MYKOLO ROMERIO UNIVERSITETO
TEISĖS MOKYKLA
PRIVATINĖS TEISĖS INSTITUTAS

KOTRYNA, RAUPYTĖ
(MOKESČIŲ IR FINANSŲ TEISĖ)

KEITIMASIS INFORMACIJA KOVOJE SU FINANSINIAIS NUSIKALTIMAIS IR ASMENS DUOMENŲ APSAUGOS REIKALAVIMAI

Magistro baigiamasis darbas

Darbo vadovas –
lekt.;
dr.,
Kazimieras Zaveckas

Vilnius, 2024

TURINYS

SANTRUMPŲ SĄRAŠAS

ES – Europos Sąjunga

FATF – Finansinių veiksmų darbo grupė, (angl. *Financial Action Task Force*)

FŽP – finansinės žvalgybos padaliniai

STR – pranešimas apie įtartinas operacijas (angl. *suspicious transaction report*)

JAV – Jungtinės Amerikos Valstijos

LED – Direktyva ES 2015/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo (*angl. law enforcement directive*)

BDAR – Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas)

EDPB – Europos duomenų apsaugos valdyba (angl. *European Data Protection Board),* nuo 2018m.

Konvencija – Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija

Chartija – Europos Sąjungos Pagrindinių teisių Chartija

WP29 – patariamoji Darbo grupė teisės į privatumą ir asmens duomenų apsaugą srityje (angl. *Article 29 Working Party*) iki 2018m.

EDPS – Europos duomenų apsaugos priežiūros pareigūnas (angl. *European Data Protection Supervisor*)

EŽTT – Europos Žmogaus Teisių Teismas

ESTT – Europos Sąjungos Teisingumo Teismas

TMNL – keitimosi duomenimis iniciatyva Olandijoje (oland. *Transactie Monitoring Nederland B.V.*)

DPA – nacionalinės asmens duomenų apsaugos institucijos (angl. *Data Protection Authority*)

FinCEN – finansinės žvalgybos padalinys Jungtinės Amerikos Valstijose (angl. *Financial Crime Enforcement Network*)

PP ir TFP – Pinigų plovimo ir teroristų finansavimo prevencija

JMLIT – keitimosi duomenimis iniciatyva Jungtinėje Karalystėje (angl. *Joint Money Laundering Intelligence Taskforce)*

SAMLIT – keitimosi duomenimis iniciatyva Švedijoje (angl. *Swedish Anti Money Laundering initiative)*

COSMIC – keitimosi duomenimis iniciatyva Singapūre (angl. *Collaborative Sharing of Money Laundering/Terrorism Financing*)

ĮVADAS

Tiriama problema ir aktualumas:

Finansiniai nusikaltimai daro žalą visuomenei, keldami grėsmę finansų sistemos stabilumui ir sudarydami kliūtis ekonomikos augimui. Nepaisant kovą su finansiniais nusikaltimais vykdančių institucijų ir tarptautinių organizacijų ilgus metus dedamų pastangų, užkirsti kelią finansiniams nusikaltimams, nusikalstamos grupuotės ypač gretai prisitaiko prie kintančios reguliacinės aplinkos, išnaudodamos globalizacijos ir skaitmenizavimo procesų teikiamas galimybes[1]. Finansinių nusikaltimų schemoms darantis vis sudėtingesnėms, apimant ne vieną jurisdikciją, įtraukiant daugiau finansų įstaigų, kovą su finansiniais nusikaltimais vykdančios institucijos turi atlikti sudėtingus tarptautinius tyrimus. Suprantama, kad tokiems tyrimams kritiškai svarbus efektyvus keitimasis informacija, tarp kovą su finansiniais nusikaltimais vykdančių institucijų. Pagal nusistovėjusią praktiką, finansų įstaigos[2] nesikeičia informacija tarpusavyje. Informacijos mainai tarp finansų įstaigų ir finansinės žvalgybos padalinių (toliau FŽP), bei FŽP ir teisėsaugos institucijų skirtingose jurisdikcijose, tai pat nevyksta sklandžiai. Todėl, kova su finansiniais nusikaltimais nėra tokia efektyvi, kokia galėtų būti. Reaguojant į susiklosčiusią situaciją, tiek atskirose Europos Sąjungos valstybėse, tiek trečiosiose šalyse, finansų įstaigos ir kompetentingos valstybės institucijos jungia jėgas kovai su finansiniais nusikaltimais, kelia glaudesnio bendradarbiavimo iniciatyvas, kurias palaiko ir teisėkūros institucijos bei tarpvyriausybinės organizacijos. Pavyzdžiui 2023m. atnaujintose FATF rekomendacijose valstybės kviečiamos peržiūrėti atitinkamų institucijų bendradarbiavimą, veiklos koordinavimą ir dalinimąsi informacija[3]. Tai pat, siekiant padidinti finansų įstaigų galimybes dalintis informacija su kitomis finansų įstaigomis, teisėsauga ir tarptautinėmis organizacijomis, peržiūrėta ES įstatyminė bazė[4]. Šiomis iniciatyvomis siekiama sukurti, keitimosi informacija tarp finansų įstaigų ir su teisėsaugoms institucijomis, modelius, duomenų mainų platformas. Naujų modelių įgyvendinimas gali atnešti, efektyvumo prasme, daug žadančių rezultatų kovoje su finansiniais nusikaltimais.

---

[1] INTERPOL General Secretariat, *Interpol's financial crime and anti-corruption centre (IFCACC)*,(Lyon, 2022),1, https://www.interpol.int/content/download/17283/file/IFCACC_Project%20sheet_EN01.pdf

[2] Terminas finansų įstaigos naudojamas referuojant į visus finansų rinkos dalyvius.

[3] Financial Action Task Force (FATF), *International standards on combating money laundering and the financing of terrorism & proliferation*, (Paris, 2023), 10-11, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

[4] Anti-money laundering: Council and Parliament strike deal on stricter rules. Council of EU press releases. 2024-01-18. https://www.consilium.europa.eu/en/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules/

Tiesa, tam, kad šias iniciatyvas būtų galima įgyvendinti reikalingas tinkamos teisinės-reguliacinės aplinkos parengimas. Kovai su finansiniais nusikaltimais renkami finansiniai duomenys, kurie tai pat kvalifikuojami, kaip asmens duomenys. Tarp kovos su finansiniais nusikaltimais ir teisės į privatumą bei asmens duomenų apsaugą glūdintis konfliktas, įvardijamas kaip pagrindinė kliūtis, sėkmingam informacijos perdavimui tarp kovą su finansiniais nusikaltimais vykdančių institucijų, ypač trūkstant teisinio tikrumo šioje srityje. Skirtingų interesų – nacionalinio saugumo, imperatyviai užtikrinamo valstybės, ir nuo demokratinės visuomenės neatsiejamos laisvės konkurencija nėra nauja problema, jau prieš du dešimtmečius taikliai įvardinta kaip mūšis tarp saugumo ir laisvės[5]. Tačiau, magistro baigiamame darbe atsiribojama nuo išsamios interesų konkurencijos analizės ir susitelkiama į teisės į privatumą bei asmens duomenų apsaugą ir kovos su finansiniais nusikaltimais teisinio reguliavimo galimybes, veikti kartu, keičiantis informacija kovoje su finansiniais nusikaltimais. Analizė grindžiama naujausiomis iniciatyvomis, vertinama kaip jos suderinamos su asmens duomenų apsaugai taikomais reikalavimais.

