenlaisten valuuttojen, etenkin bitcoinin, kanssa tulisi toimia.

Virtuaalivaluuttojen käyttö rahanpesun välineenä voi johtaa laajoihin negatiivisiin vaikutuksiin koko maailmantaloudessa. Läpi historian rahanpesu on ollut valtioille suuri haaste ja keskuspankkijärjestelmän sääntelyn avulla tilanne on ollut jokseenkin hallinnassa.[132] Virtuaalivaluuttojen käyttö on tiukasti sidoksissa rahanpesuun, sillä se tarjoaa kyseiselle toiminnalle anonymiteetin mahdollistamisella loistavan alustan. Vaikka bitcoinin arvo on vaihdellut voimakkaasti, on se ajan kuluessa tullut vakaammaksi ja sen arvo on kohonnut lukemiin, joihin niiden ei useiden asiantuntijoiden mukaan ikinä pitänyt kohota.

3.3 Terrorismin rahoittaminen

Terrorismin rahoittamisella on jopa mahdollisesti rahanpesuakin kansainvälisempi luonne. Suomessa terrorismin rahoittaminen on suhteellisen harvinainen rikos, johon voi tosin vaikuttaa se, että terrorismin rahoittamisesta tuomitseminen on usein haastavaa näytön puutteen vuoksi ja syyllisyyttä ei voida riittävissä määrin osoittaa. Terrorismirikoksen rahoittaminen on Suomessa kriminalisoitu rikoslain 34a luvussa sen 5 §:ssä seuraavasti:

> *Joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan jotakin 1, 1 a, 2–4, 4 a–4 c, 5 c tai 5 d §:ssä tarkoitettua rikosta, on tuomittava terrorismirikoksen rahoittamisesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään kahdeksaksi vuodeksi. (9.4.2021/281)*
>
> *Terrorismirikoksen rahoittamisesta tuomitaan myös se, joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan jotakin seuraavista rikoksista –".*
>
> *1) panttivangin ottaminen tai kaappaus,*
>
> *2) sellainen tuhotyö, törkeä tuhotyö tai yleisvaarallisen rikoksen valmistelu, jota on pidettävä terroristisen pommi-iskujen torjumista koskevassa kansainvälisessä yleissopimuksessa (SopS 59–60/2002) tarkoitettuna rikoksena,*

[131] Chohan, 2017, s. 7.
[132] Albrecht, 2019, s. 214.

3) sellainen tuhotyö, liikennetuhotyö, törkeä tuhotyö tai yleisvaarallisen rikoksen valmistelu, jota on pidettävä siviili-ilmailun turvallisuuteen kohdistuvien laittomien tekojen ehkäisemistä koskevassa yleissopimuksessa (SopS 56/1973), kansainväliseen siviili-ilmailuun käytettävillä lentoasemilla tapahtuvien laittomien väkivallantekojen ehkäisemistä koskevassa lisäpöytäkirjassa (SopS 43/1998), merenkulun turvallisuuteen kohdistuvien laittomien tekojen ehkäisemistä koskevassa yleissopimuksessa (SopS 11/1999) tai mannerjalustalla sijaitsevien kiinteiden lauttojen turvallisuuteen kohdistuvien laittomien tekojen ehkäisemistä koskevassa pöytäkirjassa (SopS 44/2000) tarkoitettuna rikoksena,

4) sellainen ydinräjähderikos, terveyden vaarantaminen, törkeä terveyden vaarantaminen, ydinenergian käyttörikos tai muu ydinaineeseen kohdistuva tai ydinainetta välineenä käyttäen tehty rangaistavaksi säädetty teko, jota on pidettävä ydinaineiden turvajärjestelyjä koskevista toimista tehdyssä yleissopimuksessa (SopS 72/1989) tarkoitettuna rikoksena, tai

5) murha, tappo, surma, törkeä pahoinpitely, vapaudenriisto, törkeä vapaudenriisto, törkeä ihmiskauppa, panttivangin ottaminen tai törkeä julkisrauhan rikkominen tai niillä uhkaaminen, kun teko kohdistuu henkilöön, jota tarkoitetaan kansainvälistä suojelua nauttivia henkilöitä vastaan, mukaan lukien diplomaattiset edustajat, kohdistuvien rikosten ehkäisemistä ja rankaisemista koskevassa yleissopimuksessa (SopS 62–63/1978).

(9.4.2021/281)
Yritys on rangaistava.

Terroristinen toiminta vaatii lähes aina ulkopuolista rahoitusta ja siksi on ollut erityisen tärkeää, että terrorismin rahoittaminen on kansainvälisestikin kriminalisoitu. Kriminalisointiin ja syyllisyyden arviointiin on liittynyt kuitenkin useita ongelmia, kuten se, tietääkö henkilö täysin sitä, minne hänen rahansa lopulta päätyvät.[133] Useimmiten on kyse tilanteista, joissa rahoittaja kuvittelee rahoittavansa humanitaarista toimintaa, mutta varat päätyvät lopulta terroristijärjestön haltuun. Jotta tekijä voitaisiin tuomita terrorismin rahoittamisrikoksesta, tulee teolta voida vaatia tarkoitustahallisuutta tai tietoisuutta siitä, mitä rahoitetaan. Rangaistavuuden rajojen määrittely on ollut haasteellista, sillä usein rahojen antajalla ei ole todellisia mahdollisuuksia määritellä sitä, minne hänen varansa lopulta päätyvät.[134] Ongelmaa onkin pyritty ratkaisemaan tuoreilla lainmuutoksilla, kun rikoslakiin lisättiin sen 34 a lukuun lisäykset terroristin ja terroristiryhmän rahoittamisesta. Rikoslain 34a luvun 5 a §:n mukaan,

[133] Rautio ym., 2004, jakso II, kappale 22, tunnusmerkistöt.
[134] Rautio ym., 2004, jakso II, kappale 22, tunnusmerkistöt.

> *joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan henkilöä, joka tekee 1 tai 1 a §:ssä tarkoitettuja rikoksia tai osallistuu niiden tekemiseen 5 luvun 3–6 §:ssä tarkoitettuna rikokseen osallisena, on tuomittava terroristin rahoittamisesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään kuudeksi vuodeksi.*

Vastaavasti terroristiryhmän rahoittaminen on kriminalisoitu 5 a §:ssä, jonka mukaan

> *Joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan henkilöä, joka tekee 1 tai 1 a §:ssä tarkoitettuja rikoksia tai osallistuu niiden tekemiseen 5 luvun 3–6 §:ssä tarkoitettuna rikokseen osallisena, on tuomittava terroristin rahoittamisesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään kuudeksi vuodeksi.*

Lisäyksillä pyrittiin vastaamaan kansainvälisten toimielinten Suomelle antamaan kritiikkiin terrorismirikosten sääntelyn riittämättömyydestä kansallisessa lainsäädännössämme.[135] Tässä tutkielmassa käytetään terrorismirikosten, terroristin ja terroristiryhmän rahoittamisesta yleisnimitystä ”terrorismin rahoittaminen”.

Edellä rahanpesun eri vaiheet esitettiin ns. ympyrämallina. Terrorismin rahoittamisessa on taas kyse enemmänkin lineaarisesta porrastetusta mallista, jossa raha käytetään suoraan terroristisen toiminnan rahoittamiseen. Terrorismin rahoittaminen jaetaan usein neljään vaiheeseen, jotka ovat kerääminen (raise), säilöminen (store), siirtäminen (move) ja käyttö (use).

Terrorismin rahoittamista kuvataan yleensä ympyrämallin sijaan lineaarisesti.[136]

Terrorismin rahoittamisessa on siis yksinkertaisesti kyse siitä, että terroristit keräävät rahoitusta, jotta voivat suorittaa terrorismirikoksia. Jokainen terroristiryhmä tarvitsee rahallista

[135] HE 135/2020 vp. Hallituksen esityksen perusteluissa todetaan, että ”lainsäädäntömuutosten taustalla ovat eräiden kansainvälisten toimielinten arviot terrorismin rahoittamista koskevista Suomen rangaistussäännöksistä sekä terrorismin rahoittamisrikoksia koskevat YK:n turvallisuusneuvoston päätöslauselmat. - - Lainsäädäntömuutosten myötä terrorismin rahoittamisrikoksia koskevat rangaistussäännökset muodostaisivat nykyistä johdonmukaisemman ja selkeämmän kokonaisuuden.”

[136] United Nations, Office on Drugs and Crime.Terrorist financing, https://www.unodc.org/unodc/en/money-laundering/overview.html .

tukea, jotta voisivat saavuttaa tavoitteensa. Terrorismin rahoittamisrikoksen teonkuvauksen täyttyminen ei siis vaadi samanlaista esirikosta, kuin rahanpesun toteuttaminen, vaan terrorismia voidaan rahoittaa myös laillisesti ansaituilla varoilla.

Terrorismin rahoittamisen estämiseksi on Suomessa säädetty myös Laki varojen jäädyttämisestä terrorismin torjumiseksi (325/2013). Laki on säädetty YK:n turvallisuusneuvoston vuonna 2001 hyväksymässä päätöslauselmassa 1373 (2001) YK:n jäsenvaltioille asetettujen velvoitteiden täytäntöön panemiseksi. Lain 2 §:ssä varojen jäädyttäminen määritellään sellaisiksi toimenpiteiksi, joilla estetään kaikki sellainen varojen liikkuminen, siirtäminen, muuntaminen, käyttäminen ja käsitteleminen, joka muuttaisi varojen määrää, sijaintia, omistusta, hallintaa, luonnetta tai käyttötarkoitusta, sekä toimenpiteitä, joilla estetään muut sellaiset muutokset, jotka mahdollistaisivat varojen käytön. Varojen jäädyttämisestä päättää lain 4 §:n mukaan Keskusrikospoliisi. KRP:n päätöksen toimeenpanee Ulosottolaitos.

Ulkoministeriön tehtävänä on Suomessa määrätä pakotteita terrorismin ja sen rahoittamisen estämiseksi.[137] Pakotteet tarkoittavat pakotteiden kohteena oleviin tahoihin kohdistuvia yhteistyön rajoituksia, joista olennaisimpina voidaan pitää taloudellisia pakotteita. Terrorismin rahoittamisesta on aloitettu Suomessa tähän mennessä vain kolme esitutkintaa, joista yksi vuoden 2015 jälkeen. Tuomioistuimessa terrorismin rahoittamista on käsitelty yhden kerran ja silloinkin syytteet hylättiin.[138]

3.3.1 Terrorismin rahoittaminen ja virtuaalivaluutat – miten virtuaalivaluuttoja käytetään hyödyksi terrorismin rahoittamisessa?

Viime vuosina terroristeilla on ollut hankaluuksia rahoittaa toimintaansa, kun vuoden 2001 WTC-iskujen jälkeen keskuspankkien valvontaa on kiristetty ja niille on asetettu uusia velvoitteita valvoa rahanpesua ja terrorismin rahoittamista. Ennen näitä iskuja oli valtioita, joissa em. rikoksia ei oltu lainkaan kriminalisoitu.[139] On ilmeistä, että perinteiset rahoittamiskeinot keskuspankkijärjestelmien piirissä aiheuttavat terroristijärjestöille merkittävän kiinnijäämisen riskin. Jotta terroristiryhmät voisivat luoda ja pitää yllä tehokasta rahoitusjärjestelmää ja infrastruktuuria, täytyy niiden löytää erilaisia rahoituksen lähteitä sekä

[137] Voimassaolevat pakotteet voi tarkastaa Ulkoministeriön nettisivuilta osoitteesta https://um.fi/terrorismin-vastaiset-pakotteet .
[138] Ks. Helsingin HO 23.3.2016, nro 16/111925.
[139] Irwin – Milad, 2016, s. 408.

järjestää tehokas reitti tiettyyn toimintaan tarkoitettuun rahoituksen päätymiseen oikeaan kohteeseen.[140] Terroristit käyttävät tähän samankaltaisia keinoja, kuin rahanpesurikoksissa yleisesti käytetään.[141]

Terrorismin rahoittajien vaatimuksiksi heidän käyttämilleen rahoittamiskeinoille on tutkittu ja keskeisimpiä asioita ovat vaatimukset varainsiirtojen helppoudesta ja nopeudesta, sekä siirtojen alhaisista kustannuksista.[142] Nämä ominaisuudet takaavat sen, että rahoittamisen volyymi saadaan kasvatettua mahdollisimman suureksi. Terroristijärjestö ISIS:in kannattajat ovat julkaisseet mm. Youtubessa ja erilaisilla keskustelufoorumeilla linkkejä, joissa esitellään bitcoinia ja kerrotaan sen anonymiteetin mahdollistavasta teknologiasta. Virtuaalivaluuttaa kehotetaan käyttämään erityisesti paikoissa, jossa perinteinen varojen siirto on hankalaa johtuen tiukasta valvonnasta, rajoituksista tai verkoston puutteesta.[143] Vuoden 2015 kesäkuussa amerikkalainen teini tuomittiin, kun hän oli opettanut ISIS:in jäsenille, miten bitcoin-lompakko voidaan ottaa käyttöön ja miten niihin voidaan ohjata lahjoituksia.[144] On olemassa todistusaineistoa, että bitcoinia on käytetty hyödyksi muissakin terrori-iskuissa.[145]

Vaikka tulevaisuutta on hankala ennustaa, on kuitenkin todennäköistä, että virtuaalivaluuttojen käytön lisääntyminen lisää todennäköisyyttä myös sille, että terroristijärjestöt pyrkivät hyödyntämään niitä toiminnassaan entistä enemmän. Huolenaiheena on ollut myös se, että terroristijärjestöt pyrkisivät luomaan omia virtuaalivaluuttojaan, jotka on suunniteltu nimenomaisesti heidän tarpeidensa mukaisesti.

3.3.2 Rikollisten kokemuksia virtuaalivaluuttojen käytöstä terrorismin rahoittamisessa

Vuoden 2022 alussa on julkaistu tutkimus[146], jossa on pyritty tarkemmin selvittämään sitä, miten terrorismin rahoittajat pyrkivät välttämään valvontaa ja kiinnijääntiä siirtäessään varoja rahoittajalta toimijoille. Tutkimus on tehty erityisesti virtuaalivaluuttojen näkökulmasta ja sen hypoteesina on ollut, että valtioiden kyvyttömyys estää terrorismin rahoittamista johtuu siitä, että niiltä puuttuu tieto niistä konkreettisista vaiheista, joita terroristisen toiminnan rahoittajat

[140] Irwin – Milad, 2016, s. 408.
[141] Irwin – Milad, 2016, s. 408.
[142] Freeman, 2013, s. 7.
[143] Irwin – Milad, 2016, s. 409.
[144] ks. Reuters. American teenager pleads guilty to helping Islamic State, 11.6.2015.
[145] Irwin – Milad, 2016, s. 410.
[146] Ks. Teichmann, 2022.

käyvät läpi siirtäessään varoja rajojen yli jäämättä kiinni. [147] Esitutkimuksessa on havaittu, että suuri ongelma terrorismin rahoittamisen estämisessä verrattuna rahanpesun estämiseen on se, että terrorismin rahoittamisessa käytettyjen varojen yleensä laillinen alkuperä vaikeuttaa merkittävästi viranomaisten mahdollisuuksia puuttua varojen siirtoihin. Pankeilla ei myöskään ole yleensä keinoja tunnistaa yksittäisistä siirroista sitä, mihin tarkoitukseen varat lopulta ovat päätymässä. [148]

Tutkimuksessa pystyttiin tunnistamaan konkreettisia menetelmiä, joiden avulla rahoittamisrikoksia toteutetaan ja niitä on toteutettu virtuaalivaluuttojen avulla. Välttääkseen sen, että virtuaalivaluuttojen siirroista jäisi myöhemmin jäljitettävissä olevia ”digitaalisia jalanjälkiä”, rikolliset esimerkiksi saattoivat hankkia usein uusia tietokoneita, jotka he nopeasti lyhyen käyttöajan jälkeen hävittivät ja hankkivat tilalle jälleen uuden. Tämän lisäksi rikolliset pyrkivät käyttämään julkisia Wi-Fi-yhteyksiä, jotta heitä ei sitäkään kautta saataisi tunnistettua ja verkkoyhteyksiä myös vaihdeltiin niin, että samaa yhteyttä ei käytettäisi kahta kertaa. Tämä tekee jäljittämisestä hyvin hankalaa.[149]

Tämän lisäksi tutkimuksessa havaittiin, että välttääkseen epätoivotun huomion terrorismin rahoittajat pyrkivät käyttäytymään kuin tavalliset virtuaalivaluuttojen käyttäjät ja ylläpitävät virtuaalivaluuttalompakoitaan mahdollisimman ”normaalisti”.[150] Hajauttaakseen riskiä rikolliset myös ovat käyttäneet useampia lompakoita ja välttävät hankkimasta virtuaalivaluuttaa suoraan omilla varoillaan ja omilta pankkitileiltään. Sen sijaan he pyrkivät löytämään paikallisia toimijoita, jotka ovat halukkaita vaihtamaan virtuaalivaluuttaa käteiseen tai muihin hyödykkeisiin. [151]

Tutkimuksessa ilmeni myös se, että suurin syy rikollisten toimijoiden halukkuuteen käyttää juuri virtuaalivaluuttoja terrorismin rahoittamisessa on niiden tarjoama anonymiteetti. Rikolliset ovat kuitenkin tietoisia viranomaisten jatkuvasti kasvavasta kiinnostuksesta virtuaalivaluuttojen käyttöön liittyvän rikollisuuden suhteen, sillä ne yhdistetään edelleen vahvasti rikollisuuteen ja niiden käyttö erilaiseen rikolliseen toimintaan on kansainvälisestikin laajasti huomioitu. [152] Rikolliset ovat kuitenkin tuoneet esiin myös sen, että he osaltaan luottavat

[147] Teichmann, 2022, s. 112.
[148] Teichmann, 2022, s. 114.
[149] Teichmann, 2022, s. 115.
[150] Teichmann, 2022, s. 115.
[151] Teichmann, 2022, s. 115.
[152] Teichmann, 2022, s. 116.

virallisten toimijoiden ”hitauteen” puuttua heidän toimintaansa lainsäädännön keinoin ja senkin jälkeen yritysten ja viranomaisten välinen tiedonvaihto on usein hyvin puutteellista, eikä sitä ole välttämättä mahdollista toteuttaa lain vaatimissa puitteissa.[153]

3.4 Yleisistä kriminalisointiperiaatteista

Rikosoikeus on hyvin perinteinen oikeustieteen ala ja sillä on olemassa vakiintuneet yleiset periaatteet, joita tulee noudattaa. Teknologian kehittyminen ja internetin vallankumous ovat asettaneet haasteita rikosoikeudelliselle sääntelylle ja kriminalisointiperiaatteille jo vuosikymmenten ajan, joten mikään täysin uudenlainen ilmiö ei ole kyseessä, kun puhutaan virtuaalivaluuttojen luomista uusista vaatimuksista rikosoikeudellisen sääntelyn suhteen. Mikäli lainsäätäjä ei ensin herää lainsäädännön mahdolliseen vanhentumiseen, on myös ennakkopäätöstuomioistuimilla velvollisuus linjata asiasta, mikäli jonkin rikoksen toteuttamistapa ei enää mahdu teonkuvaukseen ilman, että vastaajan oikeusturva vaarantuu. Edellä on kuvailtu yleisesti niitä haasteita, joita nimenomaan virtuaalivaluuttojen taustalla oleva teknologia aiheuttaa rahanpesun ja terrorismin rahoittamisen sääntelylle. Mahdollisista lainsäädännöllisistä muutostarpeista puhuttaessa on välttämätöntä määritellä ne raamit, joissa muutoksia edes on mahdollista tehdä. Rikosoikeudessa yleiset kriminalisointiperiaatteet ohjaavat tässä.