Mokslinis naujumas ir problemos ištyrimo lygis: Keitimosi informacija tarp finansų įstaigų modelis ir poveikis kovoje su finansiniais nusikaltimais plačiai analizuotas FATF publikacijoje[6]. Keitimosi informacija tarp finansų įstaigų ir teisėsaugos modelis analizuotas Europos Komisijos specialistų darbo grupėje[7]. Abu šie modeliai plačiai analizuoti FFIS (angl. *The Future of Financial Intelligence sharing*) programos publikacijoje[8]. B. Vogel, teoriniu aspektu, įvertino keitimąsi duomenimis tarp finansų įstaigų ir teisėsaugos[9]. Tačiau nei viename minėtame mokslo šaltinyje neatliekamas keitimosi informacija, kovoje su finansiniais nusikaltimais, teisėtumo vertinimas, iš teisės į privatumą ir asmens duomenų apsaugą perspektyvos.

[5] Robert S. Pasley, „Privacy Rights v. Anti-Money Laundering Enforcement“, *North Carolina Banking Institute* 6, 1 (2022): 150 http://scholarship.law.unc.edu/ncbi/vol6/iss1/7

[6] Financial Action Task Force (FATF), Partnering in the fight against financial crime data protection, technology and private sector information sharing, Paris, 2022, https://www.fatfgafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html

[7] Europos Komisija, „On the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing“, Commission staff working document, Briuselis, 2022, https://finance.ec.europa.eu/system/files/2022-10/221028-staff-working-document-aml-public-privatepartnerships_en.pdf

[8] Future of Financial Intelligence Sharing (FFIS) research program, „Lessons in private-private financial information sharing to detect and disrupt crime, A Survey and Policy Discussion Paper, 2022, Royal United Services Institute, https://www.futurefis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf

[9] Benjamin Vogel, „Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing“, EUCRIM Forum 1 (2022): 52-60, https://eucrim.eu/articles/potentials-and-limits-of-public-private-partnerships-against-money-laundering-and-terrorism-financing/

Kovos su finansiniais nusikaltimais reguliavimo poveikį teisei į privatumą ir asmens duomenų apsaugą, disertacijoje plačiai analizavo C. Kaiser[10]. Kovos su finansiniais nusikaltimais reguliavimo santykį su antriniais teisės šaltiniais, įtvirtinančiais teisę į privatumą ir asmens duomenų apsaugą, nagrinėjo V. Ferrari[11], W. Maxwell[12]. Tačiau, šie autoriai neišskyrė, būtent, keitimosi duomenimis kovoje su finansiniais nusikaltimais. Kituose užsienio mokslininkų darbuose daugiau dėmesio skiriama informacijos mainams tarp finansinės žvalgybos padalinių (Quintel[13], Pavlidis[14]).

Lietuvos mokslininkų darbuose teisė į privatumą ir asmens duomenų apsaugą, keičiantis informacija tarp kovą su finansiniais nusikaltimais įgyvendinančių subjektų, analizuota nebuvo. Artimiausi temai Lietuvos autorių mokslo šaltiniai yra E. Markevičiaus disertacija[15], kurioje analizuotos asmens duomenų perdavimo trečiosioms valstybėms problemos ir Mykolo Romerio universiteto mokslininkų straipsnis[16], kuriame analizuotas vieno iš BDAR principų įgyvendinimas finansų įstaigose.

Be aukščiau išvardintų mokslinių šaltinių, magistro baigiamajame darbe remiamasi teismų praktika, įstatymo keitimo projektais, įtraukiant ir naujausius LR Pinigų plovimo ir teroristų finansavimo prevencijos įstatymo pakeitimus[17], *soft law* teisės šaltiniais: kompetentingų institucijų (FATF, EDPB ir kt.) rekomendacijomis, nuomonėmis ir gairėmis.

Baigiamojo darbo reikšmė: Keitimosi informacija kovoje su finansiniais nusikaltimais ir asmens duomenų apsaugos reikalavimų analizė gali prisidėti kuriant informacijos mainų, tarp kovą su finansiniais nusikaltimais vykdančių subjektų, modelius ir tam tinkamą teisinę bazę, kartu užpildant mokslinių tyrimų šia tema trūkumą Lietuvoje.

---

[10] Carolina Kaiser, „Privacy and identity issues in financial transactions : the proportionality of the European Anti-Money laundering legislation“, PhD Thesis, University of Groningen, 2018, https://research.rug.nl/en/publications/privacy-and-identity-issues-in-financial-transactions-the-proport

[11] Valeria Ferrari, „Crosshatching Privacy: Financial Intermediaries' Data Practices between Law Enforcement and Data Economy“, European Data Protection Law Review (EDPL) 6, 4 (2020): 522-535, https://doi.org/10.21552/edpl/2020/4/8

[12] Winston Maxwell, The GDPR and private sector measures to detect criminal activity, Paris, 2021, https://hal.archives-ouvertes.fr/hal-03316259

[13] Teresa Quintel, „Data protection rules applicable to Financial Intelligence Units: still no clarity in sight“, ERA Forum, 23, 1 (2022): 53–74, https://doi.org/10.1007/s12027-021-00697-z

[14] George Pavlidis, „Financial information in the context of anti-money laundering: Broadening the access of law enforcement and facilitating information exchanges“, Journal of Money Laundering Control, 23, 2, (2020): 369–378, https://doi.org/10.1108/JMLC-10-2019-0081

[15] Edgaras Markevičius, „Asmens duomenų perdavimo elektroninėje erdvėje tarp Europos Sąjungos ir Jungtinių Amerikos Valstijų teisinės problemos“, Daktaro disertacija, Mykolo Romerio universitetas, 2022, https://www.mruni.eu/wp-content/uploads/2022/08/Edgaras-Markevicius_MRUweb.pdf

[16] Marius Laurinaitis, Darius Štitilis ir Egidijus Verenius, „Asmens duomenų kiekio mažinimo principo įgyvendinimas finansų įstaigose“, JURISPRUDENCIJA, 27, 2 (2020): 389–410, https://ojs.mruni.eu/ojs/jurisprudence/article/view/6365/5325

[17] „Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo Nr. VIII-275 2, 9, 10, 11, 15, 16, 21, 22, 23, 25, 29, 36, 39, 40, 48, 49 straipsnių pakeitimo ir Įstatymo papildymo 15-1, 15-2, 46-1 straipsniais įstatymas“, (TAR, 2024-04-25, Nr. 2024-07537), INFOLEX, žiūrėta 2024-04-28. https://www-infolex-lt.skaitykla.mruni.eu/ta/941993#Xfcc32c158c44476a8f6b690995d3a024

Tyrimo tikslas: Atlikti pokyčių, reikalingų keičiantis informacija kovoje su finansiniais nusikaltimais, teisinę analizę, vertinant poveikį teisei į privatumą ir asmens duomenų apsaugą.