Uusia linjauksia vetäessä tulee olla huolellinen, että annetut tuomiot pysyvät rikosoikeudellisen *legaliteettiperiaatteen* rajoissa. Legaliteettiperiaate on yksi rikosoikeuden ja oikeusvaltiomme kulmakivistä ja lainsäädännössämme se on tiivistetty perustuslain 8 §:ään 1 momenttiin, jonka mukaan *ketään ei saa pitää syyllisenä rikokseen eikä tuomita rangaistukseen sellaisen teon perusteella, jota ei tekohetkellä ole laissa säädetty rangaistavaksi*. Legaliteettiperiaatteeseen katsotaan nykyisin sisältyväksi myös *taannehtivuuskielto*, *praeter legem-kielto, analogiakielto* ja *epätäsmällisyyskielto*.[154] Taannehtivuuskiellolla tarkoitetaan sitä, että tekoa ei voida jälkikäteen säätää rangaistavaksi niin, että henkilöä voitaisiin syyttää teosta, joka ei tekoaikana ole ollut kriminalisoitu. Taannehtivuuskieltoon katsotaan sisältyväksi myös se, että mikäli lainsäädäntöä on teon jälkeen muutettu, tulee soveltaa tekijän kannalta lievimmän tuomion antavaa lakia. [155] Praeter-legem-kielto tarkoittaa, että tuomari ei saa päätöksessään mennä kirjoitetun lain ulkopuolelle ja analogia-kielto sitä, että analogiaan ei saa rikosoikeudessa

[153] Teichmann, 2022, s. 117.
[154] Melander, 2002, s. 940.
[155] Melander, 2002, s. 940.

turvautua syytetyn vahingoksi.[156] Epätäsmällisyyskielto taas asettaa rikoslainsäädännölle vaatimuksen säännösten täsmällisyydestä.[157]

Kriminalisoinnin edellytyksenä on edelleen kriminalisointiperiaatteiden mukaisesti, että rikosoikeutta tulee käyttää vain tärkeiden intressien suojaamiseksi (*oikeushyvien suojelun periaate*). Kriminalisoinnin tulee myös olla jonkin asian sääntelyn viimesijainen keino (*ultima ratio-periaate*) ja rangaistuksista saatavien hyötyjen on selvästi ylitettävä niistä aiheutuvat haitat (*hyöty-haitta-punninnan periaate*). Kriminalisoinnista ei myöskään saa seurata sellaisia näyttöongelmia, jotka olisivat ylitsepääsemättömiä tai mielivaltaisesti ratkaistavissa, eikä siellä voi olla sellaisia säädöksiä, joiden valvominen olisi käytännössä mahdotonta tai joiden arvioidaan olevan todellisuudessa tehottomia (*suhteellisuusvaatimus*). Rangaistusasteikon on lisäksi vastattava rikostyypin moitittavuutta.[158]

3.4.1 Toissijaisuusperiaate EU-oikeuden rajoittajana

Toissijaisuusperiaate määritellään sopimuksen Euroopan unionin toiminnasta (SEUT) 5 artiklassa. Artiklan mukaan ”unioni toimii ainoastaan jäsenvaltioiden sille perussopimuksissa antaman toimivallan rajoissa ja sellaisilla aloilla, jotka eivät kuulu sen yksinomaiseen toimivaltaan, ainoastaan jos ja siltä osin kuin jäsenvaltiot eivät voi keskushallinnon tasolla tai alueellisella taikka paikallisella tasolla riittävällä tavalla saavuttaa suunnitellun toiminnan tavoitteita, vaan ne voidaan suunnitellun toiminnan laajuuden tai vaikutusten vuoksi saavuttaa paremmin unionin tasolla.” Artiklan 4 kohdassa viitataan suhteellisuusperiaatteeseen, jonka mukaisesti ”unionin toiminnan sisältö ja muoto eivät saa ylittää sitä, mikä on tarpeen perussopimusten tavoitteiden saavuttamiseksi”.

Edellä kuvatusti kriminalisoinnille asetetaan lainsäädännössämme useita erilaisia rajoitteita. Virtuaalivaluuttojen aiheuttaessa aiemmin kuvailtuja haasteita niin lainsäädännölle, kuin rikollisuuden estämis- ja ennaltaehkäisytoimille, voi houkutus nopeatahtiseen lain uudistamiseen ja uusien kriminalisointien luomiseen olla suuri. Oikeusjärjestelmämme ydinperiaatteet on kuitenkin muotoiltu myös (tai juurikin) sellaisten tilanteiden varalle, joissa

[156] Melander, 2002, s. 940.
[157] Perustuslakivaliokunta ja lakivaliokunta ovat useasti nostaneet esille sen, että rikoksen tunnusmerkistö on rikosoikeudellisen laillisuusperiaatteen mukaisesti ilmaistava laissa riittävällä täsmällisyydellä siten, että säännöksen sanamuodon perusteella on ennakoitavissa, onko jokin toiminta tai laiminlyönti rangaistavaa. Ks. PeVL 48/2002 vp, PeVL 41/2001 vp ja PeVL 10/2000 vp.
[158] Oikeusministeriön mietintöjä ja lausuntoja, 2020:8, s. 49.

viranomaisilla tai lainsäätäjällä on voimakas tarve lähteä nopeasti vastaamaan johonkin uuteen rikolliseen ilmiöön ja niitä tulisi voida kunnioittaa silloinkin, kun intressi rikollisuuden estämiseksi on suuri.

4. Rahanpesun ja terrorismin rahoittamisen estäminen ja ennaltaehkäisy

4.1 Lähtökohtia

Rahanpesun ja terrorismin rahoittamisen estäminen ja ennaltaehkäisy on jo edellä esitetysti ollut aina hyvin kansainvälinen rikosoikeuden haara. Internetin ja teknologian kehittymisen myötä rajat ylittävän rikollisuuden estäminen on yhä vahvemmin siirtynyt kansallisen lainsäätäjän hallinnasta kansainvälisille areenoille. Erityisesti EU:ssa on korostettu jäsenvaltioiden lainsäädäntöjen harmonisoinnin merkitystä rikollisuuden torjumisessa. Seuraavaksi käydään läpi rahanpesun ja terrorismin rahoittamisen estämisen kannalta olennaisin lainsäädäntö ja alan toimijat. Tutkielman tarkoituksena ei ole esitellä mahdollisimman laajasti jokaisen toimijan vastuualueita tai yleisiä kehitystarpeita, vaan lainsäädäntöä ja mahdollisia muutostarpeita tarkastellaan nimenomaan virtuaalivaluuttojen näkökulmasta.

4.1 FATF – Financial Action Task Force

Yksi merkittävimmistä toimijoista kansainvälisessä rahanpesunvastaisessa toiminnassa on Financial Action Task Force, eli FATF. FATF on perustettu vuonna 1989 G 7-teollisuusmaiden kokouksessa ja siihen kuuluu nykyisin 37 valtiota. FATF:n vaikutusvalta on todellisuudessa suurempi, kuin sen jäsenmäärästä voisi olettaa, sillä sen jäsenvaltiot ovat taloudellisesti hyvin toimeentulevia ja vaikutusvaltaisia valtioita.[159] Tämä on johtanut tilanteeseen, jossa FATF:n linjauksilla on suuret vaikuttamismahdollisuudet myös sellaisten valtioiden toimintaan kansainvälisillä finanssimarkkinoilla, jotka eivät ole FATF:n jäsenvaltioita. Jos valtio haluaa toimia täysipainoisesti globaaleilla markkinoilla, tulee sen harmonisoida omaa lainsäädäntöään FATF:n vaatimusten mukaiseksi. [160] Tähän on vaikuttanut myös se, että EU on omassa lainsäädännössään tosiasiallisesti monesti noudattanut FATF:n vaatimuksia ja näin sellaisetkin jäsenvaltiot, jotka eivät ole FATF:n jäseniä, ovat joutuneet harmonisoimaan lainsäädäntöään sen mukaisesti. Pahimmillaan valtio voi jopa voitua niin sanotulle FATF:n ”mustalle listalle”, mikä vaikeuttaa kyseisen valtion yritysten mahdollisuuksia saada rahoitusta ja vähentää valtioon tulevia kansainvälisiä investointeja.[161]

[159] Hyttinen, 2021, s. 38.
[160] Hyttinen, 2021, s. 39
[161] Hyttinen, 2021, 40.

FATF:n ydintehtäviin kuuluu rahanpesun estäminen, jota se toteuttaa lähinnä edellyttämällä sen jäsenvaltioilta tehokasta rahanpesun vastaista lainsäädäntöä. FATF:ssa ei laadita kansainvälisiä sopimuksia näiden vaatimusten täyttämiseksi, vaan siellä koordinoidaan rahanpesun vastaista työtä ja valvotaan sitä, kuinka hyvin jäsenvaltiot onnistuvat rahanpesun vastaisissa toimissa. FATF:n toimialueeseen on rahanpesun lisäksi lisätty myös terrorismin rahoittamisen vastustaminen. FATF antaa myös suosituksia[162], jotka ovat hyvin olennainen standardi rahanpesun vastustamisessa. Ne liittyvät muun muassa kansallisten toimien koordinointiin, rahanpesun kriminalisointeihin ja asiakkaiden tunnistamiseen.[163]
Suomi on ollut FATF:n jäsen vuodesta 1991 ja kansallista FATF-asioihin liittyvää työtä tehdään FATF-johtoryhmässä ja FATF-ryhmässä.[164] Suomen FATF-ryhmän tehtäviin kuuluu muun muassa viranomaistyöstä huolehtiminen, toimintasuunnitelmien kehittäminen ja niiden täytäntöönpanosta päättäminen sekä Suomen kantojen päättäminen FATF:n työryhmien kokouksiin ja yleiskokouksiin.[165]

Hyttinen on arvostellut sitä, että FATF:n suosituksiin ja lauselmiin suhtaudutaan jopa turhankin kritiikittömästi. Hänen ensimmäinen kritiikkinsä kohdistuu siihen, että rahanpesun vastaisia toimia on FATF:ssa pyritty estämään jopa liian fundamentaalisin toimenpitein. FATF ei ole kiinnittänyt tarpeeksi huomiota mm. siihen, minkälaisia seuraamuksia rahanpesun vastaisista toimenpidevaatimuksista on laajemmin. FATF ei ole esimerkiksi suorittanut minkäänlaista kustannus-hyöty-laskelmaa siitä, ovatko kaikki toimet ovat olleet taloudellisesti perusteltuja. Tämän arvioinnin puute on Hyttisen mukaan johtanut siihen, että rahanpesun vastainen lainsäädäntö on laajentunut tarpeettomankin laajaksi ja lisännyt viranomaisvaltuuksia, mikä on taas lisännyt julkisen ja yksityisen sektorin voimavaroja. [166]

Toinen *Hyttisen* esittämä kritiikki kohdistuu siihen, että FATF ei ole huomioinut toimintavelvoitteita asettaessaan tarpeeksi perus- ja ihmisoikeusvaatimuksia ja sitä, että niiden

[162] Vuonna 2019 julkaistussa maa-arvioraportissa FATF mainitsi Suomen erityiseksi ansioksi ja vahvuudeksi kansainvälisen yhteistyön, kansallisen riskiarvioinnin ja tiedustelu- ja muun selvittelytiedon keräämisen. Keskeisimpänä heikkoutena taas mainittiin valvontatoiminnan riittämätön riskiperusteisuus, jonka taustalla oli mm. huomattava resurssien alimitoitus (ks. FATF, 2019, Anti-money laundering and counter-terrorist financing measures). FATF:n kommentit yhdessä EU:n Suomelle neljännen rahanpesudirektiivin implementoinnin antaman kritiikin kanssa johtivat siihen, että rahanpesulakia jouduttiin päivittämään, ks. kappale 4.3.1. Asiakkaan tuntemisvelvollisuus.
[163] Kimpimäki, 2015, s. 339.
[164] Valtiovarainministeriö, 2012-2022, s. 23.
[165] Valtiovarainministeriö 2012-2022, s. 24.
[166] Hyttinen, 2021, s. 40.

toteutuminen turvataan jäsenmaiden täyttäessä FATF:n asettamia velvoitteita. Vaatimukset ovat myös suhteellisen usein olleet ristiriidassa jäsenmaiden omien rikosoikeudellisten periaatteiden kanssa ja FATF:n toiminta on voinut jopa näyttäytyä niin, että rahanpesun estämisessä kaikki keinot ovat sallittuja. Suositusten on väitetty olevan sokeita kansallisille oikeuskulttuureille, systematiikalle ja traditioille. Puolustuksena on tuotu esiin, että rikosoikeuden alalla on harvemmin mahdollista jättää jokaiselle valtiolle suurta tulkinnanvaraa, jos rikoksia halutaan ehkäistä tehokkaasti. [167] Suomi joutui kahnauksiin FATF:n kanssa itsepesun kriminalisoinnin yhteydessä, kun Suomen tekemä lainsäädännöllinen kompromissi ei riittänyt FATF:lle, joka antoi kansainvälisestikin ymmärtää, että Suomi olisi itse asiassa jättänyt itsepesun ”täyskriminalisoimatta”.[168]

4.2 EU-lainsäädäntö ja rahanpesudirektiivit

Euroopan unioni on ottanut viime vuosikymmeninä vahvan roolin rahanpesun estämisessä. Merkittävimmät voimassaolevat direktiivit ovat niin sanotut neljäs ja viides rahanpesudirektiivi.[169] Alun perin tarkoituksena on ollut keskittyä erityisesti preventiivisiin toimiin, mutta viidennen rahanpesudirektiivin painotus on ollut jo selkeämmin rikosoikeuden harmonisoinnissa. Tämä on merkittävä käänne siinä mielessä, että rikosoikeuden on perinteisesti katsottu kuuluvan mahdollisimman laajasti jäsenvaltioiden oman päätäntävallan piiriin.[170] Kuten aiemmin jo sivuttiin, myös FATF:lla on ollut suuri vaikutus siihen, minkälaista rahanpesun sääntelyä EU:ssa on lähdetty viemään eteenpäin. Vaikutus ei kuitenkaan ole yksisuuntainen, vaan direktiivit ja niiden kansallinen toimeenpano vaikuttavat myös FATF:n linjauksiin.[171]

EU:n antama neljäs rahanpesudirektiivi kumosi kokonaisuudessaan sitä ennen voimassa olleen kolmannen rahanpesudirektiivin, sekä sitä täsmentävän komission direktiivin. Neljännen

[167] Hyttinen, 2021, s. 41.
[168] Ks. lisää Hyttinen, 2017, s. 334-361.
[169] Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/849 ja Euroopan parlamentin ja neuvoston direktiivi 2018/843.
[170] Valtioneuvosto on U-kirjelmässään U 1/2017 vp kommentoinut viidennen rahanpesudirektiivin aiheuttamien muutosten suhdetta toissijaisuusperiaatteeseen. Mietinnössä todetaan, että ”direktiiviehdotuksessa viitataan toissijaisuusperiaatteen osalta rahanpesun sekä siihen liittyvän terrorismirikollisuuden rajat ylittävään luonteeseen ja tarpeeseen toteuttaa kansainväliset kriminalisointivelvoitteet unionin alueella. Kattava ja riittävän yhdenmukainen oikeudellinen viitekehys on parhaiten saavutettavissa unionin tasolla, minkä vuoksi unioni voi hyväksyä toimenpiteitä. Valtioneuvosto pitää ehdotusta toissijaisuusperiaatteen mukaisena”. Valtioneuvoston kommenttia toissijaisuusperiaatteesta voidaan pitääs suhteellisen suppeana, vaikka kyseessä on merkittävä muutos unionin toimivaltaan.
[171] Hyttinen, 2021, s. 46.

rahanpesudirektiivin antamisen tarkoituksena oli päivittää jäsenmaiden rahanpesua koskeva preventiivinen sääntely 2010-luvulle. Mikäli tarkastellaan pelkästään rahanpesun estämisen ennakoivia toimia, on neljäs rahanpesudirektiivi edelleen yksi merkittävimpiä kansainvälisiä lainsäädännöllisiä instrumentteja rahanpesun estämiseksi, vaikkakin se kohdistuu suoraan vain EU:n jäsenvaltioihin. Tästä huolimatta sillä on ollut vahva vaikutus myös EU:n ulkopuolisiin valtioihin. [172]

Neljännen rahanpesudirektiivin jälkeen EU on antanut viidennen rahanpesudirektiivin tarkoituksenaan asettaa jäsenvaltioille virtuaalivaluuttoja koskevia velvoitteita ja direktiivin tarkoituksena olikin tältä osin olla neljättä rahanpesudirektiiviä täydentävä lisäsääntely. Viidennen rahanpesudirektiivin johdantokappaleen 9 kohdassa todetaan, että virtuaalivaluuttojen anonyymiys mahdollistaa niiden väärinkäytön rikollisiin tarkoituksiin, eikä virtuaalivaluuttojen ja fiat-valuuttojen välisten vaihtopalvelujen ja lompakkopalvelujen tarjoajien sisällyttäminen direktiivin soveltamisalaan poista kokonaan tätä anonyymiyden ongelmaa, sillä virtuaalivaluuttojen käyttäjät voivat edelleen halutessaan käyttää virtuaalivaluuttoja ilman näiden palveluntarjoajien alustoja. Direktiivin johdannossa jatketaan, että kansallisten rahanpesun selvittelykeskusten on voitava hankkia sellaisia tietoja, joiden avulla virtuaalivaluuttojen käyttäjien henkilöllisyys pystytään selvittämään ja EU-jäsenmaiden olisi myös tarkemmin selvitettävä mahdollisuutta sille, että käyttäjät voisivat tehdä vapaaehtoisia ilmoituksia viranomaisille.