Tyrimo uždaviniai:

1. Apžvelgti informacijos mainus ir reikalingus pokyčius kovoje su finansiniais nusikaltimais.
2. Nustatyti, iš teisės į privatumą ir asmens duomenų apsaugą kylančius reikalavimus, keitimuisi informacija kovoje su finansiniais nusikaltimais, užtikrinant dviejų svarbių interesų pusiausvyrą.
3. Išanalizuoti atskirų valstybių iniciatyvas, keistis informacija tarp finansų įstaigų (angl. *private-private partnership),* ir situaciją Lietuvoje.
4. Išanalizuoti atskirų valstybių iniciatyvas, keistis informacija tarp teisėsaugos ir finansų įstaigų (angl. *public-private partnership),* ir situaciją Lietuvoje.

Tyrimo metodika: Įgyvendinant tikslą ir uždavinius, magistro baigiamajame darbe, kompleksiškai naudojami teisės aiškinimo ir taikymo moksliniai pažinimo metodai. Naudojant *lyginamąjį istorinį metodą*, analizuojama kovos su finansiniais nusikaltimais, teisės į privatumą ir asmens duomenų apsaugą teisinio reguliavimo raida. Taikant *dokumentų ir mokslinių šaltinių analizės metodą*, gilinamasi į mokslinę literatūrą, pirminės ir antrinės teisės šaltinius, *soft law*. Analizuojant įstatymų nuostatas, teismų sprendimus, taikomas *loginės, sisteminės analizės metodas*. Taikant *apibendrinimo metodą* pateikiamos išvados ir apibendrinimai.

Tyrimo struktūra: Magistro baigiamąjį darbą sudaro: titulinis lapas, turinys, santrumpų sąrašas, įvadas, dėstomoji dalis. Dėstomoji dalis išskirta į tris struktūrines dalis. Pirmoje dalyje atskleidžiama, kaip keičiamasi informacija tarp kovą su finansiniais nusikaltimais įgyvendinančių institucijų, ir kokie pokyčiai reikalingi. Antroje dalyje gilinamasi, kokie reikalavimai kyla iš teisės į privatumą ir asmens duomenų apsaugą, keičiantis informacija kovoje su finansiniais nusikaltimais. Trečioje dalyje atliekama iniciatyvas įgyvendinančių atskirų valstybių praktikos analizė ir susisteminamas keitimosi informacija modelių poveikis teisei į privatumą ir asmens duomenų apsaugą. Toliau pateikiamos struktūrizuotos išvados ir pasiūlymai, literatūros sąrašas, anotacija ir santrauka lietuvių bei anglų kalbomis.

Ginamasis teiginys:

Keitimosi informacija tarp finansų įstaigų modeliai yra būtinai reikalinga priemonė kovoje su finansiniais nusikaltimais ir gali būti suderinami su teise į privatumą ir asmens duomenų apsaugą, išlaikant interesų balansą.

1. KOVOS SU FINANSINIAIS NUSIKALTIMAIS APŽVALGA

1.1 Pinigų sekimo principas

Teisinė pareiga, finansų įstaigoms kovoti su finansiniais nusikaltimais, pirmą kartą įtvirtinta 1970m., JAV, Banko paslapties akte (*angl. Bank Secrecy Act)*. Tuomet, finansų įstaigoms nustatyta pareiga stebėti į JAV įeinančius ir išeinančius mokėjimus ir nustatyti juos atliekančių asmenų tapatybę, siekiant aptikti galimus pinigų plovimo atvejus[18]. Kitose pasaulio valstybėse pinigų plovimo prevencijos pradžia galima laikyti 1989 metus, kai G7 šalys įkūrė Finansinių veiksmų darbo grupę (*angl. Financial Action Task Force,* toliau FATF). FATF yra tarptautinė organizacija, atsakinga už kovos su pinigų plovimu standartų nustatymą. Nors FATF rekomendacijos nėra teisiškai privalomos, ši organizacija turi didelę politinę įtaką. Išsivysčiusios pasaulio valstybės perkelia FATF rekomendacijas į savo nacionalinę teisę.

Europos Sąjungoje (toliau ES) pinigų plovimo prevencijos era prasidėjo 1991m., priėmus 1-ąją Direktyvą dėl finansų sistemos naudojimo pinigų plovimui prevencijos. Daugiau nei per du dešimtmečius, priėmus 5 Direktyvas, ir nuolat derinant teisinę sistemą su FATF rekomendacijomis, padaryta didelė pažanga kovojant su finansiniais nusikaltimais[19].

Maždaug tuo pačiu metu, tarp 7 ir 9 dešimtmečio, vietoje iki tol vyravusio tradicinio požiūrio surasti ir išardyti organizuotas nusikalstamas grupuotes, teisėsauga pradėjo taikyti pinigų sekimo principą (*angl. follow the money*)[20]. Pinigų sekimo principas, paremtas idėja, kad pagrindinis organizuoto nusikalstamumo motyvas yra finansinė nauda[21], todėl užtikrinus, kad nusikaltėliai negalės panaudoti nusikalstamu būdu įgytų lėšų, mažės paskata nusikalsti. Taigi, pinigų sekimas yra kovos su finansiniais nusikaltimais būdas, kuriam būdingas ne tik nubaudimo, bet ir prevencijos elementas.

Taikant pinigų sekimo principą, finansinių operacijų duomenys yra svarbiausias teisėsaugos institucijų informacijos šaltinis[22]. Kadangi, šiuos duomenis turi finansų įstaigos, kova su finansiniais nusikaltimais tapo neatsiejama nuo valstybinio ir privataus sektoriaus

---

[18] „History of Anti-Money Laundering (AML) Laws“, Sigma360, žiūrėta 2023-01-27, https://www.sigma360.com/knowledge-center/history-of-aml-laws

[19] Foivi Mouzakiti, „Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive“, *New Journal of European Criminal Law* 11, 3 (2020): 352. https://doi.org/10.1177/2032284420943303

[20] Tom R. Naylor, *Follow-the-money methods in crime control policy*, (Toronto, 1999), 1, https://www.ncjrs.gov/nathanson/washout.html

[21] EPP Group, *How to combat organised crime in the European Union*, 2022, 3, https://www.eppgroup.eu/newsroom/publications/epp-group-position-paper-on-how-to-combat-organised-crime-in-the-european-union

[22] Ferrari, *supra note*, 11: 524.

bendradarbiavimo, o finansų įtaigoms priskirtas kvazi-valstybinis vaidmuo[23], įgyvendinat politinius tikslus.

Pradėtas naudoti tiriant pinigų plovimą, pinigų sekimo principas greitai perimtas ir kitiems finansiniams nusikaltimams tirti. 2001m., po rugsėjo 11 įvykių, supratus, kad pinigai yra „gyvybiškai“ svarbus šaltinis teroristinėms operacijoms[24], kriminalizuotas teroristų finansavimas. Šalia pinigų plovimo prevencijos vykdymo, finansų įstaigos įpareigotos stebėti pinigų srautus, kurie gali būti skirti teroristų finansavimui. Tai pat, po 2008m. pasaulinės finansų krizės, ir 2013-2016m. duomenų nutekinimo iš ofšorinių jurisdikcijų skandalų, finansų įstaigos įpareigotos stebėti, kad naudojantis jų paslaugomis nebūtų legalizuojamos korupcijos[25] ir mokesčių vengimo[26] kilmės lėšos. Negana to, finansų įstaigos įpareigotos įgyvendinti ir tarptautinės politikos priemonę – tarptautines sankcijas. Sankcijų įgyvendinimas reikalauja užtikrinti, kad tiksliniai subjektai, į kuriuos nukreipti ribojimai, negautų prieigos prie finansinių išteklių, naudojantis finansų įstaigų paslaugomis. Taip, finansų įstaigos tapo „vartų saugotojomis“ [27], kovoje su finansiniais nusikaltimais.

Kita vertus, pinigų sekimo principo taikymas sugriovė tradicines finansinio privatumo prielaidas, kartu finansų įstaigoms atnešdamas naštą, rasti tinkamą pusiausvyrą tarp privataus gyvenimo apsaugos ir valstybės saugumo interesų užtikrinimo[28]. Finansiniai duomenys laikomi asmens duomenimis[29], todėl nuogąstavimų, dėl teisės į privatumą apsaugos, finansų įstaigoms renkant asmens duomenis finansiniams nusikaltimams tirti, atsirado nuo pat pinigų plovimo prevencijos vykdymo pradžios[30]. Šiame magistro baigiamajame darbe nagrinėjamas tik keitimosi duomenimis tarp kovą su finansiniais nusikaltimais vykdančių subjektų klausimas. Siekiant visapusiškos keitimosi informacija kovoje su finansiniais nusikaltimais ir taikomų asmens duomenų apsaugos reikalavimų analizės, pirmiausia, analizuojama kaip įpareigoti subjektai ir teisėsaugos institucijos keičiasi duomenimis, ir kokie pokyčiai svarstomi.

---

[23] Robert E. Litan, Michael Pomerleano, Vasudevan Sundararajan, Financial sector governance: the roles of the public and private sectors (Brookings Institution Press, 2002) cituota iš Ferrari, *supra note*, 11: 525.
[24] Gauri Sinha, „AML-CTF: a forced marriage post 9/11 and its effect on financial institutions“, *Journal of Money Laundering Control*, 16, 2 (2013): 142, https://doi.org/10.1108/13685201311318494
[25] Nadim Kyriakos-Saad, Gianluca Esposito ir Nadine Schwarz, „The Incestuous Relationship Between Corruption and Money Laundering”, *Revue internationale de droit pénal* 83, 1–2 (2012): 165, https://www.cairn.info/revue-internationale-de-droit-penal-2012-1-page-161.htm
[26] Dean Kemsley, Sean A. Kemsley ir Frank T. Morgan, „Tax evasion on lawful income: is it a form of money laundering?“ *Journal of Financial Crime* 31, 1 (2023): 2, https://doi.org/10.1108/JFC-11-2022-0268
[27] World Economic Forum. *The Role and Responsibilities of Gatekeepers in the Fight against Illicit Financial Flows: A Unifying Framework*, 2021, 2, https://www3.weforum.org/docs/WEF_Gatekeepers_A_Unifying_Framework_2021.pdf
[28] Maxwell, *supra note,* 12: 2.
[29] Ferrari, *supra note*, 11: 522.
[30] Pasley, *supra note*, 5: 147.

1.2 Finansinių nusikaltimų prevenciją įgyvendinantys subjektai

1.2.1 Finansų įstaigos

Kaip ir minėta ankstesniame poskyryje, kova su finansiniais nusikaltimais pagrįsta pareigų perdavimų privačiam sektoriui. Finansų įstaigos, kaip „vartų saugotojos“, turi užtikrinti, kad pasinaudojant finansų sistema nebūtų vykdomi finansiniai nusikaltimai. Ši užduotis įgyvendinama taikant deramo kliento patikrinimo procedūrą (angl. *Customer Due Diligence*). Tai reiškia, kad finansų įstaigos turi pažinti klientus (*angl. Know Your Customer*). Kliento pažinimo principo taikymas reikalauja identifikuoti visus klientus, saugoti finansinių operacijų įrašus, ir informuoti kompetentingas valstybines institucijas apie įtartinas finansines operacijas.

Atliekant bet kokį sandorį finansų įstaigoje, turi būti nustatoma siuntėjo ir gavėjo tapatybė. Juridinių asmenų atliekamų sandorių galutinis naudos gavėjas nustatomas iki fizinio asmens. Be tapatybės nustatymo, kliento pažinimo principas reikalauja surinkti ir tokią informaciją, kaip duomenis apie gaunamas pajamas, lėšų kilmę, verslo santykių pobūdį ir pan. Kliento pažinimo etape surinkta informacija toliau naudojama atliekant nuolatinę stebėseną. Finansų įstaiga nuolat stebi visas klientų sąskaitose vykdomas operacijas, siekiant nustatyti ar nėra jokios neįprastos veiklos, ar kliento vykdomos operacijos atitinka jo mokėjimo įpročius, pajamų šaltinius, verslo logiką ir pan. Aptikus neįprastą veiklą, sustabdomos kliento operacijos ir informacija perduodama už finansinių nusikaltimų tyrimą atsakingai valstybės institucijai – finansinės žvalgybos padaliniui (toliau FŽP), užpildant pranešimą apie įtartinas pinigines operacijas, ar įtartinus sandorius (*angl. suspicious transaction report,* toliau STR). Šioje vietoje svarbu pažymėti, kad būtent nuolatinis kliento stebėjimas yra daugiausia diskusijų keliantis klausimas, vertinat iš teisės į privatumą ir asmens duomenų apsaugą perspektyvos (plačiau 2.4.2 skyrelyje).