Viidennen rahanpesudirektiivin johdannon kohdassa 12 todetaan myös, että liiketoimia suuririskisiin kolmansiin maihin tulisi rajoittaa silloin, kun näiden maiden rahanpesun ja terrorismin rahoittamisen torjuntatoimissa havaitaan suuria puutteita. Jäsenvaltioiden tulisi myös näiden suuririskisten maiden kanssa toimiessa vaatia tehostettua asiakkaan tuntemisvelvollisuutta ja soveltaa samanaikaisesti myös muita riskinvähentämistoimenpiteitä ja ottaa huomioon esim. FATF:n suositukset.

4.2.1 Maksajan tiedot-asetus

EU-lainsäädännössä tärkeä asetus rahanpesun ja terrorismin rahoittamisen näkökulmasta on ollut ns. maksajan tiedot-asetus[173], joka on säädetty FATF:n antamien suositusten

[172] Hyttinen, 2021, s. 51.
[173] Euroopan parlamentin ja neuvoston asetus 2015/847

mukaisesti.[174] Asetuksen 4 artiklassa määrätään, että maksajan käyttämän maksupalveluntarjoajan on varmistettava, että varainsiirtojen mukana toimitetaan tiettyjä tietoja maksajan henkilöllisyydestä. Asetuksen 7 artikla koskee maksupalveluntarjoajan velvollisuuksia ja artiklan 2 kohdassa todetaan, että maksunsaajan käyttämän maksupalveluntarjoajan on otettava käyttöön tehokkaat menettelyt, joiden avulla se havaitsee, puuttuuko maksajasta tai maksunsaajasta tietoja sellaisista varainsiirroista, joita he ovat siirtäneet unioniin tai unionin ulkopuolelle. FATF on antanut useita huomautuksia, että ”matkasääntöä” ei noudateta tarpeeksi tiukasti ja EU onkin pyrkinyt vastaamaan tähän uudella lainsäädäntöpaketilla, joka käsitellään myöhemmin kappaleessa 6.2.

4.3 Kotimainen lainsäädäntö – keskiössä ilmoitusvelvolliset ja asiakkaan tuntemisvelvollisuus

Suomessa on jo kauan vastattu rahanpesun ja terrorismin rahoittamisen haasteisiin pyrkimällä implementoimaan kansainvälisten toimijoiden, pääasiassa EU-lainsäädäntöä ja FATF:n antamia suosituksia. Vuonna 2017 Suomessa säädettiin Laki rahanpesun ja terrorismin rahoittamisen estämisestä (28.6.2017/444) (jäljempänä rahanpesulaki). Lain tavoitteena on sen 1 §:n mukaan *estää rahanpesua ja terrorismin rahoittamista, edistää tällaisen toiminnan paljastamista ja selvittämistä sekä tehostaa rikoksen tuottaman hyödyn jäljittämistä ja takaisinsaantia.* Virtuaalivaluuttojen tarjoajien ja käyttäjien kannalta lakiin tehtiin merkittävä muutos vuonna 2019, kun sen soveltamisalaan lisättiin lain 2 §:n 8 a-kohdan mukaisesti virtuaalivaluutan tarjoajista annetussa laissa tarkoitettu virtuaalivaluutan tarjoaja. Tämän muutoksen myötä virtuaalivaluuttojen tarjoajat tuotiin samojen velvoitteiden ja rahanpesulainsäädännön piiriin, kuin muutkin perinteiset finanssialan toimijat.

Lain 2 luvun 3 §:ssä säädetään ilmoitusvelvollisten velvollisuudesta laatia *riskiarvio* rahanpesun ja terrorismin rahoittamisen riskien tunnistamiseksi ja arvioimiseksi. Riskiarvio tulee päivittää säännöllisesti ja siihen tehtävät muutokset on toimitettava toimivaltaiselle valvontaviranomaiselle tai asianajajayhdistykselle tämän pyynnöstä ilman aiheetonta viivytystä. Rahanpesulakiin tehtiin tärkeä muutos vuonna 2021, kun asiakkaan tuntemista ja riskiperusteista arviointia koskevaa säännöstä täsmennettiin lisäämällä rahanpesun ja

[174] FATF on päivittänyt vuonna 2021 omaa ohjeistustaan niin, että suosituksen velvoite koskisi myös virtuaalivaluuttojen tarjoajia, ks, FATF, 2021. EU on lähtenyt vastaamaan tähän haasteeseen, ks. enemmän. kappale 6.2. EU:n maksajan tiedot-asetus on säädetty FATF:n antaman huomautuksen johdosta.

terrorismin rahoittamisen riskien huomioon ottamisen osalta maininta mm. uusista teknologioista.[175]

Päivitetyn lain 3 luvun 1 §:n 2 momentin mukaan,

> *Ilmoitusvelvollisen on asiakassuhteeseen liittyviä rahanpesun ja terrorismin rahoittamisen riskejä arvioidessaan otettava huomioon uusiin ja jo olemassa oleviin asiakkaisiin, maihin tai maantieteellisiin alueisiin sekä uusiin, kehitettäviin ja jo olemassa oleviin tuotteisiin, palveluihin ja liiketoimiin sekä jakelukanaviin ja teknologioihin liittyvät rahanpesun ja terrorismin rahoittamisen riskit (riskiperusteinen arviointi).*

Virtuaalivaluuttojen näkökulmasta olennainen oli myös muutos rahanpesulain 2 §:ään, jonka 1 momentissa todetaan, että

> *Ilmoitusvelvollisella ei saa olla tässä pykälässä säädettyjä poikkeuksia lukuun ottamatta anonyymeja tai tekaistuilla nimillä olevia tilejä tai asiakkuuksia. Ilmoitusvelvollisen on tunnistettava asiakkaansa ja todennettava tämän henkilöllisyys vakituista asiakassuhdetta perustettaessa. Lisäksi ilmoitusvelvollisen on tunnistettava asiakkaansa ja todennettava tämän henkilöllisyys, jos; - -*
>
> *c) kyse on virtuaalivaluutan tarjoajista annetussa laissa tarkoitetussa virtuaalivaluuttaan liittyvässä palvelussa tehdystä liiketoimesta, jonka määrä ylittää 1 000 euroa.*

Rahanpesulain 10 §:ssä säädetään tehostetusta asiakkaan tuntemisvelvollisuudesta. Siinä ilmoitusvelvolliset velvoitetaan soveltamaan tehostettua menettelyä asiakkaan tuntemiseksi, *mikäli edellä mainitussa riskiarviossa asiakassuhteeseen tai yksittäiseen liiketoimeen liittyy tavanomaista suurempi rahanpesun ja terrorismin rahoittamisen riski*.

Vuonna 2019 tuli voimaan myös Laki pankki- ja maksutilien valvontajärjestelmästä (571/2019). Lain tarkoituksena on sen 1 §:n 2 momentin mukaan *edistää viranomaisten sähköistä tiedonsaantia pankki- ja maksutileistä sekä tehostaa viranomaisten tiedustelujen oikeaa kohdentumista*. Lain avulla pyritään tarjoamaan toimivaltaisille viranomaisille oikeus käyttää pankki- ja maksutilien valvontajärjestelmää, jos se on välttämätöntä rahanpesun ja terrorismin rahoittamisen estämiseksi, paljastamiseksi ja selvittämiseksi. Tämän lisäksi viranomaisilla on mahdollisuus määrätä talouspakotteita tai varojen jäädytyksiä, joista

[175] HE 261/2020 vp, s. 5.

säädetään Suomessa tarkemmin Laissa varojen jäädyttämisestä terrorismin torjumiseksi (325/2014).

Lakien yksityiskohtaisen luettelemisen tai läpikäymisen sijaan on tärkeää ymmärtää, mihin lainsäädäntömme rahanpesun ja terrorismin rahoittamisen estämisessä ja ennaltaehkäisyssä perustuu ja miten rikoksia tosiasiallisesti pyritään estämään. Viranomaistoiminnan keskiössä on ilmoitusvelvollisten vastuu toimittaa viranomaisille lainmukaiset tiedot esimerkiksi varojen siirroista ja niiden taustalla olevista henkilöistä. Seuraavaksi esitellään lyhyesti keskeisimmät kotimaiset toimijat rahanpesun ja terrorismin rahoittamisen estämisen kentällä.

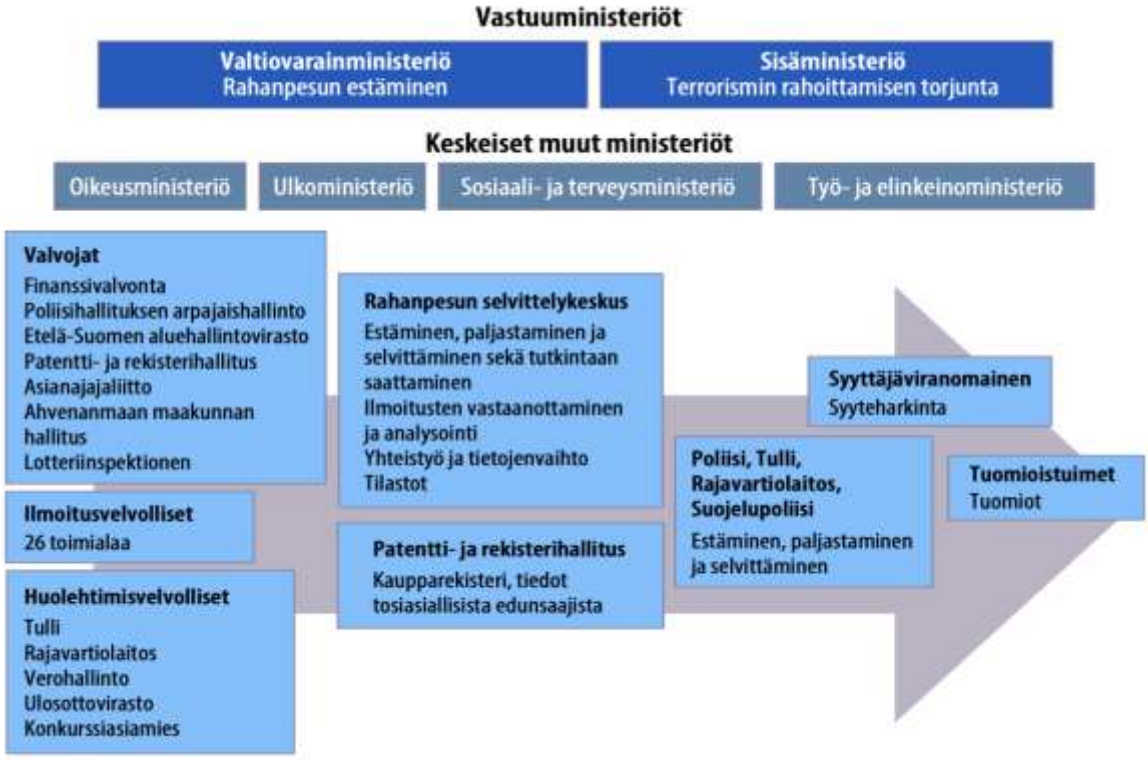
4.4 Kansalliset toimijat rahanpesun ja terrorismin rahoittamisen estämisessä

Suomessa on rahanpesulaissa asetettu valvontavelvoitteita useille eri viranomaisille ja asianajajayhdistykselle[176]. Valvontaviranomaisilla on valtuudet määrätä erilaisia hallinnollisia seuraamuksia rahanpesulaissa säädettyjen velvoitteiden laiminlyönnistä tai rikkomisesta. Hallinnollisen seuraamusjärjestelmän tarkoitus on ehkäistä lainvastaisen toiminnan harjoittamista tai vaihtoehtoisesti estää sen toistuminen. Tällaisia hallinnollisia seuraamuksia ovat esimerkiksi rikemaksu ja julkinen varoitus.[177]

Valtiovarainministeriö on tehnyt kyselytutkimuksen, jonka tarkoituksena on ollut kartoittaa organisaatioiden käytettävissä olevia rahanpesun ja terrorismin rahoittamisen torjunnan riittävyyttä ja resursseja ja sen perusteella havaittiin, että nykyiset resurssit koettiin riittämättömiksi.[178] Myös FATF on kiinnittänyt huomiota Suomea koskevassa maa-arvioraportissaan, että resurssit rahanpesun ja terrorismin rahoittamisen estämiseen ovat vähäiset.[179] Viranomaisten velvoitteet ovat lisääntyneet rahanpesulainsäädännön kehittymisen

[176] Asianajajayhdistystä koskee hallinnollisten seuraamusten suhteen erityissäännös, jonka mukaan yhdistyksellä täytyy tehdä seuraamuksen määräämiseksi erillinen esitys Etelä-Suomen aluehallintovirastolle. Valvontaviranomaiset voivat määrätä rikemaksun suoritettavaksi, mikäli ilmoitusvelvollinen tahallaan tai huolimattomuudesta rikkoo velvoitteitaan ja edellytyksenä silloinkin on, että velvoitteita laiminlyödään tai rikotaan vakavasti, toistuvasti ja järjestelmällisesti, Valtiovarainministeriön julkaisuja 2021:17, s 19-21.
[177] Valtiovarainministeriön julkaisuja 2021:17, s 20.
[178] Valtiovarainministeriön julkaisuja 2021:17, s. 22.
[179] FATF, 2019, s. 13. Raportissa puute on todettu seuraavasti: ”Finland should allocate adequate resources to AML/CFT supervisors, and specifically FIN-FSA and RSAA, including human resources to enable them to conduct their AML/CFT supervisory responsibilities in an adequate and effective manner”.

ja kansainvälistymisen myötä ja laajojen valvontakenttien hallitsemiseksi tarvittaisiin laajempia resursseja.[180]



Keskeiset toimijat rahanpesun ja terrorismin rahoittamisen estämisessä Suomessa. [181]

4.4.1 Rahanpesun selvittelykeskus

Suomessa yksi tärkeimmistä toimijoista rahanpesun ja terrorismin rahoittamisen estämisessä on KRP:n alaisuudessa toimiva rahanpesun selvittelykeskus. Se on myös merkittävä tiedon vastaanottaja rahanpesu- ja terrorismirikosten sekä muiden talousrikosten selvittelyssä. Selvittelykeskus tekee myös kansanvälistä yhteistyötä ja sillä on edellytykset muodostaa yksittäisten tapausten perusteella laajempaa kuvaa siitä, mihin suuntaan kokonaiskuva on menossa ja ottaa osaa myös suurempien kansainvälisten tapausten selvittelyyn. [182]

Rahanpesun selvittelykeskuksen tehtävistä on säädetty laissa rahanpesun selvittelykeskuksesta (445/2017).[183] Lain 2 §:n mukaan selvittelykeskuksen tehtävänä on;

[180] Valtiovarainministeriön julkaisuja 2021:17, s.22.
[181] Valtiovarainministeriön julkaisuja 2021:17, s. 19.
[182] Andérsen, 2020, s. 153.
[183] Ks. lisää HE 228/2016.

1) *rahanpesun ja terrorismin rahoittamisen estäminen, paljastaminen ja selvittäminen sekä tutkintaan saattaminen;*
2) *rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain (444/2017) 4 luvun 1 §:ssä tarkoitettujen ilmoitusten vastaanottaminen ja analysointi sekä palautteen antaminen niiden vaikutuksista;*
3) *yhteistyö viranomaisten kanssa rahanpesun ja terrorismin torjunnassa;*
4) *yhteistyö ja tietojenvaihto rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä huolehtivien vieraan valtion viranomaisten ja kansainvälisten järjestöjen kanssa;*
5) *yhteistyö ilmoitusvelvollisten kanssa*
6) *tilaston pitäminen rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain 4 luvun 1 §:ssä tarkoitettujen ilmoitusten ja mainitun luvun 5 §:ssä säädettyjen liiketoimien keskeytysten lukumäärästä, tutkintaan saatettujen epäilyttäviä liiketoimia koskevien ilmoitusten lukumäärästä sekä tehdyistä, vastaanotetuista, evätyistä ja vastatuista tietopyynnöistä;*
7) *varojen jäädyttämisestä terrorismin torjumiseksi annetun lain (353/2013) 3 §:n 2 momentissa tarkoitettujen ilmoitusten vastaanotto ja käsittely, mainitun lain 4 §:ssä tarkoitettujen jäädyttämispäätösten edellytysten selvittäminen ja jäädyttämispäätöksiä koskevien esitysten tekeminen;*
8) *operatiivisten ja strategisten analyysien tekeminen koskien rahanpesun ja terrorismin rahoittamisen ja sen rikoksen, jolla rahanpesun tai terrorismin rahoittamisen kohteena oleva omaisuus tai rikoshyöty on saatu tai saataisiin, tekotapoja, ilmiöitä, suuntauksia ja menetelmiä.*

Saman pykälän 4 momentissa todetaan vielä, että KRP:n tulee antaa vuosittain Poliisihallitukselle selvitys rahanpesun selvittelykeskuksen toiminnasta rahanpesulain 4 luvun 1 §:ssä tarkoitettujen ilmoitusten ja tämän lain 6 §:ssä tarkoitettujen liiketoimien keskeyttämistä koskevien määräysten lukumääristä sekä rahanpesun ja terrorismin rahoittamisen vastaisen toiminnan yleisestä edistymisestä Suomessa.