Šiuo metu, ES teisėje neįtvirtinta galimybė finansų įstaigoms tarpusavyje dalintis informacija apie klientus ir jų vykdomas operacijas. Išskyrus, Direktyvoje ES 2015/849 dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos (toliau 4-oji pinigų plovimo prevencijos Direktyva), įtvirtintą leidimą, dalintis pradinio mokėtojo ir naudos gavėjo informacija, įtraukta vykdant mokėjimo pavedimus[31], ar leidimą, dalintis finansinių nusikaltimų prevencijos tikslais surinkta kliento informacija, tarp tai pačiai įmonių grupei priklausančių

[31] Europos Parlamento ir Tarybos Direktyva (ES) 2015/849 2015 m. gegužės 20d. „Dėl finansų sistemos naudojimo pinigu plovimui ar teroristu finansavimui prevencijos, kuria iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 ir panaikinama Europos Parlamento ir Tarybos direktyva 2005/60/EB bei Komisijos direktyva 2006/70/EB“, 39 str. 5d., EUR-LEX, žiūrėta 2023-01-26, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32015L0849

finansų įstaigų [32]. Informacija apie klientus ir vykdomas operacijas, kelianti įtarimų dėl galimo finansinių nusikaltimo vykdymo, perduodama FŽP. Tai pat, finansų įstaigos įpareigotos teikti informaciją apie klientą, kai to prašo FŽP, ar teisėsaugos institucijos.

1.2.2 Finansinės žvalgybos padaliniai ir teisėsaugos institucijos

Kaip ir minėta 1.1 poskyryje, tirti finansiniams nusikaltimams reikalingi finansų įstaigų turimi finansiniai duomenys. Šie duomenys yra konfidencialūs ir patenka privatumo bei asmens duomenų apsaugos reguliavimo sritį. Iki FATF įkūrimo, norint gauti prieigą prie finansų įstaigose laikomų duomenų, teisėsaugos institucijos turėdavo gauti teismo leidimą. Ieškant būdų efektyviau tirti finansinius nusikaltimus, suprasta, kad teisėsaugai reikia suteikti paprastesnę prieigą prie duomenų, tačiau buvo reikalingas filtras, nes ne kiekvienas įtarimas būtinai reiškia nusikaltimą[33]: Nefiltruotos prieigos teisėsaugos institucijoms suteikimas, pažeistų teisę į privatumą. Taip, 1990m., Jungtinės Amerikos Valstijose (toliau JAV) įkurtas pirmasis FŽP. Šiuo metu, Egmonto grupės – pasaulinio neformalaus FŽP tinklo nariais yra FŽP iš 170 valstybių. ES, kuriant FŽP, iš dalies dėl savo prevencinės paskirties, iš dalies dėl to, kad Europos Sąjungos Sutartimi nacionalinio saugumo klausimas paliktas išsiimtinai kiekvienos valstybės kompetencijai[34], FŽP nebuvo „tradiciškai“ priskirti prie teisėsaugos institucijų, o įsteigtos specialios institucijos[35]. Šių institucijų organizacinė struktūra ir padėtis nacionalinėje teisės sistemoje liko mažai harmonizuota ES lygmeniu[36]. Trūkstant detalių nurodymų iš įstatymų leidėjo, valstybės narės naudojosi plačia diskrecija pasirenkant FŽP modelį. Šiai dienai, valstybės narės įprastai yra pasirinkusios vieną iš dviejų pagrindinių modelių: administracinį arba teisėsaugos. Pastarajame modelyje FŽP funkcijos suteikiamos specialiam policijos padaliniui, turinčiam stiprių analitinių, tyrimo įgūdžių ir galių, pavyzdžiui, dalytis taktine žvalgybos informacija su teisėsauga ir finansų sektoriumi, taip pat areštuoti įtartiną sandorį. Toks FŽP įprastai neatlieka reguliacinės priežiūros funkcijų. Teisėsaugos FŽP pavyzdžiais yra *Finansinių nusikaltimų tyrimo tarnyba* Lietuvoje, *Zentralstelle für Finanztransaktionsuntersuchungen,* Vokietijoje. Pagal administracinį modelį, FŽP steigiamas viešojo administravimo struktūrose, paprastai prie Finansų ministerijos. Šiuo atveju, FŽP neatlieka ikiteisminių tyrimų, o turi pareigą teikti taktinę žvalgybos informaciją teisėsaugai, tačiau neturi

[32] Europos Parlamento ir Tarybos Direktyva (ES) 2015/849, *supra note*, 31: 39 str. 3 ir 4 d.
[33] Jean-Francois Thony, *Use of Information Exchange in Criminal Matters to Combat Money Laundering and Financing of Terrorism*, (IMF, 2007), 9, https://www.elibrary.imf.org/display/book/9781589064874/ch001.xml
[34] „Europos Sąjungos Sutartis“, 1957 m., suvestinė redakcija 2012-10-26, 4 str., EUR-LEX, žiūrėta 2023-01-26, https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=celex%3A12012E%2FTXT
[35] Mouzakiti, *supra note*, 19: 352-353.
[36] Magdalena Brewczynska, „Financial Intelligence Units: Reflections on the applicable data protection legal framework“, *Computer Law and Security Review*, 43 (2021), 2, https://doi.org/10.1016/j.clsr.2021.105612

teisės dalytis tokia informacija tiesiogiai su finansų įstaigomis. Toks FŽP dažnai atlieka priežiūros ir (arba) reguliuotojo vaidmenį, užtikrinant, kad įpareigoti subjektai tinkamai vykdytų kovos su finansiniais nusikaltimais įstatyminius reikalavimus. Administracinio FŽP pavyzdžiu gali būti Italijos FŽP – *Unitàdi Informazione Finanziaria per l'Italia*, pavaldus centriniam Italijos bankui. Valstybės, su stipriomis banko paslapties tradicijomis, pvz. Liuksemburgas, įsteigė trečiojo tipo – teisminį FŽP, kuris steigiamas kaip specialus Generalinės prokuratūros padalinys. Toks FŽP modelis apjungia teisėsaugos ir administracinio tipo FŽP bruožus. Taip pat, gali būti hibridinis FŽP modelis, apjungiantis administracinio, teisminio ir teisėsaugos FŽP požymius[37].