Siinä vaiheessa, kun ilmoitusvelvollinen on havainnut tarpeen ilmoituksen tekemisestä, tulee tämän tehdä ilmoitus Rahanpesun selvittelykeskukselle joko sähköisesti verkossa tai lomakkeella. Ilmoituksen voi tehdä niin organisaation edustajana kuin yksityishenkilönäkin.[184] Vaikka selvittelykeskukselle on asetettu lainsäädännössä runsaasti velvoitteita, keskuksella on kuitenkin rajalliset resurssit ja jatkuvasti lisääntyvän sääntelyn maailmassa niitä on entisestään kohdennettava olennaisimpiin toimintoihin. Jotta tulevaisuudessakin terrorismin rahoittamista

[184] Andérsen, 2020, s. 155.

ja rahanpesua voitaisiin tehokkaasti ehkäistä ja samalla säilyttää toiminnan laadukas taso, tulee selvittelykeskuksen resursseja merkittävästikin lisätä.[185]

Lain rahanpesun selvittelykeskuksen tehtävistä 5 §:ssä säädetään myös eräitä viranomaisia koskevasta yleisestä huolehtimisvelvoitteesta siten, että tulli-, rajavartio-, vero- ja ulosottoviranomaisen sekä konkurssiasiamiehen on huolehdittava siitä, että sen toiminnassa kiinnitetään huomiota rahanpesun ja terrorismin estämiseen ja paljastamiseen sekä tehtäviensä hoidon yhteydessä ilmi tulleiden epäilyttävien liiketoimien tai terrorismin rahoittamisen epäilyn ilmoittamisen rahanpesun selvittelykeskukselle.

[185] Andérsen, 2020, s. 155.

5. Virtuaalivaluutat kansallisessa riskiarviossa – rikollisuuden määrä kasvussa

5.1 Kansallisen rahanpesun selvittelykeskuksen riskiarvio

Neljännen rahanpesudirektiivin säätämisen yhteydessä asetettiin Euroopan komissiolle velvoite laatia riskiarvio niistä rahanpesun ja terrorismin rahoittamisen riskeistä, jotka liittyvät rajat ylittäviin toimiin. Tätä riskiarviota kutsutaan SNRA:ksi, eli Supra National Risk Assessmentiksi ja se on saatettava ajan tasalle vähintään kahden vuoden välein ja tarvittaessa useamminkin. [186] Osana näitä estämistoimia myös Suomen tulee laatia oma kansallinen riskiarvionsa. Arviossa on arvioitava ja tunnistettava niitä kansallisia riskejä ja uhkia, joita liittyy rahanpesuun ja terrorismin rahoittamiseen. Tässä arviossa on otettava huomioon myös edellä mainittu ylikansallinen riskiarvio. Rahanpesulaissa sisäministeriö on velvoitettu vastaamaan kansallisen terrorismin rahoittamisen riskiarvion laadinnasta ja valtiovarainministeriö taas rahanpesuun liittyvästä vastaavasta riskiarviosta. Riskiarvion lisäksi laaditaan myös toimintasuunnitelma, jossa esitetään keinoja niiden riskien pienentämiseksi, joita riskiarviossa nostetaan esiin. [187] Olennainen osa tätä työtä on myös arvioida sitä, että rahanpesun ja terrorismin rahoittamisen estämiseksi tehtävät toimet ovat oikeassa suhteessa rikosten aiheuttamiin haittoihin nähden. FATF ja EU edellyttävät kuitenkin vahvoja toimia näiden rikosten estämiseksi ja nämä toimet on myös tuotava esille toimintasuunnitelmassa (ns. Action Plan), joka laaditaan riskiarvion pohjalta.[188]

Valtiovarainministeriö on riskiarviossaan 2021 määritellyt riskin siten, että sillä tarkoitetaan uhan, haavoittuvuuden ja seurauksen yhdistelmästä koostuvaa tekijää. Tämä perustuu FATF:n määritelmiin, joiden mukaan uhka on ”henkilö tai ryhmä ihmisiä, esine tai toimintaa, joka voi aiheuttaa haittaa esimerkiksi valtiolle, yhteiskunnalle tai taloudelle.” FATF:n mukaan rahanpesussa ja terrorismin rahoittamisessa näihin lukeutuu rikolliset ja terroristiryhmät, heidän varansa ja ne toimijat, jotka edistävät heidän toimintaansa. Uhka on yleensä juuri tyypillisin lähtökohta, kun arvioidaan rahanpesuun ja terrorismin rahoittamiseen liittyviä riskejä. [189]

[186] Finanssivalvonta, 2021. Ylikansallinen riskiarvio, suora linkki https://www.finanssivalvonta.fi/paaomamarkkinat/rahanpesun-estaminen/riskiarvio/.
[187]Finanssivalvonta, 2021, Kansallinen riskiarvio, suora linkki https://www.finanssivalvonta.fi/paaomamarkkinat/rahanpesun-estaminen/riskiarvio/
[188] Valtiovarainministeriön julkaisuja 2021:17, s. 12.
[189] FATF, 2013, s. 8.

FATF:n mukaan haavoittuvuudet ovat niitä asioita, joihin uhat voivat iskeä ja joita ne voivat hyödyntää. Haavoittuvuudet voivat edesauttaa tai tukea uhkien realisoitumista ja ne voivat olla esimerkiksi jonkin sektorin tai palvelun tyyppejä, jotka tekevät ne erityisen alttiiksi terrorismin rahoittamiselle ja rahanpesulle.[190] Virtuaalivaluutat edustavat selkeästi tällaista haavoittuvuutta. Kolmas FATF:n laatiman riskin määritelmän osanen on seuraus ja sillä tarkoitetaan kaikkia niitä vaikutuksia ja haittoja, joita terrorismin rahoittaminen ja rahanpesu aiheuttavat. Nämä rikolliset toimet aiheuttavat monenlaisia vaikutuksia rahoitusjärjestelmiin, talouteen ja yhteiskuntaan. [191]

Rahanpesun selvittelykeskus on laatinut vuosikertomuksen vuodelta 2020 ja puolivuosikatsauksen vuodelta 2021. Vuoden 2021 vuosikertomuksessa kerrotaan, että erityisesti pankkien tekemien epäilyttävää liiketoimea koskevien ilmoitusten määrän jatkuva kasvu sekä virtuaalivaluutan tarjoajat uutena ilmoitusvelvollisryhmänä ovat olleet merkittävä tiedon lähde selvittelykeskuksen keskeisimmässä tehtävässä, eli rahanpesun ja terrorismin rahoittamisen estämisessä, paljastamisessa ja selvittämisessä sekä tutkintaan saattamisessa. [192]

Sen jälkeen, kun virtuaalivaluutan tarjoajat tulivat ilmoitusvelvollisiksi joulukuussa 2019, ovat ne vuoden 2020 aikana tehneet selvittelykeskukselle 9000 ilmoitusta.[193] Vuoden 2021 puolivuosikatsauksessa vuoden puoliväliin mennessä virtuaalivaluuttojen tarjoajien tekemät rahanpesuilmoitukset olivat jo kasvaneet valtavasti ja niiden määrä oli 3 439 842. Kasvu selittyy osin niillä muutoksilla, joita on tapahtunut ilmoittajatahojen raportointikäytänteiden muutoksilla. Osa vuoden 2021 alkupuolen ilmoituksista on myös takautuvia ilmoituksia vuosilta 2020 ja 2019. [194] Puolivuosikatsauksessa todetaan, että virtuaalivaluuttoihin liittyvän suuren ilmoitusmäärän takia näitä ilmoituksia tullaan tarkastelemaan vuoden 2021 vuosikertomuksessa muista ilmoittajaryhmistä erillään. [195]

Vuonna 2020 muiden kuin virtuaalivaluuttoihin liittyvien ilmoitusten määrä laski jonkin verran, mutta vuoden 2021 alkupuolella nousua on taas tapahtunut ja vuoden alkupuoliskon ilmoitusmäärä on ylittänyt vuoden takaiset vastaavat lukemat. Virtuaalivaluuttapalvelujen

[190] FATF, 2013, s. 7.
[191] FATF, 2013, s. 7.
[192] Rahanpesun selvittelykeskus, 2020, s. 1.
[193] Rahanpesun selvittelykeskus, 2020, s. 4.
[194] Rahanpesun selvittelykeskus, 2021, s. 1.
[195] Vuoden 2021 vuosikertomus tullaan julkaisemaan vuoden 2022 aikana ja se on löydettävissä osoitteesta https://poliisi.fi/katsauksia-ja-raportteja-rahanpesun-ja-terrorismin-rahoituksen-torjunnasta .

tarjoajien ilmoitusvelvollisuus on saanut aikaan pienen kasvusysäyksen ilmoitusten määrissä. Selvittelykeskus pyrkii vastaamaan ilmoitusten määrän nousevaan trendiin mm. kehittämällä ilmoitusten käsittelyn automaatiota ja priorisoimalla toiminnassaan ilmoitusten käsittelyä. 1.7.2021 on myös käynnistetty ns. ILMO-hanke, jolla pyritään entisestään kehittämään ilmoitusten käsittelyn automatisointia. [196]

Vuonna 2020 selvittelykeskuksen toimintaa on kehitetty kiivaasti ja etenkin rahanpesurekisterin toiminnan varmistamiseen on panostettu. Keskuksessa on myös käynnistetty hanke (RANKKA), jotta rahanpesun ja terrorismin rahoittamisen estämisessä voitaisiin alkaa hyödyntämään tekoälyä. Selvittelykeskus pyrkii jatkamaan näitä hankkeita ja saamaan niihin rahoitusta keskuksen digitalisaation edistämiseksi mm. EU:n elpymis- ja palautumistukivälineestä. Selvittelykeskus käynnisti myös vuonna 2020 Finanssiala ry:n, kaikkien pankkien ja Veikkauksen kanssa operatiivisen viranomaisten ja ilmoitusvelvollisten AML-asiantuntijaryhmän toiminnan. Vuoden 2020 aikana selvittelykeskus on tarjonnut merkittävän määrän asiantuntijuutta ja tarjonnut tietoa FATF:n ja YK:n terrorismin vastaisen komitean tarpeisiin. Selvittelykeskus on myös tukenut Suomen kansallisen riskiarvion laatimista rahanpesusta ja terrorismin rahoittamisesta sekä osallistunut lainsäädäntöhankkeisiin. [197]

Rahanpesun selvittelykeskuksen 2020 vuosikertomuksen mukaan perinteiseksi luokiteltavissa petosilmiöissä (esim. helpdesk-huijaukset) on alettu käyttämään enenevissä määrin virtuaalivaluuttoja. Helpdesk-huijauksessa rikolliset soittavat potentiaaliselle uhrille esittäytyen Microsoftin helpdesk-avustajana. Huijauksissa huijari pyrkii yleensä saamaan uhrin suorittamaan verkkopankissaan maksun, jolloin huijari samaan aikaan asentaa uhrin tietokoneelle etäkäyttöohjelman, jolla saadaan kaapattua uhrin tiedot. Isossa osassa tapauksia nämä maksut on ohjattu uhrin tietämättä virtuaalivaluutan vaihtopalveluille, joille on uhrin henkilötiedoilla avattu virtuaalivaluuttalompakko. Näistä lompakoista varat on siirretty hyvin nopeasti eteenpäin huijareiden omiin lompakoihin, minkä seurauksena varojen takaisin saaminen ja niiden jäljittäminen on ollut hyvin haastavaa.[198]

Vuosikertomuksen mukaan virtuaalivaluuttasijoittamiseen liittyvien huijausten määrä on jatkanut kasvuaan Euroopassa. Sijoitusmaailmaan liittyvissä huijauksissa tekijät ovat yleensä

[196] Rahanpesun selvittelykeskus, 2021, s. 2.
[197] Rahanpesun selvittelykeskus, 2020, s. 5.
[198] Rahanpesun selvittelykeskus, 2020, s. 14.

vahvasti organisoituneita ja taitavia. Potentiaalisille uhreille soitellaan eri puolilta Eurooppaa ja tarjotaan uusia sijoituskohteita, jotka vaikuttavat ulospäin ammattimaisilta ja vaikuttavilta. Huijarit ovat luoneet sijoitusalustoja, joiden avulla uhrit voisivat seurata sijoitustensa kehittymistä. Näiden alustojen antamat tiedot ovat kuitenkin olleet virheellisiä ja todelliset varat on siirretty uhrin ulottumattomiin esimerkiksi eri virtuaalivaluuttojen vaihtelupalveluihin siinä vaiheessa, kun huijaus paljastuu.[199]

Suomessa on poliisille tulleiden ilmoitusten perusteella ollut jo sadoittain sijoitushuijauksien uhreja, mutta yleensä näiden rikosten tekijöiden yhteyttä Suomeen on ollut hankala osoittaa. Muualla Euroopassa tässä on myös onnistuttu ja esim. Ranskassa on käynnistetty tutkintoja investointipetoksiin liittyen ja onnistuttu saamaan näitä rikoksia tehtailevien verkostojen osia kiinni. Rahanpesun selvittelykeskus on ollut mukana näissä Euroopan laajuisissa tutkinnoissa esimerkiksi tunnistamalla Suomessa asuvia uhreja, tiedottamalla näistä rikoksista ja ilmiöistä ilmoitusvelvollisille tahoille Suomessa ja tekemällä analyysejä virtuaalivaluuttatransaktioista.[200]

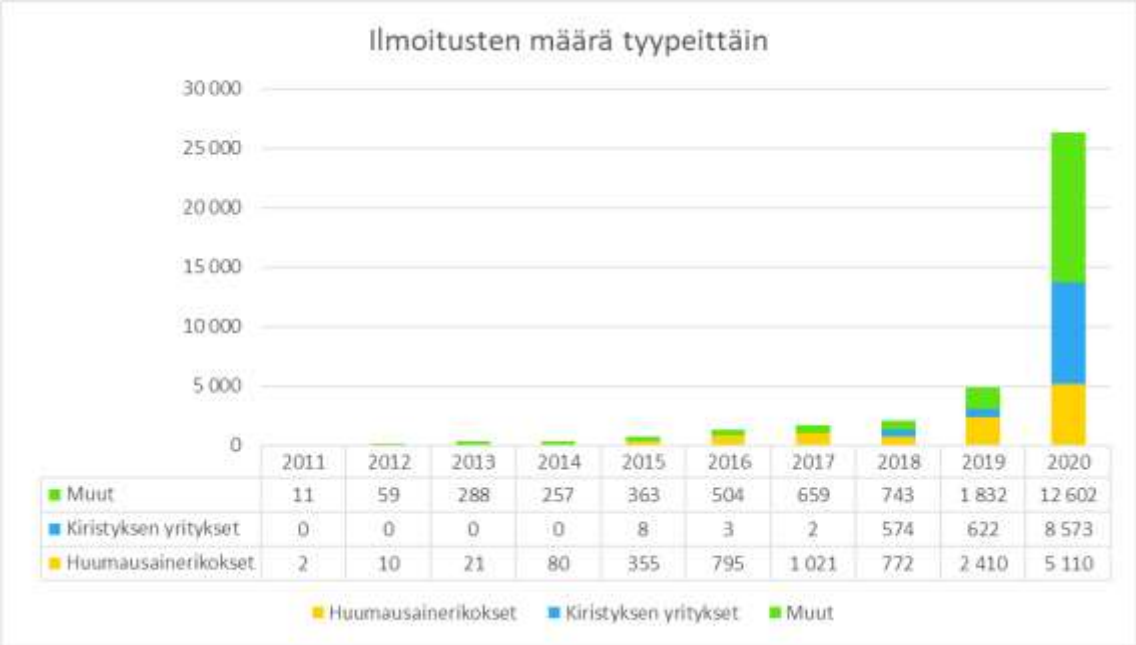
5.1.1 Virtuaalivaluutat ja rahanpesu

Rahanpesun selvittelykeskuksen vuoden 2020 vuosikertomuksessa kerrotaan, että vuosi 2020 oli selvittelykeskuksen virtuaalivaluuttaosaajille erittäin kiireinen. Käynnissä oli esimerkiksi valtakunnallisestikin merkittäviä esitutkintoja, joissa virtuaalivaluutat näyttelivät merkittävää roolia. Asiantuntijoita pyydettiin usein erilaisiin koulutuksiin kouluttajaksi ja myös oikeudenkäynteihin asiantuntijatodistajiksi.[201]

Kuten aiemmin on jo tuotu esiin, virtuaalivaluutan tarjoajat ovat 1.12.2019 lähtien olleet velvollisia ilmoittamaan epäilyttävistä liiketoimista ja mahdollisesta terrorismin rahoittamisesta rahanpesun selvittelykeskukselle. Tämän muutoksen johdosta selvittelykeskuksella on myös oikeus määrätä virtuaalivaluuttalompakoissa tapahtuvat toimet keskeytettäväksi, mikäli se on välttämätöntä sen selvittämiseksi, ovatko liiketoimet laillisia. [202] Vuoden 2020 aikana näitä määräyksiä tehtiin useita, yhteensä yli sadan bitcoinin arvosta.[203]

[199] Rahanpesun selvittelykeskus, 2020, s. 14.
[200] Rahanpesun selvittelykeskus, 2020, s.15.
[201] Rahanpesun selvittelykeskus, 2020, s. 30.
[202] Rahanpesun selvittelykeskus, 2020, s. 30.
[203] Vuoden 2020 aikana yhden bitcoinin arvo vaihteli vuoden alun (1.1.2020) n. 6500 eurosta loppuvuoden (31.12.2020) n. 40 000 euroon. Bitcoinin kurssi haettu osoitteesta https://coinmotion.com/fi/ .