Dėl skirtingų FŽP modelių, kyla keblumų keičiantis informacija, nes taikomi skirtingi asmens duomenų apsaugos teisės aktai. Administracinio tipo FŽP taiko Reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo[38] (toliau BDAR), o teisėsaugos tipo FŽP – Direktyvą ES 2015/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo (*angl. law enforcement directive,* toliau LED)[39]. Skirtingai taikomi duomenų apsaugos įstatymai kelia neaiškumų ir įstatyminiame reguliavime. Pavyzdžiui 4-oji pinigų plovimo prevencijos Direktyva nurodo, taikyti BDAR, kai tuo tarpu Direktyva ES 2019/1153, kuria nustatomos taisyklės dėl paprastesnio finansinės ir kitos informacijos naudojimo tam tikrų nusikalstamų veikų prevencijos, nustatymo, tyrimo ir baudžiamojo persekiojimo už jas tikslais (pagal šią direktyvą FŽP keičiasi informacija tarpusavyje), referuoja tiek į LED, tiek į BDAR[40]. Tvarkant asmens duomenis remiantis LED, galimi didesni asmens teisių suvaržymai, nei tvarkant duomenis pagal BDAR. Praktiniu aspektu, kyla problema, kad teikiančiam FŽP perduodant asmens duomenis, duomenų apsaugos reikalavimai gali nesutapti su priimančiojo FŽP taikomais reikalavimais. Šioje vietoje, svarbu atkreipti dėmesį, kad informacijos manai yra

[37] Katarzyna J. McNaughton, „The variability and clustering of Financial Intelligence Units (FIUs) – A comparative analysis of national models of FIUs in selected western and eastern (post-Soviet) countries", *Journal of Economic Criminology*, 2, (2023), 3, https://doi.org/10.1016/j.jeconc.2023.100036

[38] Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679, 2016 m. balandžio 27 d, „Dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)", 63 konstatuojama dalis, EUR-LEX, žiūrėta 2023-01-26, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679

[39] Europos Parlamento ir Tarybos direktyva (ES) 2016/680, 2016 m. balandžio 27d, „ Dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR", EUR-LEX, žiūrėta 2023-01-26, https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L0680

[40] Europos Parlamento ir Tarybos Direktyva (ES) 2019/1153, 2019 m. birželio 20d. „kuria nustatomos taisyklės dėl paprastesnio finansinės ir kitos informacijos naudojimo tam tikrų nusikalstamų veikų prevencijos, nustatymo, tyrimo ir baudžiamojo persekiojimo už jas tikslais ir kuria panaikinamas Tarybos sprendimas 2000/642/TVR", 25 konstatuojama dalis, EUR-LEX, žiūrėta 2023-01-26, https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019L

neįprastai svarbūs tinkamam FŽP funkcijų vykdymui, nes FŽP veikia kaip tarpinė institucija tarp privataus sektoriaus ir teisėsaugos, atsakinga už STR informacijos analizę ir perdavimą[41].

Atlikdama analizę, FŽP iš finansų įstaigų gauna užpildytus STR. Po teroristų išpuolio Paryžiuje ir *Panama papers* skandalo[42], siekiant stiprinti finansų įstaigų ir FŽP bendradarbiavimą bei palengvinti informacijos mainų procesą, mažiau formaliais kanalais, nei STR perdavimas, Direktyvoje ES 2018/843 (toliau 5-oji Pinigų plovimo prevencijos Direktyva), kuria iš dalies keičiama Direktyva (ES) 2015/849, buvo įtvirtinta „galimybė prašyti informacijos iš bet kurio įpareigotojo subjekto [....] net jei anksčiau nebuvo pateiktas STR“[43].

Tai pat, atliekant analizę, FŽP keičiasi informacija su kitų valstybių narių FŽP. 4-ojoje pinigų plovimo prevencijos Direktyvoje, valstybėms narėms nustatyta pareiga užtikrinti, kad FŽP kuo labiau bendradarbiautų tarpusavyje nepriklausomai nuo jų organizacinio statuso[44]. FŽP keičiasi informacija su FŽP kitoje jurisdikcijoje:

1) savo iniciatyva, kai mano, kad turima informacija arba atlikta analizė gali būti naudinga kitos valstybės narės FŽP,
2) privalomai turi perduoti informaciją, kai ji susijusi su kita valstybe nare,
3) atsakant į kitų valstybių narių FŽP užklausas[45].

Kai atlikus analizę pasitvirtinta STR užpildymo metu kilusių įtarimų pagrįstumas, FŽP perduoda informaciją teisėsaugos institucijoms. Sąvoka teisėsaugos institucijos, magistro baigiamajame darbe, naudojama referuojant į nacionalines institucijas, atsakingas už ikiteisminį finansinių nusikaltimų tyrimą ir baudžiamojo persekiojimo vykdymą.

Kartais atlikti analizei, FŽP reikalinga informacija iš užsienio teisėsaugos institucijų ir atvirkščiai. 4-ają Pinigų plovimo prevencijos Direktyva, valstybės narės įpareigotos suteikti FŽP „tiesioginę arba netiesioginę prieigą prie finansinės, administracinės ir teisėsaugos informacijos, kurios jiems reikia, kad galėtų tinkamai atlikti savo užduotis“[46]. Tai pat, Direktyva 2019/1153, įtvirtinta pareiga valstybėms narėms užtikrinti, kad jų nacionalinis FŽP bendradarbiautų su paskirtomis teisėsaugos institucijomis ir laiku reaguotų į prašymus, pateikti informaciją, ar atlikti analizę, o paskirtosios institucijos atsakytų į nacionalinio FŽP prašymus pateikti informaciją[47]. Negana to, valstybių narių teisėsaugos institucijos ir FŽP turėtų galėti atsakyti į Europolo (ES

[41] Teresa Quintel, „Data protection rules applicable to Financial Intelligence Units: still no clarity in sight“, *ERA Forum*, 23, 1 (2022): 53, https://doi.org/10.1007/s12027-021-00697-z
[42] *ibid.,* 58.
[43] Europos Parlamento ir Tarybos direktyva (ES) 2018/843, 2018 m. gegužės 30d., „kuria iš dalies keičiama Direktyva (ES) 2015/849 Dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičiamos Direktyvos 2009/138/EB ir 2013/36/ES“, 32 str. 9d., EUR-LEX, žiūrėta 2023-01-26, https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32018L0843
[44] Europos Parlamento ir Tarybos Direktyva (ES) 2015/849, *supra note*, 31: 52 str.
[45] Mouzakiti, *supra note*, 19: 360.
[46] Europos Parlamento ir Tarybos Direktyva (ES) 2015/849, *op. cit*., 32 str. 4d.
[47] Europos Parlamento ir Tarybos Direktyva (ES) 2019/1153, *supra note,* 40: 7 str. 1d.

teisėsaugos bendradarbiavimo agentūra) prašymus, pateikti banko sąskaitų informaciją, arba atlikti analizę[48]. Norint gauti informaciją iš teisėsaugos institucijų, FŽP turi naudotis tradiciniais teisinės pagalbos kanalais arba kreiptis į FŽP kitoje jurisdikcijoje, kad jis savo ruožtu surinktų informaciją iš teisėsaugos institucijų. Visgi, kitoje jurisdikcijoje veikiantis FŽP ar teisėsaugos institucija, gavus informacijos prašymą, turi teisę reikalauti Susitarimo Memorandumo, ar oficialios tarpusavio pagalbos užklausos[49]. Prieiga gali būti nesuteikta, arba apribotas tolesnis informacijos naudojimas. Ypač, kai to reikalauja administracinio arba hibridinio tipo FŽP, iš teisėsaugos tipo FŽP, nes pastarasis laiko informaciją, kurioje, dažnu atveju, nebeįmanoma atskirti ribų, tarp STR analizės ir nusikaltimo tyrimo[50].