Virtuaalivaluuttoihin liittyvät rikosilmoitukset ovat olleet tasaisessa kasvussa aina vuodesta 2011 saakka. Vuonna 2020 niissä kuitenkin tapahtui dramaattinen kasvu, joka näyttää jatkuneen vuonna 2021. Vuoden 2020 kasvua voidaan selittää osin huumausainerikosten kasvulla ja laajoilla tietoverkkorikoksilla. [204]



	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Muut	11	59	288	257	363	504	659	743	1 832	12 602
Kiristyksen yritykset	0	0	0	0	8	3	2	574	622	8 573
Huumausainerikokset	2	10	21	80	355	795	1 021	772	2 410	5 110

Rahanpesun selvittelykeskus on havainnollistanut vuosikertomuksessaan 2020 virtuaalivaluuttoihin liittyvien ilmoitusten määrän kasvua yllä olevalla kuvaajalla. Tiedot ovat peräisin Poliisiasiain tietojärjestelmästä. [205]

Vuoden 2020 Covid-tilanne aiheutti sen, että kansainvälinen yhteistyö virtuaalivaluuttaosaajien keskuudessa supistui pelkästään virtuaaliseksi ja tavanomaiseksi tiedonvaihdoksi. Kotimaisten viranomaisten (syyttäjälaitos, veroviranomaiset jne.) keskuudessa taas yhteistyötä tehtiin sen sijaan runsaasti.[206]

Valtiovarainministeriö on riskiarviossaan arvioinut virtuaalivaluuttasektoriin kohdistuvaksi kokonaisriskitasoksi 4, mikä tarkoittaa erittäin merkittävää riskiä. Arviossa huomautetaan, että myös Finanssivalvonta on vuonna 2020 arvioinut, että virtuaalivaluuttapalvelut ja ns. sähköraha (e-money) ovat merkittävän riskin palveluita. Riskitason arviointiin on osallistunut 19 asiantuntijaa niin yksityiseltä, kuin julkiseltakin sektorilta. [207]

[204] Rahanpesun selvittelykeskus, 2020, s. 31.
[205] Rahanpesun selvittelykeskus, 2020, s. 31.
[206] Rahanpesun selvittelykeskus, 2020, s. 32.
[207] Valtiovarainministeriön julkaisuja 2021:17, s.63.

Riskiarvion mukaan erityisen merkittävän riskin ja uhan muodostavat järjestäytyneet rikollisryhmät, jotka käyttävät virtuaalivaluuttoja rahanpesussa. Riskiä nostaa tässä jo esille tuotu virtuaalivaluutoille ominainen anonymiteetti tai pseudoanonymiteetti, minkä vuoksi varoja on hankalaa tai mahdotonta jäljittää ja varojen alkuperää selvittää. Riskiskenaariossa valtiovarainministeriö on myös arvioinut mahdollista tilannetta, jossa jokin rikollisryhmä luo oman uuden virtuaalivaluuttansa tai vaihtoehtoisesti lohkoketjuhankkeen, jota käytetään petos- ja rahanpesurikoksiin. Virtuaalivaluuttatoimijoiden suuren määrän takia olisi hyvin hankalaa tunnistaa ne lohkoketjut, jotka on luotu rikollisten tarkoitusperien pohjalta.[208]

Erittäin merkittävänä riskinä riskiarviossa pidetään myös sitä, että varojen alkuperän selvittäminen jää puutteelliseksi. Perinteisiin finanssisektorin toimijoihin verrattuna virtuaalivaluutan tarjoajien mahdollisuudet selvittää varojen alkuperä on huomattavasti heikompi. Näiden toimijoiden siirryttyä valvonnan piiriin vuonna 2019 vaikuttaa tosin todennäköisesti positiivisesti näiden toimintamallien kehittymiseen.[209]

Riskiarvion mukaan maantieteelliset riskit ovat myös merkittäviä riskejä virtuaalivaluutan tarjoajien osalta. Toimijoiden rahanpesuriskiä nostavat niin etätunnistamisen valtavirtaisuus ja niiden käytettävyyteen eri valtioissa liittyvät haasteet, globaalit asiakkaat, erilaiset toimintatavat ja se, että kansainvälisiä kaikkia sitovia standardeja ei vielä ainakaan laajasti ole käytössä. Virtuaalivaluuttoja on myös mahdollista hajauttaa eri vaihtopalveluihin. Vaihtopalvelujen suuren määrän takia virtuaalivaluuttojen alkuperää voidaan tehokkaasti häivyttää useita vaihtopalveluja käyttämällä. Riskiarviossa mainitaan uhkana myös ns. mixer-palvelut, joiden avulla pyritään katkaisemaan virtuaalivaluuttojen jäljitettävyys. [210]

Seuraava riskiarviossa mainittu merkittävä riski virtuaalivaluuttojen tarjoamisessa on transaktioiden reaaliaikaisuus, jonka johdosta varoja on mahdollista siirtää nopeasti viranomaisten ulottumattomiin. Näihin transaktioihin ei ole myöskään mahdollista soveltaa varojen palautuspyyntöä, sillä virtuaalivaluuttatransaktioita ei voida peruuttaa. Riskiarvion mukaan myös näiden transaktioiden suuri määrä nostaa rahanpesuriskiä. [211] Kuten edellä on esitetty, lohkoketjuteknologian takia (tai ansiosta) lohkoketjuja ja siinä tehtyjä transaktioita ei ole mahdollista jälkeenpäin muuttaa. Rahanpesuriskiin vaikuttaa olennaisesti myös se, että ala

[208] Valtiovarainministeriön julkaisuja 2021:17, s. 63.
[209] Valtiovarainministeriön julkaisuja 2021:17, s. 63.
[210] Valtiovarainministeriön julkaisuja 2021:17, s. 64. Ks. mixer-palvelut, kappale 2.2.3.
[211] Valtiovarainministeriön julkaisuja 2021:17, s. 64.

muuttuu jatkuvasti ja nopealla tahdilla. Alan nopeatahtisuus vaatii paljon resursseja, joita ei ole koettu olevan riittävästi.

Suomessakin ainakin suurimpiin kaupunkeihin on voinut nähdä ilmestyvän kauppakeskuksiin virtuaalivaluutta-automaatteja, yleensä bitcoin-automaatteja.[212] Valtiovarainministeriön riskiarviossa automaattien on mainittu olevan haavoittuvaisia väärinkäytöksille. Automaattien kautta rikoksella ansaittu raha on helposti muutettavissa virtuaalivaluutaksi ja vastaavasti rikoshyöty käteiseksi.[213]

Virtuaalivaluutan tarjoajien keskinäinen tietojen vaihtaminen on myös havaittu riskiksi siinä tapauksessa, mikäli sitä ei tapahdu heidän välillään. Tietojen saannin ongelmat voivat johtaa siihen, että virtuaalivaluuttasektoriin kohdistuvia rahanpesuriskejä ei tunnisteta ja näin ollen torjua tehokkaasti tietämyksen ollessa aukollista ja hajanaista.[214]

5.1.2 Virtuaalivaluutat ja terrorismin rahoittaminen

Terrorismin rahoittamisesta ei ole Suomessa annettu yhtään lainvoimaista tuomiota. Tämä vaikuttaa väistämättä siihen, että riskien arviointi ja niiden ennaltaehkäisy on haastavaa, sillä mitään konkreettisia tapausesimerkkejä ei ole. Nämä asiat ovat valtiovarainministeriön riskiarvion mukaan koettu haasteeksi niin yksityisellä, kuin julkisellakin sektorilla. Terrorismin rahoittaminen myös usein niputetaan yhteen rahanpesun kanssa, vaikka terrorismin rahoittamisessa on useita poikkeavia piirteitä rahanpesuun nähden. Selkeän ohjeistuksen puuttuessa toimijoiden menetelmät terrorismin rahoittamisen estämiseksi eivät myöskään välttämättä ole kovin tehokkaita.[215]

Yksi selittävä tekijä sille, että terrorismin rahoittamisesta ei ole Suomessa paljon oikeuskäytäntöä, on se, että terrorismin rahoittamisen tunnusmerkistön täyttyminen edellyttää rahoittajalta tietoisuutta siitä, että varoja käytetään nimenomaan tietyntyyppiseen terroristiseen tekoon. Tämän on todettu käytännössä olevan hyvin hankalaa näyttää toteen. Terroristiset teot tapahtuvat tämän lisäksi yleensä kriisialueilla, joista selvitystä ei usein ole mahdollista saada lainkaan. [216] Oikeusministeriön työryhmä on kuitenkin mietinnössään todennut, että ”jotakin

[212] Esimerkiksi Oulussa tällainen automaatti löytyy ydinkeskustan Valkea-kauppakeskuksesta.
[213] Valtiovarainministeriön julkaisuja 2021:17, s. 64.
[214] Valtiovarainministeriön julkaisuja 2021:17, s.64.
[215] Valtiovarainministeriön julkaisuja 2021:17, s.79.
[216] Valtiovarainministeriön julkaisuja 2021:17, s. 79.

rikosta koskevat näytön hankkimiseen ja arviointiin liittyvät haasteet eivät ole - - sellaisenaan peruste säätää rangaistavaksi jokin uusi samankaltainen rikos, jonka tunnusmerkistötekijöiden voidaan arvioida olevan helpommin toteen näytettäviä."[217]

Terrorismin rahoittamisen tunnistaminen voi olla vaikeaa myös siksi, että usein siihen käytetyt varat ovat laillisista lähteistä saatuja, esimerkiksi tavallisia palkkatuloja. Tämän lisäksi rahanlähteinä ovat Euroopassa toimineet mm. sosiaalituet ja hyväntekeväisyyteen liittyvät rahankeräykset.[218] Jihadistiselle liikehdinnälle on Euroopassa ominaista se, että hyvin suppea joukko tietää tai on perillä yksityiskohdista ja kynnys sille, että asioista kerrottaisiin eteenpäin, on erittäin korkea.[219] Suomesta on lähetetty ja täällä on kerätty varoja aseellisille ryhmittymille (esim. al-Shabaab) ja niiden jäseninä toimineille henkilöille.[220]

Riskiarviossa todetaan, että varojen loppukäyttäjän tunnistaminen on monilla sektoreilla haasteellista. Jo edellä mainituilta ulkoministeriön pakotelistoilta toimijoilla on mahdollisuus tunnistaa joitain henkilöitä tai mahdollisesti tiettyjen indikaattoreiden perusteella muita epäilyttäviä henkilöitä ja kieltäytyä yhteistyöstä heidän kanssaan. Mikäli asiakkuus ei muuten herätä epäilyksiä, on toimijoilla tosiasiallisesti heikohkot mahdollisuudet selvittää varojen tosiasialliset saajat, jos muita selkeitä indikaattoreita ei ole. Etätunnistamiseen suhtaudutaan usein myös hieman epäilevästi ja toimijat voisivatkin hyötyä vahvasta sähköisestä tunnistamisesta ja niihin liittyvistä suosituksista.[221]

5.1.3 Virtuaalivaluutan tarjoajiin liitännäiset terrorismin rahoittamisen riskit

Riskiarviossa virtuaalivaluutan tarjoajiin kohdistuva kokonaisriskitaso terrorismin rahoittamiseen on merkittävä. Tähän arviointiin on osallistunut yhteensä 20 asiantuntijaa niin yksityiseltä, kuin julkiseltakin sektorilta. Kuten edellä jo rahanpesun kohdalla, myös terrorismin rahoittamisen ilmiöiden ja riskien tunnistaminen on virtuaalivaluutan tarjoajien sektorilla koettu haastavaksi. Tässäkin syynä on kyseisen toimialan uutuus, minkä johdosta alalle ei ole ehtinyt muodostua selkeää riskiskenaariota terrorismin rahoittamisrikoksista.

[217] Oikeusministeriön julkaisuja: Mietintöjä ja lausuntoja 2020:8, s. 56.
[218] Sisäministeriön julkaisuja 2019:14, s.91.
[219] Sisäministeriön julkaisuja 2019:14, s. 19.
[220] Sisäministeriön julkaisuja 2019:14, s.91.
[221] Valtiovarainministeriön julkaisuja 2021:17, s.80.

Virtuaalivaluutan tarjoajat ovat myös niin uusi ilmoitusvelvollisten ryhmä, että niiden sisäiset prosessit eivät ole vielä ehtineet muotoutua valmiiksi. [222]

Riskiarviossa on nähty haavoittuvuuden näkökulmasta erittäin suureksi riskiksi se, että transaktioita on hyvin hankala valvoa niiden suuren määrän ja rajat ylittävän luonteen vuoksi. Virtuaalivaluuttasektori on lähtenyt kehittymään suhteellisen sääntelemättömässä ympäristössä ja se on nopeassa ajassa pyritty tuomaan sääntelyn piiriin, eivätkä monitorointijärjestelmät ole ehtineet kehittyä vastaamaan tarpeita. Nämä erot eri järjestelmien välillä (virtuaalivaluutan tarjoajat vs. perinteinen pankkijärjestelmä) voivat riskiarvion mukaan johtaa siihen, että potentiaaliset terrorismin rahoittajat päättävät valita virtuaalivaluutan tarjoajan perinteisen pankin ohi, sillä kiinnijäämisen riski ei välttämättä ole niin suuri.[223] Virtuaalivaluuttojen houkuttelevuutta voi kuitenkin vähentää se, että niitä ei ainakaan vielä useinkaan hyväksytä maksuvälineiksi perinteisessä palveluiden ja tavaroiden kaupassa. [224]

Riskiarviossa ETA-alueen ulkopuolisia asiakkaita pidetään erittäin merkittävänä maantieteellisenä riskinä. Riski on suuri etenkin silloin, kun vahvaa sähköistä tunnistautumista ei voida käyttää. Asiakkaat toimittavat näissä tapauksissa muita tunnistautumisasiakirjoja, joiden todenmukaisuutta voi olla vaikea arvioida. Myös varojen siirrot ETA-alueen ulkopuolelle koetaan riskinä, sillä siirtojen todellisia syitä on vaikea saada selville. [225] Kuten rahanpesussa, myös terrorismin rahoittamisessa virtuaalivaluutoille ominainen anonymiteetti ja pseudoanonymiteetti luetaan merkittäväksi riskiksi. Tämän lisäksi suurena riskinä on terrorismin rahoittamiseen käytettävien varojen kerääminen jo alun alkaenkin virtuaalivaluuttana. Näitä voivat olla esimerkiksi jo aiemmin esiin tuodut hyväntekeväisyyskeräyksiksi naamioidut keräykset.

KRP:lla on sen rahanpesukeskuksen erityisselvittelyryhmässä virtuaalivaluuttojen ja terrorismin rahoittamisen torjunnan selvittelytoiminnot. Selvittelykeskuksen vuosikertomuksen mukaan terrorismin rahoittamisen estämisen asiantuntijoita työllistivät erityisesti laajat selvittelykokonaisuudet, jotka liittyivät Suomessa mahdollisesti toimiviin

[222] Valtiovarainministeriö, 2021, s.93.
[223] Valtiovarainministeriö, 2021, s.93.
[224] Vuonna 2021 helmikuussa autovalmistaja Tesla ilmoitti aikeistaan hyväksyä bitcoinin maksuvälineeksi, mutta on myöhemmin ilmoittanut luopuneensa ajatuksesta siihen asti, kunnes bitcoinin ilmastovaikutusongelmat on ratkaistu, ks. https://www.cnbc.com/2021/02/08/tesla-buys-1point5-billion-in-bitcoin.html . Teslan toimitusjohtaja ja perustaja Elon Musk on aktiivinen ilmastonmuutoksen estämisen puolestapuhuja.
[225] Valtiovarainministeriö, 2021 , s.93.

laajoihin terrorismin rahoitusverkostoihin, kartoitukset liittyen vierastaistelijailmiöön, muiden valtioiden viranomaisten tukeminen terrorismin rahoittamiseen liittyvissä tutkinnoissa ja näiden rikosten torjuntaan liittyvät asiantuntijatehtävät. [226] Vuonna 2020 tehtiin yhteensä 125 terrorismin rahoittamiseen liittyvää tai terrorismin rahoittamista indikoivaa ilmoitusta suomalaisten ilmoitusvelvollisten toimesta, mikä on ennätyslukema. [227]

Viime vuosina on vaikuttanut siltä, että erilaisten rahanvälitysmuotojen käyttäminen terrorismin rahoittamisrikoksissa on lisääntynyt vuonna 2020. Rahanpesun selvittelykeskuksen käynnistämissä selvittelyissä ja muun muassa kansainvälisessä uutisoinnissa on samana vuonna havaittu, että terroristijärjestöt ja –verkostot käyttävät varojen keruun tapana ja terrorismin rahoituksessa myös virtuaalivaluuttoja. Yhdysvalloissa oikeusministeriö ilmoitti 13.8.2020 suurimmasta virtuaalivaluuttojen takavarikosta kautta aikojen. Tapauksessa epäiltiin, että virtuaalivaluuttoja on kerätty terroristijärjestöille[228] online-kampanjoiden avulla. Rahanpesun selvittelykeskuksen mukaan terroristijärjestöt ovat kiinnostuneita virtuaalivaluutoista, sillä niiden avulla varoja voidaan käyttää anonyymisti ja niitä voidaan helpommin liikutella valtioiden rajojen yli. Selvittelykeskus jatkaa aktiivisesti selvitystyötä aihepiiriin liittyen. Selvittelykeskus toimii aktiivisesti yhteistyössä muiden Euroopan maiden, KRP:n yksiköiden ja Suojelupoliisin kanssa.[229]

Europolin mukaan Isisissä on tiedostettu virtuaalivaluutan mahdollisuudet jo pitkään, mutta vasta vuonna 2017 se päätti järjestää laajamittaisen kampanjan, jossa kannattajia kehotettiin muun muassa käyttämään bitcoinia ja vielä anonyymimpää ”zcashia” lahjoitusten tekemisessä. Suurin osa näistä varoista käytettiin terroristien verkkoinfrastruktuurin rakentamiseen, mutta tiedossa on myös ainakin yksi kampanja, johon lahjoitettuja varoja on ollut tarkoitus käyttää mm. Syyriassa olevien taistelijoiden aseisiin.[230]

Tällä hetkellä virtuaalivaluuttojen käyttämisestä terrorismin rahoittamiseen ei ole olemassa kansainvälisestikään paljoa oikeuskäytäntöä. Vuonna 2015 annettiin Yhdysvalloissa 11 vuoden vankeustuomio Ali Shukri Aminille, joka oli antanut Isisille materiaalista tukea käyttäen apunaan Twitter-tiliään @Amreekiwitnees, jossa hän oli neuvonut, kuinka Isisille ja sen vierastaistelijoille voidaan lähettää bitcoineja. Amin tunnusti myös avustaneensa

[226] Rahanpesun selvittelykeskus, 2020, s. 26.
[227] Rahanpesun selvittelykeskus, 2020, s. 27.
[228] Esimerkiksi al Qaedalle, Isilille, Hamasille ja al Qassamille.
[229] Rahanpesun selvittelykeskus, 2020, s. 28-29.
[230] Europol, 2018, s. 53.

yhdysvaltalaista teiniä matkustamaan Syyriaan. Twitter-tilillä oli yli 4000 seuraajaa ja sillä julkaistiin yli 7000 Isisiin liittyvää julkaisua. [231]

[231] Tuomaala – Järvinen, 2020, s. 106.

6. Haasteisiin vastaaminen ja tulevaisuuden näkymät

6.1 Kansallisen rahanpesun selvittelykeskuksen toimintasuunnitelma 2021-2023

Aiemmin on käsitelty valtiovarainministeriön teettämää rahanpesuun ja terrorismin rahoittamiseen liittyvää riskiarviota. Kyseisen riskiarvion pohjalta laaditaan valtiovarainministeriössä myös toimintasuunnitelma, jossa esitellään niitä toimenpiteitä, joilla riskiarviossa esiin nostettuihin riskeihin voidaan reagoida ja näin ehkäistä niistä.

Toimintasuunnitelmassa on lueteltu yleisiä strategisia painopisteitä, joiden pohjalta terrorismin rahoittamista ja rahanpesua pyritään ehkäisemään. Vuoden 2021 strategiset painopisteet ovat:

1. Yleisen tietoisuuden lisääminen rahanpesusta ja terrorismin rahoittamisesta
2. Tietojenvaihdon, tilastoinnin ja kansallisen lainsäädännön kehittäminen
3. Viranomaisten ja ilmoitusvelvollisten käytössä olevien rekisterien ajantasaisuuden ja sisällön edistäminen
4. Riskiarvion esiin nostamien merkittävimpien yksittäisten riskien pienentämistoimien toteuttaminen
5. Rahanpesun ja terrorismin rahoittamisen estämisen valvonnan ja riskien hallinnan digitalisoinnin kehittäminen

Toimintasuunnitelman mukaan näiden painopisteiden tavoitteena on ”rahanpesun ja terrorismin rahoittamisen estäminen, epäilyttävien liiketoimien havaitseminen ja valvonnan tehostaminen.”[232] Virtuaalivaluutan tarjoajia koskevia lainsäädännön muutostarpeita on täsmennetty kohdassa 5, eli rahanpesun ja terrorismin rahoittamisen estämisen valvonnan ja riskien hallinnan digitalisoinnin kehittämisessä. Toimenpiteen tarkoituksena on selvittää mahdollisia tarpeita lainsäädännön muuttamiselle.[233]

Yhtenä muutostarpeena toimintasuunnitelmassa on nähty se, että virtuaalivaluutan tarjoaminen ilman rekisteröintiä tulisi säätää rikokseksi. Tämän lisäksi on katsottu, että laissa virtuaalivaluutan tarjojajista ”olisi tarvetta tarkentaa ulkomailla perustettujen yhteisöjen Suomeen rekisteröitymisen velvollisuuden kynnystä ja kynnyksen ylittymisestä seuraavia

[232]Valtiovarainministeriö, 2021b, s. 8.
[233]Valtiovarainministeriö, 2021b, s. 23.

toimenpiteitä".[234] Toimintasuunnitelmassa todetaan, että virtuaalivaluutat ovat vielä tällä hetkellä niin nopeasti muuttuva ja kehittyvä ilmiö, että on hyvä säännöllisin väliajoin arvioida sitä, kaipaavatko lain määritelmät muutoksia. Aikaisemmin on sivuttu yleisiä kriminalisointiperiaatteita ja uusia kriminalisointeja tulisikin tehdä harkiten tarkasti hyötyjä ja haittoja, sekä sitä, onko tilanne jo virtuaalivaluuttojen osalta niin stabilisoitunut, että kriminalisointi voitaisiin tehdä ilman, että lainsäädäntöä jouduttaisiin taas mahdollisesti lyhyen ajan sisällä muuttamaan uudestaan.

6.2 EU:n komission ehdotus uudeksi lainsäädäntöpaketiksi

Euroopan unionin komissio esitteli 20.7.2021 neljä lainsäädäntöehdotusta, joiden tarkoituksena on kyetä vastaamaan niihin haasteisiin, joita nopeasti muuttuva toimintaympäristö rahanpesun ja terrorismin rahoittamisen estämiselle asettaa. Lainsäädäntöehdotusten tavoitteena on yhtenäistää rahanpesuun ja terrorismin rahoittamiseen liittyvää lainsäädäntöä EU-alueella, sekä samalla toteuttaa valvontaa ja perustaa rahanpesun selvittelykeskusten koordinointi- ja tukimekanismi. Komissio on näiden tavoitteiden lisäksi pyrkinyt ehdotuksella vahvistamaan rahanpesun ja terrorismin rahoittamisen estämistä koskevan toimintapolitiikan kansainvälistä ulottuvuutta EU-alueella. [235]

Ehdotuksessa ehdotetaan säädettäväksi uusi rahanpesuasetus, jonka tarkoituksena olisi tehostaa EU:n rahanpesusääntelyn yksityiskohtaisuutta ja täsmällisyyttä. Tämän lisäksi sen avulla pyrittäisiin ennaltaehkäisemään niitä haittoja, joita on aiheutunut valtioiden toteuttaessa aikaisempien rahanpesudirektiivien täytäntöönpanoa eri tavoilla. Kyseinen asetusehdotus sisältää suurimman osan jo aikaisemmilla rahanpesudirektiiveillä säännellyistä asioista, erityisesti niiltä osin, jotka koskevat suoraan oikeushenkilöitä ja ilmoitusvelvollisia. Komissio on ehdottanut rahanpesuasetuksen soveltamisen alkamisajaksi kolme vuotta sen voimaantulosta, jotta tekniset sääntelystandardit ehditään laatia ja hyväksyä ennen sitä.[236]

Lainsäädäntöpaketissa on myös ehdotus kuudenneksi rahanpesudirektiiviksi, johon jätettäisiin ne säännökset, jotka eivät siirry rahanpesuasetukseen ja säännökset esimerkiksi toimivaltaisten viranomaisten tehtävistä rekistereistä, jotka koskevat pankki- ja maksutilien rekistereitä sekä tosiasiallisia edunsaajia.[237] Ehdotuksessa todetaan, että tarkoituksena ei kuitenkaan ole

[234]Valtiovarainministeriö, 2021b, s. 23.
[235] Finanssivalvonta, 2021, s. 1.
[236] Finanssivalvonta, 2021, s. 2.
[237] Euroopan komissio, 2021b, s. 3.

ainoastaan siirtää ”ylimääräisiä” säännöksiä uuteen direktiiviin, vaan sisältöön tehtäisiin ”*useita muutoksia valvojien ja rahanpesun selvittelykeskusten käytäntöjen sekä toimivaltaisten viranomaisten yhteistyön yhtenäistämiseks*i”.[238] Kuudennella rahanpesudirektiivillä kumottaisiin nykyinen rahanpesudirektiivi ja se olisi implementoitava kahden vuoden kuluessa sen voimaantulosta.[239] Direktiiviehdotuksessa todetaan, että komission vuonna 2019 esittämässä rahanpesutorjuntapaketissa on tuotu esiin se, että rikolliset ovat pyrkineet käyttämään hyväksi jäsenvaltioiden lainsäädännöissä olevia eroja omaksi edukseen. Terrorismin rahoittaminen ja rahanpesuun liittyvien varojen virrat voivat uhata sisämarkkinoiden vakaata toimintaa ja vahingoittaa EU:n rahoitusjärjestelmän mainetta ja vakautta. Jos toimia tehdään ainoastaan kansallisesti, voi niillä olla jopa haitallisia vaikutuksia sisämarkkinoihin luoden hajaantuneisuutta EU:n sisälle. [240]

Kolmas ehdotus koskee ns. maksajan tiedot-asetuksen uudelleen laatimista niin. että sen soveltamisalaan lisättäisiin myös virtuaalivaluuttojen tarjoajat. Virtuaalivaluuttojen tarjoajilla olisi siis velvollisuus hankkia tiedot virtuaalivaluutoilla tehtävien liiketoimien osapuolista. Muutoksella pyritään myös vastaamaan paremmin FATF:n asettamiin vaatimuksiin. [241]

6.2.1 AMLA

Ehkä merkittävin ja neljäs lainsäädäntöehdotus koskee AMLA:n, eli EU:n rahanpesun ja terrorismin rahoittamisen torjuntaviranomaisen perustamista. Komissio pyrkii tällä tehostamaan terrorismin rahoittamisen ja rahanpesun estämistä koskevien velvoitteiden noudattamisen valvontaa perustamalla toimielimen, joka täydentäisi kansallisten valvojien tehtävien täyttämistä EU:n tasolla.

Komission ehdotuksen mukaan torjuntaviranomaisen perustaminen on välttämätöntä, jotta rahanpesun ja terrorismin rahoittamisen aiheuttamiin haasteisiin voitaisiin puuttua. Komissio on perustellut tätä sillä, että näiden rikosten estämistoimet perustuvat tällä hetkellä käytännössä kokonaan jäsenvaltioiden omiin sääntelytoimiin.[242] Eri jäsenvaltioiden tosiasialliset resurssit ja käytänteet kuitenkin vaihtelevat niin voimakkaasti, että sääntelyn laatu ja vaikuttavuus eivät

[238] Euroopan komissio, 2021b, s. 3. Ehdotuksessa listataan lukuisia tavoitteita, joilla pyritään hyvin vahvasti harmonisoimaan rahanpesun ja terrorismin rahoittamisen sääntelyn kenttää EU:n alueella.
[239] Finanssivalvonta, 2021, s. 2.
[240] Euroopan komissio, 2021b, s. 5.
[241] Finanssivalvonta, 2021, s. 3.
[242] Euroopan komissio, 2021, s. 3.

ole EU:n alueella tasaisen vahvoja.[243] Komission jäsenvaltioille tekemässä kyselytutkimuksessa oli käynyt ilmi, että jäsenvaltioiden selkeä kanta oli ollut, että rahanpesun ja terrorismin rahoittamisen riskien arvioimiseksi ja niiden tunnistamiseksi tarvitaan yhteinen ja johdonmukainen menetelmä.[244] Jotta nämä EU:n alueella ilmi tulleet puutteet rahanpesun ja terrorismin rahoittamisen estämisessä voidaan korjata, on keskitetyn valvontajärjestelmän perustaminen välttämätöntä.

AMLA tulee osallistumaan unionissa suoraan terrorismin rahoittamisen ja rahanpesun estämiseen muun muassa valvomalla suoraan riskialtteimpia kansainvälisiä finanssialan ilmoitusvelvollisia. AMLA tulee myös tekemään näitä koskevia päätöksiä itsenäisesti.[245] Näillä toimilla pyritään paikkaamaan niitä puutteita, joita on EU:n alueella havaittu, kun yksityiset yritykset tai muut toimijat eivät ole puuttuneet ongelmiin rahanpesudirektiivien vaatimalla tavalla.[246]

Komission ehdotuksessa kerrotaan, että kaikissa hiljattain EU:n alueella tapahtuneissa merkittävissä rahanpesurikoksissa on ollut ”rajat ylittävä ulottuvuus”. Näiden rikosten havaitseminen on kuitenkin tähän asti jäänyt kansallisten rahanpesun selvittelykeskusten ja niiden välisen jokseenkin sääntelemättömän yhteistyön huolehdittavaksi. Ehdotuksessa todetaan, että vaikka tämä toisaalta kertoo kansallisten rahanpesun selvittelykeskuksen riippumattomuudesta ja itsenäisyydestä, ovat tarvittavat toimet kuitenkin usein jääneet puutteellisiksi tai tekemättä. Syynä tälle ovat mm. vahvojen yhtenäisten rakenteiden ja resurssien puute. Näiden puutteiden seurauksena on ollut hajanaiset toimintatavat, jotka ovat alttiita rahanpesuun ja terrorismin rahoittamiseen liittyville väärinkäytöksille.[247]

Komissio on esittänyt AMLAlle valtuuksia koordinoida jäsenvaltioiden valvojien toimintaa, antaa lausuntoja esiin tulleista rahanpesuun liittyvistä riskitekijöistä ja oikeutta valvoa korkeariskisimpiä valtioiden rajat ylittäviä rahoitussektorin ilmoitusvelvollisia. EBA:n

[243] EBA, 2020, s. 21-22. Huomionarvoista EBA:n raportissa on se, että viranomaiset eivät maininneet lainsäädännöllisiä esteitä yhteistyölle, vaan se oli tilanne, johon oltiin ajauduttu. Viestit saattoivat myös kulkea epävirallisia reittejä pitkin henkilöltä toiselle, jos mitään virallisia rakenteita tai velvoitteita näiden viestien vaihtamiselle ei ollut.
[244] Euroopan komissio, 2021, s. 3.
[245] Euroopan komissio, 2021, s. 3.
[246] Euroopan tilintarkastustuomioistuin on antanut vuonna 2021 erityiskertomuksessaan rajuakin kritiikkiä EU:n toimille rahanpesun torjumiseksi pankkisektorilla. Tilintarkastustuomioistuimen mukaan EU:n toimet rahanpesun torjumiseksi pankkisektorilla ovat olleet hajanaisia, täytäntöönpano riittämätöntä ja viranomaisten välinen tietojenvaihto epätasaista ja tehotonta, ks. Euroopan tilintarkastustuomioistuin, 2021.
[247] Euroopan komissio, 2021, s. 4.

nykyiset rahanpesuun ja terrorismin rahoittamiseen liittyvät tehtävät tulisivat myös siirtymään AMLAlle. Ehdotuksessa esitetään aikatauluksi, että AMLA perustettaisiin vuonna 2023, se aloittaisi toimintansa 2024 ja sen aktiivinen suora valvonta alkaisi 2026.[248]

6.3 Lainsäädännön potentiaaliset muutostarpeet ja niihin liittyvä kritiikki

Kuten on jo käynyt useaan otteeseen ilmi, perustuu rahanpesun ja terrorismin rahoittamisrikosten estäminen ja sääntely vahvasti preventiiviselle lähtökohdalle. Virtuaalivaluutat epäilemättä ovat aiheuttaneet rikosten ennaltaehkäisytoimille suuria haasteita, joihin on pyritty myös lainsäädännön päivittämisellä vastaamaan. Samaan aikaan kuitenkin myös kriittiset äänenpainot ovat lisääntyneet sen suhteen, kuinka laajalle viranomaisten ja erilaisten valvonta- ja kontrollijärjestelmien sallitaan ulottuvan. *Hyttinen* on arvostellut rahanpesun preventiivistä lainsäädäntöä siitä, että se ”*vaikuttaa johtavan lähes luonnonlain välttämättömyydellä siihen, että rahanpesu saa uusia tekomuotoja, joita jo voimassa oleva preventiivinen sääntely ei tavoita*.”[249] *Hyttisen* mukaan tästä seuraa se, että voimassaolevan sääntelyn legitimiteetin turvaamiseksi joudutaan laatimaan aina uutta preventiivistä sääntelyä, jotka myös osaltaan lisäävät uudenlaisia tekoja rahanpesun määritelmään piiriin, mikä jälleen edellyttää uutta preventiivistä sääntelyä.[250]

Kritiikki on varmasti aiheellista, jos huomioidaan FATF:n ja EU:n[251] kuin itsestään laajeneva valta sanella valtioille, mitä muutoksia ja lisäyksiä kansallisiin rikoslakeihin tulisi tehdä. Yleisten kriminalisointiperiaatteiden valossa tulisikin tarkastella kriittisesti sitä, missä vaiheessa loputon kilpajuoksu rikollisten kanssa johtaa siihen, että uudet kriminalisoinnit vain kasvattavat yhteiskunnallisia kustannuksia vailla suhteellisuusvaatimuksen ja hyöty-haitta-punninnan periaatteen vaatimusten riittävää reflektointia. Kansallisessa riskiarviossa ja FATF:n suosituksissa on tuotu esiin vaatimukset lisätä viranomaistoiminnan resursseja, jotta ne voivat tehokkaasti valvoa ja hoitaa niille kuuluvia velvoitteita. Samaan aikaan kuitenkin jo nyt resurssipulan kanssa painiskeleville toimijoille asetetaan jatkuvasti uusia velvoitteita, joiden

[248] Finanssivalvonta, 2021, s. 2.
[249] Hyttinen, 2021, s. 104.
[250] Hyttinen, 2021, s. 104.
[251] Komission ehdotuksessa kuudenneksi rahanpesudirektiiviksi sen perusteluissa todetaan, että ”tehokas täytäntöönpano on ratkaisevan tärkeää rahanpesun ja terrorismin rahoittamisen estämisessä. Komissio käyttää jatkossakin kaikkia keinoja ja mekanismeja voidakseen tarkistaa paitsi sen, että unionissa asetetut vaatimukset on saatettu asianmukaisesti kansallisen lainsäädännön osaksi, myös sen, että jäsenvaltiot panevat ne tehokkaasti käytäntöön päivittäisissä käytännöissä.” Perustelut kuulostavat suhteellisen jyrkiltä, kun otetaan huomioon, että kyse on rikoslainsäädännön harmonisoinnista.

täyttämättä jättämiseen esimerkiksi FATF reagoi voimakkaasti, kuten kävi esimerkiksi Suomessa itsepesun kriminalisoinnin osalta. EU:n ehdotus keskitetystä valvontaviranomaisesta pyrkii osaltaan vastaamaan tähän resurssipulaan.

Terrorismin rahoittamisen suhteen Suomessa on perustuslakivaliokunnan lausunnoissa tullut monta kertaa esiin, että terrorismissa on kyse niin vakavasta yhteiskunnan perustoimintoja, ihmisten henkeä, turvallisuutta ja terveyttä sekä koko oikeusjärjestystä uhkaavasta toiminnasta, että sen keskeyttämiselle ja estämiselle on perusoikeusjärjestelmänkin näkökulmasta erittäin painavat ja hyväksyttävät perusteet.[252] Valiokunnan näkemys perustuu siihen, että terrori-iskuja edistävien toimien ja tekojen rangaistavaksi säätäminen ehkäisee terroristisessa tarkoituksessa tehtyjen rikosten tekemistä. Syvällisempää pohdintaa preventiivisen lainsäädännön mahdollisista haitoista tai rajoista ei kuitenkaan vaikuttaisi olevan tehty.