Nors po 5-osios Pinigų plovimo prevencijos Direktyvos priėmimo FŽP galėtų surinkti daugiau teisėsaugai reikalingos informacijos, matoma, kad informacijos perdavimas yra sudėtingas; galimi uždelsimai. Todėl, įprastai praktikoje, informacijos perdavimas apsiriboja STR analizės duomenimis[51]. Teisėsaugos institucijos, neturėdamos visos informacijos apie sąskaitos savininką ir jo vykdomas operacijas, papildomai kreipiasi į finansų įstaigas, išsiunčiant taip vadinamas „bendrąsias užklausas“ (*angl. blanket requests*)[52] . Vertinat iš teisės į privatumą ir asmens duomenų apsaugą perspektyvos, „bendrų užklausų“ praktika yra problematiška, nes nepatvirtintais įtarimais pagrįstos užklausos, gali lemti netikslingą asmens priskyrimą aukštesnei rizikos kategorijai[53], finansų įstaigoje.

1.3 Pokyčiai reikalingi keičiantis informacija kovoje su finansiniais nusikaltimais

1.3.1 Kovos su finansiniais nusikaltimais trūkumai

Nepaisant tris dešimtmečius dedamų pastangų, dabartinė kovos su finansiniais nusikaltimais sistema nėra pakankamai efektyvi, ir sulaukia kritikos dėl abejotino poveikio, mažinant finansinių nusikaltimų mąstą. „Nors kovai su finansiniais nusikaltimais taikomų

[48] „Using financial information for preventing, detecting, investigating and prosecuting criminal offences“, Summaries of EU Legislation, https://eur-lex.europa.eu/EN/legal-content/summary/using-financial-information-for-preventing-detecting-investigating-and-prosecuting-criminal-offences.html
[49] Pavlidis, *supra note,* 14: 373.
[50] *Ibid.,* 372.
[51] *Ibid.,* 373.
[52] *Ibid.*
[53] Europos Komisija, *Accompanying the document Proposal for a Directive of the European Parliament and of the Council on laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA*, Commission staff working document, (Strasbūras, 2018), 7, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0114

priemonių ratas labai išsiplėtė, gaunama nauda ribota[54]“. Tarptautinių atsiskaitymų banko pateiktoje, apibendrintoje 2023m. statistikoje, nurodoma, kad per vienerius metus pasaulyje „išplaunamų“ pinigų vertė sudaro 2–5% pasaulio BVP, arba nuo 2 trilijonų iki 5 trilijonų dolerių. Kasmet konfiskuojama mažiau nei 1 proc. šios sumos, arba nuo 20 iki 50 milijardų dolerių. Tai pat, kova su finansiniais nusikaltimais, vien finansų įstaigoms, neminint FŽP ir teisėsaugos institucijoms skiriamo finansavimo iš valstybės biudžeto, globaliu mastu, kainuoja vidutiniškai 274 milijardus dolerio, o išlaidos auga kasmet [55]. Už netinkamą finansinių nusikaltimų prevencijos įgyvendinimą, finansų įstaigoms, gresia didelės baudos. Todėl finansų įstaigos yra linkusios, verčiau daryti daugiau, nei daryti mažiau. Dėl tokios gynybinės finansų įstaigų pozicijos, FŽP kasdien pasiekia tūkstančiai STR, kurių dalis gali būti ne itin pagrįsti. Dažnu atveju, FŽP neturi pakankamai resursų atrinkti svarbius pranešimus, kurie vestų į ikiteisminio tyrimo pradėjimą. Europos bankų federacijos (toliau EBF) pateiktoje konsoliduotoje statistikoje, nurodoma, kad per metus FŽP gauna milijonus STR iš finansų įstaigų. Ikiteisminiai tyrimai yra pradedami tik dėl mažiau nei 1 % iš šių STR[56].

Susiklosčius tokiai situacijai, politikų ir visuomenės tarpe kyla diskusijų, ar kovai su finansiniais nusikaltimais skirti resursai neturėtų būti panaudojami kitaip[57]. Bet esamos sistemos kritikavimas, be tinkamų priemonių pasiūlymo, niekaip nesprendžia problemos. Pažymint, kad „ nusikaltėliai prisitaiko greičiau nei įstatymo leidėjas“[58], EBF kviečia kritiškai peržiūrėti kovos su finansiniais nusikaltimais reguliavimą[59]. Norint pasiekti pageidaujamų rezultatų, reikia suprasti, kodėl kova su finansiniais nusikaltimas nėra efektyvi, ir kaip ją būtų galima pagerinti. Dabartinė situacija taikliai apibūdinama kaip „pasaulis, kuriame pinigai lengvai juda tarp valstybių vieno mygtuko paspaudimu, bet informacija apie pinigų judėjimą – ne”[60]. Pavienės valstybių pastangos neduoda norimų rezultatų kovoje su finansiniais nusikaltimais, nes nusikaltėliai nepaiso valstybių sienų[61]. Vykdyti nusikaltimams išnaudojama ne viena finansų įstaiga, įsisteigusi ne vienoje jurisdikcijoje. Susiklosčius tokiai situacijai, informacijos mainai tarp kovą su finansiniais nusikaltimais vykdančių tampa kritiškai svarbūs[62]. Vis dėl to, tyrimai vyksta fragmentuotai: nei

[54] Centre for European Policy Studies (CEPS), Anti-money laundering in the EU time to get serious, (Briuselis, 2021), 6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805607
[55] Bank for International Settlements (BIS), Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders, (2023), 10, https://www.bis.org/publ/othp66.htm
[56] European Banking Federation, Lifting the spell of dirty money: blueprint for an effective EU framework to fight money laundering, (2020), 6, https://www.ebf.eu/wp-content/uploads/2020/03/EBF-Blueprint-for-an-effective-EU-framework-to-fight-money-laundering-Lifting-the-Spell-of-Dirty-Money-.pdf
[57] Kaiser, *supra note,* 10: 101
[58] European Banking Federation, *op. cit.,* 4.
[59] *Ibid*., 5.
[60] Mouzakiti, *supra note*, 19: 352.
[61] Financial Action Task Force (FATF), *supra* note, 6: 15.
[62] Financial Action Task Force (FATF), *supra note*, 6: 15.

finansų įstaigos, nei FŽP, nei teisėsauga neturi plataus, visapusio finansinių nusikaltimų schemų vaizdo, kuris gali būti sudėliojamas tik turint prieigą, prie kitų subjektų surinktos informacijos. Vienas iš būdų kaip pagerinti sistemos veikimą, yra pokyčiai įgalinantys informacijos mainus, tarp kovą su finansiniais nusikaltimais įgyvendinančių subjektų. Pirma, sukuriant teisinę bazę, leidžiančią dalintis informacija finansų įstaigoms tarpusavyje (angl. *private-private partnership*). Antra, stiprinant privataus ir valstybinio sektoriaus bendradarbiavimą (angl. *public-private partnership*).