6.3.1 Mixer-palveluiden ja rekisteröimättömien virtuaalivaluuttalompakkojen hallinnan kriminalisointimahdollisuudet

Tutkielman alkupuolella esitellyt mixer-palvelut ja niiden tarjoajat ovat osoittautuneet viranomaisten selvityksissä riskialttiiksi teknologioiksi rahanpesun ja terrorismin rahoittamisen estämistoimien näkökulmasta. On selvää, että tällä hetkellä suurin syy mixer-palveluiden käytölle on pyrkimys häivyttää rikoksella ansaitun rahan alkuperää tai mahdollisesti pyrkiä peittelemään sitä, keneltä terrorismin rahoittamiseen tarkoitetut rahat ovat alun perin peräisin. Vastaamo-tapauksessa esimerkiksi haluttiin estää viranomaisia selvittämästä sitä, kenelle kiristämällä ansaitut virtuaalivaluutat lopulta päätyivät.

Edellä on käyty läpi yleisiä kriminalisointiperiaatteita ja lähtökohtia sille, missä vaiheessa jokin ilmiö on niin haitallinen, että siitä voidaan säätää rikoslaissa. Valtiovarainministeriö on päättänyt kansallisen riskiarvion toimintasuunnitelmassaan lähteä selvittämään, voitaisiinko mixer-palvelut kieltää kansallisella lainsäädännöllä.[253] Yleisten kriminalisointiperiaatteiden näkökulmasta jonkin teknologian yksiselitteinen kieltäminen rikoslainsäädännön keinoin tuntuu hieman erikoiselle. Vertailukohtaa voidaan hakea muualta internetin maailmasta ja niin sanotusta VPN (virtual private network)-palveluista. VPN on tietoliikenteen salausohjelmisto, jonka tarkoituksena on netin käyttäjän IP-osoitteen ja muiden yksilöivien tietojen

[252] Ks. PeVL 26/2014 vp. s, 2, PeVL 37/2016 vp, s. 2 ja PeVL 20/2018 vp, s. 2.
[253] Valtiovarainministeriö, 2021b, s. 24.

salaaminen.[254] VPN:n hankkiminen ja sen käyttö on usein liitetty rikolliseen toimintaan, mutta rikoslaissa sitä ei ole lähdetty kriminalisoimaan, vaikka viranomaiset ovatkin tiettyjä VPN-palveluita sulkeneet.[255]

Edellä mainitun lisäksi rikoslaissa voimassaolevat lainkohdat rahanpesusta ja terrorismin rahoittamisesta mahdollistavat mixer-palveluiden avulla suoritettujen rikosten tuomitsemisen. Rikoslain 32 luvun 6 §:n mukaan rahanpesusta voidaan tuomita henkilö, joka esimerkiksi *pyrkii peittämään tai häivyttämään omaisuuden laittoman alkuperän tai niiden tilalle tulleen omaisuuden rikollisen alkuperän*.[256] Mixer-palveluiden tarjoaminen esimerkiksi markkinoimalla sitä rahanpesutarkoituksissa käytettäväksi, voitaisiin taas katsoa rahanpesun *yllytyksenä* rangaistavaksi.

Ultima ratio-periaatteen ja suhteellisuusvaatimuksen näkökulmasta mixer-palveluiden kriminalisointi vaikuttaisi jokseenkin kyseenalaiselta huomioon ottaen, että niiden käyttö rikollisessa toiminnassa voidaan tuomita jo nykyisen rikoslain sanamuodon puitteissa, mikäli palvelun tarjoajan rikollinen tarkoitus voitaisiin osoittaa. Perustuslakivaliokunta on linjannut suhteellisuusvaatimuksesta, että perusoikeuksien rajoitusten tulee olla *välttämättömiä* hyväksyttävän tarkoituksen saavuttamiseksi.[257] Ymmärrettävästi selkeästi rikolliseen toimintaan liittyvän teknologian kieltäminen varmasti tuntuu helpolta ratkaisulta rikollisuuden estämiseksi, mutta rikosoikeudellisen sääntelyn laajenemiseen tulisi suhtautua pidättyvästi etenkin tilanteessa, jossa uusi teknologinen ilmiö on vasta löytämässä paikkaansa yhteiskunnassa. *Hyttisen* edellisessä kappaleessa esittämä kritiikki ”preventiivisen lainsäädännön noidankehästä” tulisi ottaa tässäkin vakavasti huomioon. Kansainvälisten vahvojen toimijoiden, kuten FATF:n linjaukset eivät myöskään saisi irtaannuttaa kansallista lainsäädäntöä ja sen kehittämistä oikeusjärjestelmän ydinperiaatteista, varsinkaan jos perusteluina käytetään lyhyesti ”yleistä etua ja turvallisuutta”.

[254] Ks. Norton, 24.2.2022.
[255] Ilta-Sanomat uutisoi huhtikuussa 2022, että korkein oikeus on todennut KRP:n suorittaman takavarikon kielletyksi keinoksi vpn-suojattua internet-yhteyttä käyttäneen henkilön paljastamiseksi. Jutussa tulkitaan KRP:n tekemä takavarikko tavaksi kokeilla poliisin toimivallan rajoja, johon KKO reagoi, ks. Ilta-Sanomat, 6.4.2022.
[256] Ks. kappale 3.2.
[257] PeVM 25/1994, s. 5.

6.3.2 Virtuaalivaluuttojen tarjoajat tiukentuvien velvoitteiden piiriin – problematiikkana oikeushenkilön rangaistusvastuu

Päivitetty virtuaalivaluuttalaki ja EU:n maksajan tiedot-asetus asettavat virtuaalivaluuttojen tarjoajat yhä tiukentuvien velvoitteiden piiriin. Virtuaalivaluuttojen tarjoajilla tulee nykyisin tunnistaa asiakkaansa ja tulevaisuudessa myös monitoroida tarkemmin sitä, mistä varat heille tulevat. Mikäli toimijat eivät täytä velvollisuuksiaan, on heille mahdollista asettaa jo edellä kuvatusti muun muassa hallinnollisia seuraamusmaksuja.

Valtiovarainministeriö on kansallisen riskiarvion toimenpideohjelmassaan ehdottanut selvitystä siitä, voitaisiinko virtuaalivaluutan tarjoaminen ilman rekisteröintiä säätää rikokseksi. Tämän lisäksi valtiovarainministeriö toivoisi tarkennusta ”ulkomailla perustettujen yhteisöjen Suomeen rekisteröitymisen velvollisuuden kynnystä ja kynnyksen ylittymisestä seuraavia toimenpiteitä.”[258]

Haasteellista vaatimusten lisääntymisessä on myös oikeushenkilön rangaistusvastuuseen liittyvä problematiikka. *Tapani* on tiivistänyt rikoslain 9 luvun 1 ja 2 §:n vaatimukset niin, että oikeushenkilön rangaistusvastuu edellyttää sitä, että 1) oikeushenkilön toiminnassa on tehty rikos, 2) luonnollisen henkilön rikokseen syyllistyminen voidaan kytkeä tiettyyn oikeushenkilön rangaistusvastuun perusteeseen, 3) rikoksentekijän ja oikeushenkilön välillä vallitsee tietynlainen suhde ja 4) rikos katsotaan tehdyksi oikeushenkilön puolesta tai hyväksi.[259] Rikoslain 9 luvusta ja sen esitöistä voidaan *Tapanin* mukaan päätellä, että oikeushenkilön rangaistusvastuun perustana voi käytännössä olla ns. *samastaminen, organisaatiohuolimattomuus ja anonyymi syyllisyys.*[260] Rekisteröimättömien virtuaalivaluuttalompakoiden tarjoamisen mahdollista kriminalisointia pohdittaessa oikeushenkilön rangaistusvastuun kysymykset eivät luultavasti tuota suuriakaan ongelmia, sillä kyseessä on suhteellisen selkeästi toimi, jonka teonkuvaus täyttyisi *aktiivisella toiminnalla*. Kyseessä ei siis olisi vain huolellisuusvelvoitteen rikkominen, mikäli toimija aktiivisesti tarjoaisi virtuaalivaluuttalompakkoja käytettäväksi ilman asianmukaista asiakkaan tunnistamista.

[258] Valtiovarainministeriö, 2021b, s. 23.
[259] Oikeusministeriön julkaisuja, 2020:22, s. 15.
[260] Oikeusministeriön julkaisuja, 2020:22, s. 16.

Ongelmallisempaa yksittäisten toimijoiden ja yleisten kriminalisointiperiaatteiden näkökulmasta olisi edellä mainittuun *organisaatiohuolimattomuuteen* perustuva kriminalisointi, jossa virtuaalivaluuttojen tarjoajat joutuisivat esimerkiksi vastaamaan syytteisiin terrorismin rahoittamisesta tilanteessa, jossa virtuaalivaluuttoja on siirretty heidän palveluistaan terroristien käyttöön. Kuten on tuotu esiin, terroristiseen toimintaan lähetettävät rahasiirrot eivät välttämättä ole kovinkaan suuria, eivätkä ne välttämättä kiinnitä samalla tavalla huomioita, kuin rahanpesutarkoituksessa siirrettävät, suuremmat summat. Virtuaalivaluuttojen pohjalla oleva lohkoketjuteknologia aiheuttaa sen, että jopa asiaan erityisesti vihkiytyneellä KRP:llä on haasteita jäljittää virtuaalivaluuttojen liikkeitä lohkoketjuissa. Vaikuttaisikin siis siltä, että tämän tyyppisissä rikoksissa virtuaalivaluuttojen tarjoajille jää lähinnä tiedonantajan rooli, mikäli epäillyn rikoksen esitutkinnassa jäljet johtaisivat virtuaalivaluutan tarjoajien luo.

6.3.3 Viranomaisten tiedonsaantioikeuksien laajentamismahdollisuudet ja tiedonvaihdon kehittäminen

Viranomaisten suosituksia tutkiessa on käynyt selväksi, että viranomaisten välinen ja myös viranomaisten ja yksityisten välinen tiedonvaihto[261] ja sen kehittäminen nähtiin merkittävänä kehittämiskohteena rahanpesun ja terrorismin rahoittamisen estämisessä.[262] Kansallisesti tietojenvaihdon on nähty vielä olevan suhteellisen hyvällä tasolla, mutta ongelmat lisääntyvät, mitä laajemmalle alueelle tarkastelua ulotetaan. Suomalaisten ilmoitusvelvollisten on myös kerrottu kaipaavan selkeämpää ohjeistusta viranomaisilta liittyen rahanpesun ja terrorismin rahoittamisen estämistoimintaan. [263]

Euroopan tietosuojavaltuutettu on lausunut,[264] että rahanpesun ja terrorismin rahoittamisen ehkäisemisessä tulee ottaa huomioon myös henkilötietojen suoja ja löytää tasapaino rikosten ehkäisyn ja yksityisyydensuojan välillä.[265] Tämän lisäksi tietosuojavaltuutettu on ottanut kantaa myös PPP-tietojenvaihtoon, jossa tulisi painottaa myös sitä, että operatiivisen tiedon jakaminen ilmoitusvelvollisen ja viranomaisen välillä on merkittävä riski henkilötietojen

[261] Viranomaisten ja yksityisten välistä tiedonvaihtoa kutsutaan vakiintuneesti ns. PPP-tiedonvaihdoksi (Public-Private Partnership).
[262] Tiedonvaihdon parantaminen ja valvonnan tehostaminen rahanpesun ja terrorismin rahoituksen torjumiseksi on kirjattu myös Sanna Marinin hallituksen ohjelmaan, ks. https://valtioneuvosto.fi/marinin-hallitus/hallitusohjelma/kestavan-talouden-suomi .
[263] Valtiovarainministeriö, 2022, s. 6.
[264] Valtiovarainministeriö, 2022, s. 18. Tietosuojavaltuutettu antoi lausunnon komission 7.5.2020 antamaan toimintasuunnitelmaan.
[265] Valtiovarainministeriö, 2022, s. 75.

suojan näkökulmasta.[266] Myös sellaiseen tietojenvaihtoon, jossa epäillystä luovutettaisiin ilmoitusvelvollisille jonkinlaisia tietoja yksittäisiin liiketoimiin liittyen tai että ilmoitusvelvollisilla olisi jonkinlainen mahdollisuus valvoa epäiltyjä viranomaisilta saatujen tietojen perusteella, on tietosuojavaltuutetun mukaan suhtauduttava erityisen torjuvasti.[267] Tällä linjauksella halutaan pitää kiinni ns. *käyttötarkoitussidonnaisuuden periaatteesta*, jonka mukaan henkilötieto voidaan kerätä laillisin perustein vain johonkin tiettyyn käyttötarkoitukseen, eikä sitä voida myöhemmin enää jatkokäsitellä.[268]

Mahdollisessa tietojenvaihdon ja viranomaisten tietojensaannin laajentamisessa haasteena on oikeudellisten reunaehtojen asettamien rajoitteiden lisäksi viranomaisten todelliset resurssit pitää tiiviisti yhteyttä toisiin viranomaisiin ja yksityisiin toimijoihin.

6.4 Finanssimaailman muutospaineet – tuleeko tekoäly helpottamaan viranomaisten työtä?

Vuoden 2021 joulukuun 1. päivänä EU:n neuvosto julkaisi lehdistötiedotteen, jossa kerrottiin, että neuvosto on sopinut valtuutuksesta neuvotella Euroopan parlamentin kanssa päivitysehdotuksesta, joka koskee varainsiirtojen mukana toimitettavia tietoja. Tiedotteen mukaan päivityksen tarkoituksena olisi laajentaa sääntöjen soveltamisalaa kryptovaroihin.[269] Slovenian valtiovarainministeri Andrej Šircelj kommentoi tiedotteessa asiaa seuraavasti:

> *”Tänään saavutettu yhteisymmärrys on tärkeä askel kohti rahoitusjärjestelmien sellaisten puutteiden korjaamista, joita rikolliset käyttävät rikoshyödyn pesemiseen tai terrorismin rahoittamiseen. Kasvavana riskinä on, että kryptovaroja käytetään rahanpesuun ja rikollisiin tarkoituksiin, ja olen iloinen, että neuvosto eteni nopeasti tämän kiireellisen ehdotuksen käsittelyssä.”*

Ehdotuksessa on tarkoituksena velvoittaa virtuaalivaluuttojen tarjoajat keräämään ja asettamaan saataville täydelliset tiedot välittämiensä virtuaalivarasiirtojen vastaanottajasta ja lähettäjästä. Tällä pyritään varmistamaan se, että virtuaalivaluuttojen siirrot voidaan jäljittää ja että epäilyttävät liiketoimet voidaan helpommin tunnistaa ja estää. Nämä muutokset komission

[266] Valtiovarainministeriö, 2022, s. 75.
[267] Valtiovarainministeriö, 2022, s. 75-76.
[268] Valtiovarainministeriö, 2022, s. 75. Vaikka henkilötietojen suoja, tietosuoja-asetus ja käyttötarkoitussidonnaisuuden periaate rajoittaa etenkin PPP-yhteistyötä, voivat viranomaiset ja ilmoitusvelvolliset kuitenkin jakaa hyödylliseksi kokemaansa ilmiötason tietoa, josta on hyötyä rahanpesun ja terrorismin rahoittamisen ehkäisyssä.
[269] Eurooppa-neuvosto. Lehdistötiedotteet. Rahanpesun torjunta: neuvosto hyväksyi neuvotteluvaltuutuksen kryptovarojen siirtojen avoimuudesta, 1.12.2021.

ehdotukseen selkeyttävät aiempaa ehdotusta. Erityisesti on tarkoituksena ottaa käyttöön virtuaalivaluuttapalvelujen tarjoajien ja ns. isännöimättömien virtuaalivaluuttalompakoiden välisiä kryptovarojen siirtoja koskevia vaatimuksia. [270]

Tulevaisuudessa rahanpesuun liittyvä valvonta ja tarve uudenlaisille toimenpiteille tulee todennäköisesti lisääntymään entisestään. Viranomaisten pyrkimykset puuttua yhteiskunnan ja talouden toimintaan sekä maksuliikenteeseen tulee myös luultavasti kasvamaan. Tavanomaisessa rahoitusjärjestelmässä rahojen siirtely jättää enenevissä määrin yhä pidempiä jälkiä rahan digitalisoituessa, kun kaikki tilisiirrot tehdään sähköisesti ja ne rekisteröityvät pankkien järjestelmiin. Dataa on siis saatavilla ennennäkemättömiä määriä ja laskentatehon ja tietoliikennekapasiteetin kasvaessa jatkuvasti, ovat monimutkaiset laskelmat muuttuneet toteuttamiskelpoisiksi. Tekoäly tulee todennäköisesti helpottamaan tätä tulevaisuudessa entisestään.[271] Kun valvonta automatisoituu, tulevaisuudessa voi olla mahdollista, että eri tietojärjestelmät valvoisivat toisiaan. Sama järjestelmä siis voisi käytännössä toteuttaa maksuliikenteen ja myös valvoa sen toimintaa. [272] Myös valtiovarainministeriö on sen kansallisen riskiarvion toimenpideohjelmassa esittänyt toimenpiteeksi tekoäly- ja robotiikkahankkeita, joiden tarkoituksena on selvittää sitä, miten tekoälyä voitaisiin hyödyntää terrorismin rahoittamista ja epäilyttäviä liiketoimia koskevien ilmoitusten käsittelyssä. Hanke on tällä hetkellä käynnissä rahanpesun selvittelykeskuksessa.[273]

Aiemmin on jo käyty läpi niitä heikkouksia, jotka liittyvät virtuaalivaluuttojen mahdolliseen laajempaan käyttöönottoon. Jotta jokin valuutta voitaisiin luokitella luotettavaksi, tulisi sen olla vakaa ja luotettava. Näitä ominaisuuksia virtuaalivaluutoilla ei ainakaan toistaiseksi ole, vaikkakin on todennäköistä, että sääntelyn lisääntyessä ja virtuaalivaluuttojen yleistyessä nämäkin ominaisuudet jossain vaiheessa saavutetaan. Mahdollista on sekin, että jossain vaiheessa virtuaalivaluuttojen pohjana oleva lohkoketjuteknologia mahdollistaakin rahasiirtojen täydellisen jäljitettävyyden ja seurattavuuden.[274]

Finanssimaailmaan liittyvä sääntely on jatkuvasti valtavan muutospaineen alla. Sääntelyn muutoksessa digitalisaatio on tavallisesti huomioitu siten, että erilaisille toimijoille asetetaan

[270] Eurooppa-neuvosto. Lehdistötiedotteet. Rahanpesun torjunta: neuvosto hyväksyi neuvotteluvaltuutuksen kryptovarojen siirtojen avoimuudesta, 1.12.2021.
[271] Andérsen, 2020, s. 171.
[272] Andérsen, 2020, s. 172.
[273] Valtiovarainiministeriö, 2021b, s. 32.
[274] Andérsen, 2020, s. 172.

mm. ilmoitus- ja tiedonluovuttamisvelvoitteita. *Andérsen*[275] on kiinnittänyt huomiota erityisesti siihen, miten sääntely suhtautuu vastuuseen ja miten sääntely käytännössä pohjautuu aina analogiselle ajatusmaailmalle. Tämä oletus sisältää ajatuksen, että jokaisen transaktion tekisi ja sen takana olisi oikea ihminen. Todellisuudessa tämä ei enää pidä paikkaansa, vaan siirtojen takana on jo nykyisin jopa useimmiten tietokone. Tällä hetkellä sääntely keskittyy lähinnä määrittelemään toimintatapoja finanssilaitoksille ja niissä työskenteleville luonnollisille henkilöille. Silloinkin, kun myyjä ja ostaja itse toteuttavat transaktion, voivat he suorittaa sen alustalla, joka voi olla kumppanina kahdelle finanssilaitokselle: ostajalle ja myyjälle. Osaa näistä säännellään ja osaa ei.[276]

Oikeutus pankkien olemassaololle lähtee siitä, että ne lisäävät taloudellisiin transaktioihin liittyvää varmuutta ja luotettavuutta. Digitalisaatio on lisännyt varmuutta entisestään, sillä transaktioihin liittyvää dataa voidaan seurata ja niihin liittyvät riskit pienenevät. Sääntelyn pohjautuessa analogiselle ajattelutavalle sääntely ei välttämättä toteuta tavoitetta tarjota puitteet mahdollisimman tehokkaille ja vakaille rahoitusmarkkinoille, vaan tilalle tarvittaisiin prosessisääntelyä verkostoille.[277]

Useiden valtioiden keskuspankit pohtivat ja tutkivat tällä hetkellä, voisivatko he laskea liikkeelle omia lohkoketjuteknologiaan pohjaavia virtuaalivaluuttojaan. Keskuspankit ovat listanneet useita selvitettäviä asioita ja mahdollisia riskejä, joita virtuaalivaluuttoihin liittyy. Riskeiksi on lueteltu mm. oikeusvarmuus ja laillisuus, luotettavat hallintomallit, verotukselliset asiat, kuluttajansuoja, taloudellinen luotettavuus ja tietosuoja sekä muut operatiiviset riskit.[278]

Edellä luetellut ongelmat ovat jo ennestään tuttuja perinteisen rahoitusjärjestelmän piirissä ja niiden varalle on olemassa oma lainsäädäntönsä. Tätä sääntelyä tulisi voida soveltaa myös virtuaalivaluuttoihin ja mikäli nykyinen sääntely ei ole riittävää, tulee lainsäädäntöä päivittää. *Andérsenin* mukaan rahanpesun ja terrorismin rahoittamisen estämiseksi virtuaalivaluuttojen käyttöön olisi siirryttävä laajasti niin pian, kuin mahdollista. *Andersén* perustelee tätä sillä, että lohkoketjujen vaihdantaketjun rikkoutumattomuuden ja hajautetun rekisteröinnin ansiosta

[275] Teoksessa Rahanpesun estäminen, 2020. KTT Atso Andérsenilla on pitkä työkokemus finanssimaailman tehtävistä. Nykyään hän toimii neuvonantajana yhteiskunnallisesti tärkeissä hankkeissa sekä start up-yrityksissä.
[276] Andérsen, 2020, s. 173.
[277] Andérsen, 2020, s. 174.
[278] Ks. lisää Committee on Payments and Market Infrastructures and the Bank for International Settlements: ”G7 Working Group on Stablecoins; Investigating the impact of global stablecoins” (October 2019), https://www.bis.org/cpmi/publ/d187.pdf .

vaihdantaa ei voida väärentää ja kaikkien transaktioiden tekijöiden toimet tallentuvat pysyvästi lohkoketjuun. Oleellista virtuaalivaluuttojen luotettavuuden parantamisessa on *Andérsenin* mielestä käyttäjien tunnistamisen varmistaminen. Tätä varmennusta tarvitaan tekemään aina jokin ulkopuolinen taho, esimerkiksi luvan saaneet finanssilaitokset. [279]

[279] Andérsen, 2020, s. 175.

7. Loppupäätelmät

Tämän tutkielman keskeisin tutkimuskysymys oli ”*Mitä haasteita virtuaalivaluutoista aiheutuu rahanpesu- ja terrorismin rahoittamissääntelylle?*”. Edellä kysymykseen on pyritty vastaamaan suhteellisen yleisesti ja olennaisimpia ongelmia esitellen. Suuri osa sääntelyn ongelmista johtuu virtuaalivaluuttojen taustalla olevasta teknologiasta ja niiden erityisistä ominaisuuksista, joita ei esimerkiksi fiat-valuutoilla ei ole. Merkittävimpiä haasteita ovat virtuaalivaluuttojen käyttöön liittyvän *teknologian nopea kehittyminen*, minkä perässä lainsäädäntö ei ole ainakaan tähän asti täysin kyennyt täysin pysymään. Lainsäädäntöä on luotu aluksi osittain myös jokseenkin summittaisesti ja johonkin yksittäiseen ongelmaan (esim. verotukselliset kysymykset) vastaten.

Virtuaalivaluuttojen *hajautunut luonne* aiheuttaa sen, että niiden tehokas sääntely vaatii kansainvälisiä toimia. Ongelmiin ei ole mahdollista vastata vain yhdestä valtiosta käsin ja kuten käytäntö on osoittanut, ei niiden hankkimisen ja käyttämisen täyskielto ja kriminalisointikaan ole ollut aukoton ratkaisu. Virtuaalivaluuttojen *anonymiteetti* taas on ollut luultavasti olennaisin syy sille, miksi rikolliset ovat ensinnäkään omaksuneet virtuaalivaluutat käyttöönsä. Anonymiteetin purkaminen on myös sääntelyn kannalta ollut se olennainen asia, johon lainsäätäjäkin on ensisijaisesti lähtenyt keskittymään. Suomessa asiaan puututtiin aluksi velvoittamalla virtuaalivaluuttojen tarjoajat tunnistamaan asiakkaansa, sekä valvomaan mahdollisesti virtuaalivaluuttoihin liittyvää epäilyttävää toimintaa ja ilmoittamaan niistä asianomaisille viranomaisille. Tullin takavarikoitua Silkkitie-palvelimen, on virtuaalivaluuttojen käyttäjiä ja niiden avulla huumausaineita tilanneita henkilöitä myös Suomessa pystytty jäljittämään poliisin käytössä olevan teknologian avulla. Teknologia ei siis kehity vain rikollisten hyväksi, vaan kehittyneiden teknologioiden ja esimerkiksi *tekoälyn* avulla on mahdollista yhä tehokkaammin seurata ja valvoa internetin kautta tapahtuvaa rikollisuutta. Tekoälyn avulla voidaan vastata myös viranomaisten resurssipulaan, jos tulevaisuudessa esimerkiksi virtuaalivaluuttojen siirtoja lohkoketjuissa ei tarvitse manuaalisesti jäljittää ihmisen toimesta.

Internetin kehittymisen myötä myös rikolliset ovat alkaneet käyttämään hyväksi sen tarjoamia mahdollisuuksia toimia kansainvälisesti ja tehokkaasti ilman, että toimet rajoittuisivat esimerkiksi vain yhden valtion sisälle. Uuden teknologian rantautuessa rikolliseen käyttöön voi viranomaisilla olla vahva houkutus kieltää ja kriminalisoida kyseinen ilmiö kokonaisuudessaan.

Rikosoikeudelliset kriminalisointiperiaatteet osaltaan hillitsevät liian voimakkaita reaktioita kehityksen alussa ja vaikka lainsäädännön hidasta muutosta voi myös arvostella, mahdollistaa se kuitenkin sellaisen aikaikkunan, jonka sisällä ehditään puntaroida sitä, mitkä toimet ovat riittäviä rikollisuuden estämiseksi ja ennaltaehkäisemiseksi. Usein myös olemassa oleva lainsäädäntö joustaa sen verran, että vakavimmat rikkomukset saadaan tuomittua, vaikka täysin päivitettyjä säännöksiä ei olisikaan. Rikoslaissa olevien rikosten teonkuvaukset onkin lähtökohtaisesti hyvä kirjoittaa *teknologianeutraalisti* niin, että jatkuvassa muutoksessa oleva teknologia ja siihen liittyvät uudet ilmiöt eivät rajoita tuomioistuinten toimivaltaa antaa rangaistusta, mikäli rikoksen tunnusmerkistö olennaisilta osiltaan täyttyy.

Huomionarvoista oli se, että tutkimuksissa rikollisten on todettu myös suoraan tiedostavan, että valtiot eivät kykene riittävän nopeassa tahdissa luomaan uutta lainsäädäntöä ja että *tietojenvaihto* etenkin yksityisten ja julkisten toimijoiden välillä on usein hyvin puutteellista. On hyvä pohtia sitä, onko viranomaisten oletettu hitaus asia, jonka olemme vain hyväksyneet tietynlaisena muuttumattomana ilmiönä, vai voisiko siihen vaikuttaa. Yleensä ongelma ei kuitenkaan ole ymmärryksen puutteessa, vaan kyse on *rajallisten resurssien ongelmasta*. Vaikka tiedostamme rikollisuuden ennaltaehkäisyn haasteet, on asia usein tavallisille ihmisille niin etäinen ja jopa abstrakti, että poliitikolle ei ole kovin houkuttelevaa kampanjoida rahanpesun selvittelykeskuksen resurssipulasta, kun äänestäjät eivät yleensä havaitse niiden suoraan merkitystä omassa arjessaan. Lisääntyvä sääntely ja uudet kriminalisoinnit toisaalta myös voivat kuormittaa viranomaisia entisestään, vaikka tarkoitus jonkin asian kriminalisoinnilla olisi hyvä.

Rahanpesua ja terrorismin rahoittamista on pyritty jo aikaisemmin sääntelemään kansainvälisesti ja etenkin EU-tasolla sitä tehty jo ennen virtuaalivaluuttojen olemassaoloa. Molempiin rikoksiin on jo ennestään kuulunut kansainvälinen luonne, mutta virtuaalivaluutat ovat korostaneet näitä ongelmia entisestään. Kaikki ne toimijat, jotka ovat tekemisissä rahanpesun ja terrorismin rahoittamisen estämisen ja ennaltaehkäisyn kanssa, ovat painottaneet, että virtuaalivaluuttoja koskeva sääntely tulisi ratkoa kansainvälisesti ja minkään valtion ei tulisi tarjota rikollisille ns. turvapaikkaa, josta käsin he voisivat harjoittaa rikollista toimintaa virtuaalivaluuttojen avulla ilman rikosoikeudellisia seuraamuksia. Rikosoikeus on yleensä nähty hyvin perinteisenä oikeudenalana, joka on jätetty valtioiden oman säädösvallan piiriin. Jopa EU-tasolla rikosoikeuden harmonisointi on suuri muutos, joskin huomioon ottaen yleinen globaali kehitys, käytännössä väistämätöntä tehokkaan rikollisuudentorjunnan näkökulmasta. Tulevaisuus näyttää, miten EU:n uusi kuudes rahanpesudirektiivi, rahanpesuasetus ja AMLA

kykenevät vastaamaan näihin haasteisiin. Jossain vaiheessa joudutaan myös luultavasti päivittämään käsityksiämme rikoslain kansallisesta luonteesta ja niihin liittyvistä periaatteista.

Suomessa lainsäädäntöön on tehty muutoksia ja sinne on lisätty lakeja, jotta virtuaalivaluuttojen avulla suoritettavaa rahanpesua ja terrorismin rahoittamista saataisiin kitkettyä. Tämän hetken voimassa oleva oikeus keskittyy sääntelemään niitä oikeushenkilöitä, jotka tarjoavat virtuaalivaluuttoja käyttäjille. Haasteita on syntynyt jonkin verran siihen liittyen, onko virtuaalivaluuttojen tarjoajilla todellisuudessa mahdollista esimerkiksi seurata virtuaalivaluuttojen liikkeitä ja havaita epäilyttävään toimintaan mahdollisesti liittyviä siirtoja. Virtuaalivaluuttojen tarjoajille siis siirrettiin sellainen tehtävä, johon edes viranomaiset eivät välttämättä pysty vastaamaan. Suomessa ei ainakaan toistaiseksi ole vielä ollut oikeustapauksia, joissa virtuaalivaluuttojen tarjoajia oltaisiin syytetty velvollisuuksiensa laiminlyönnistä. Ongelmaksi voi muodostua myös se, että virtuaalivaluuttoja otetaan käyttöön näiden viranomaisvalvonnan alaisena olevien toimijoiden ulkopuolella. Veronsa maksavat ja niin sanotusti ”lailliset” toimijat ovatkin virtuaalivaluuttojen piirissä suhteellisen uusi ilmiö, eikä mikään käytännössä estä virtuaalivaluuttojen hankintaa esimerkiksi Tor-verkosta. Poliisin seurantamenetelmien kehittyessä tämä toki käy jatkuvasti rikollisten kannalta riskialttiimmaksi. Vaikuttaakin osaksi siltä, että rikollisen toiminnan estämiseksi ratkaisu ei enää ole jatkuvasti tiukentuva tai aukottomampi lainsäädäntö, vaan tekoälyn ja teknologian kehittäminen löytämään ja estämään tätä rikollisuutta verkossa.

Selvää on se, että rikollisuuden ehkäisemiseksi virtuaalivaluuttoja on välttämätöntä säädellä *kansainvälisesti.* Viranomaistahojen alkushokin jälkeen ja tilanteen tasaantuessa uusia keinoja luultavasti löydetään, vaikkakin ongelmia varmasti tulee riittämään. Suomalainen lainsäätäjä voi lopulta jäädä kehityksessä enimmäkseen kansainvälisten säädösten implementoijan rooliin, mutta vastuu rikollisuuden torjunnan riittävästä resursoinnista on silti jokaisella valtiolla itsellään. Virtuaalivaluuttojen liikkeiden seuraamiseen ja mahdollisuuksiin voi vaikutusta olla myös jatkuvasti kehittyvillä *yksityisyydensuojasäännöksillä*. Jokainen virtuaalivaluuttojen käyttäjä ei lähtökohtaisesti voi olla rikoksesta epäilty, jonka toimia seurataan valtion viranomaisten toimesta tarkkaan. Aihetta sivuten mielenkiintoista on myös se, miten tulevaisuudessa esimerkiksi somejättien, kuten Metan tai Twitterin, keräämää dataa meistä voidaan käyttää apuna rikosten selvittämisessä. Rajanvetoa joudutaan pohtimaan etenkin, kun algoritmit kehittyvät jatkuvasti ja niiden avulla pystytään jo nykyisin luomaan aktiivisen sosiaalisen median käyttäjän tietojen perusteella hätkähdyttävän tarkka kuva käyttäjästä ja

hänen toimistaan. Tällä hetkellä algoritmeja käytetään aktiivisesti lähinnä kohdennetun mainonnan ja käyttäjää kiinnostavien muiden sisältöjen näyttämiseen.

Yleisesti voisi vielä todeta, että rahanpesun ja terrorismin rahoittamisen ehkäisemiseksi ja estämiseksi voidaan luultavasti loputtomiin pohtia erilaisia keinoja ja säätää lakeja. Lopulta tehokas rikostentorjunta vaatii kuitenkin sitä, että vastuuviranomaisilla on käytössään *riittävästi resursseja* niiltä vaadittavien toimenpiteiden toteuttamiseksi ja että kansainväliselle tiedonvaihdolle ja yhteydenpidolle eri viranomaisten ja myös yksityisten ja viranomaisten välille on toimivat rakenteet. Kriminalisointeja on turhaa suunnitella, mikäli nykyisiäkään velvoitteita ei pystytä täyttämään.

Vaikka Satoshi Nakamoto ei ehkä kyennyt luomaan täysin anonyymiä virtuaalivaluuttaa, joka mullistaisi maailman, avasi hän (tai he) oven sellaiselle polulle, jossa tekniikka kehittyy edelleen kiihtyvää tahtia, uusia lohkoketjuja perustetaan ja valtiot ovat alkaneet herätä siihen, että tehokkaita kansainvälisiä toimia tarvitaan. Hajaantuneisuuden ongelma on kuitenkin hyvin samankaltainen, kuin internetin kanssa sen alkuvuosina ja tilanteen tasoittuessa luultavasti löydetään ratkaisuja, jotka eivät lähde liiaksi laajentamaan rikosoikeudellista sääntelyä sille kuulumattomille urille.

Jatkotutkimuksen kannalta tutkielman aihe on erittäin hedelmällinen ja vaikka aihe olisi vuoden tai parin päästä tismalleen sama, on seuraavalla tutkijalla luultavasti jo aihepiiriin paljon uutta annettavaa. Tämän tutkielman jokaisesta pääjaksosta saisi myös varmasti muotoiltua tutkimuskysymyksen, johon voi lähteä laajastikin vastaamaan. Lähitulevaisuudessa erityisen kiinnostavaa on EU:n ja FATF:n tiukentuvat vaatimukset rikoslainsäädäntöjen harmonisoinnista ja kansallisvaltioiden reaktiot niihin, AMLA:n todellinen kyky välittää tietoa ja valvoa rahanpesua ja terrorismirikoksia EU:n alueella, sekä valtioiden mahdollisten omien virtuaalivaluuttaprojektien kehittäminen.