1.3.2 Poreikis keistis informacija tarp finansų įstaigų

Norint veiksmingai nustatyti ir kovoti su įtartina veikla, vykdoma už atskirų finansinių institucijų ir nacionalinių sienų ribų, būtinas holistinis požiūris į finansinių operacijų duomenis[63]. Kaip ir minėta 1.2.1 skyrelyje, ES teisėje, neįtvirtinta galimybė finansų įstaigoms tarpusavyje dalintis informacija apie klientus ir jų vykdomas operacijas. Nors finansų įstaigos yra „vartų saugotojos“, jų matomas finansinių operacijų vaizdas – izoliuotas. Finansų įstaigos neturi teisės įspėti viena kitą apie galimai įtartiną veiklą, susijusią su jų klientais. Finansų įstaiga, priskirdama klientą rizikos kategorijai, remiasi tik savo pačios supratimu ir ribotai surinkta informacija. Nusikaltėliai išnaudoja šį trūkumą, vykdydami operacijas per subjektų, turinčių sąskaitas skirtingose finansų įstaigose, tinklą. Atskira finansų įstaiga nemato pakankamai informacijos, kad galėtų laiku aptikti ir nutraukti neteisėtas operacijas[64]. Nusikalstama veika galėtų būti aptinkama, jei finansų įstaiga gautų informaciją iš kitų finansų įstaigų.

1.3.3 Poreikis keistis informacija tarp finansų įstaigų ir teisėsaugos

Privataus ir valstybinio sektoriaus bendradarbiavimas susideda iš dalijimosi strategine ir taktine informacija tarp finansų įstaigų, FŽP ir teisėsaugos institucijų. Strateginė informacija apima dalijimąsi žiniomis apie finansinių nusikaltimų tipologijas, tendencijas, atsirandančias naujas rizikas, atsiliepimų po STR perdavimo teikimą finansų įstaigoms. Privataus ir valstybinio sektoriaus bendradarbiavimo pavyzdys strateginės informacijos mainams yra Pinigų plovimo kompetencijų centras Lietuvoje. Toliau keitimasis strategine informacija magistro baigiamajame darbe nenagrinėjamas, nes tokie informacijos mainai neapima konfidencialios informacijos apie

[63] Bank for International Settlements (BIS), *supra note,* 55: 13.
[64] Future of Financial Intelligence Sharing (FFIS) research program, *supra note* 8: 14.

konkrečius atvejus, asmenis, ar sandorius perdavimo. Dalinimasis strategine informacija neturi sąryšio su teise į privatumą ir asmens duomenų apsaugą.

Nei FŽP, nei teisėsauga neturi „gyvo“ finansinių operacijų vaizdo ir atlieka analizę tik pagal tam tikrą finansinės elgsenos segmentą, matomą iš STR[65]. Nepaisant to, kad FŽP iš finansų įstaigų, per užpildomus STR, gauna didžiulį informacijos srautą, STR yra tik formalus pranešimas iš vienos finansų įstaigos, kuriuo remiantis atlikta analizė perduodama teisėsaugos institucijoms. Galimybė dalintis taktine informacija su finansų institucijomis, gali būti matoma kaip būdas ištaisyti esamus trūkumus**.** Dalintis taktine informacija reiškia konkretaus asmens duomenų perdavimą iš FŽP ir teisėsaugos institucijų privačiam sektoriui, siekiant paskatinti dominančio asmens finansinio elgesio stebėseną, arba tikslingą paiešką finansinių operacijų įrašuose. Finansų įstaigos, gavusios tokią informaciją, suvokia prioritetines grėsmes ir gali iš anksto reaguoti į įtartinus požymius, atliekant deramą kliento patikrinimą, ar transakcijų stebėseną. Iš FŽP ir teisėsaugos institucijų perspektyvos, dalinimasis tokia informacija „gali padėti atlikti veiksmingesnius tyrimus ir pritaikyti tinkamus teisėsaugos veiksmus, kurie teigimai paveiktų visą tolesnį procesą, įskaitant kaltininkų patraukimą baudžiamojon atsakomybėn ir nuteisimą, bei neteisėtai įgyto turto konfiskavimą“[66]. Vis dėl to, keitimasis taktine informacija reikalauja keistis asmens duomenimis tarp valstybinio ir privataus sektoriaus, dėl to kyla klausimų, kaip turėtų būti įgyvendinami iš teisės į privatumą ir asmens duomenų apsaugą užtikrinimo kylantys reikalavimai.

1.3.4 Siūlomi teisės aktų pakeitimai

„Norint nugalėti tinklą, reikia sukurti tinklą“[67]. Atliekant jungtinę analizę ir dalinantis informacija siekiama pamatyti platesnį dėlionės vaizdą, giliau suprasti ir turėti geresnę prieigą identifikuojant su finansinių nusikaltimų vykdymu susijusias finansines operacijas, siekiant, kad kuo daugiau finansinių nusikaltimų vykdymo atvejų pasibaigtų veiksmingais tyrimais. ES įstatymo leidėjui uždelsus šiuo klausimu, atskirose valstybėse narėse, finansų įstaigos, FŽP ir teisėsaugos institucijos savo iniciatyva jungia jėgas kovai su finansiniais nusikaltimais ir rengia tam reikalingą įstatymų bazę nacionalinės teisės sistemoje. Svarbu paminėti, kad lygiai taip pat ir Lietuvoje, 2024m. priimti įstatymo pakeitimai, leidžiantys finansų įstaigoms keistis informacija tarpusavyje (žr. 3.1.3)

Reaguodama į susiklosčiusią situaciją, 2021m. Europos Komisija pasiūlė teisės aktų paketą, kuriuo siekiama sustiprinti ES kovos su pinigų plovimu ir kovos su terorizmo finansavimu

[65] Future of Financial Intelligence Sharing (FFIS) research program, *supra note* 8: 20.
[66] Europos Komisija, *supra note* 7:19.
[67] Bank for International Settlements (BIS), *supra note,* 55: 14.

taisykles. Pasiūlymas įtraukia Reglamentą dėl finansų sistemos naudojimo pinigų plovimui ar terorizmo finansavimui prevencijos ir Direktyvą dėl mechanizmų, kuriuos turi įdiegti valstybės narės finansų sistemos naudojimo pinigų plovimui ar terorizmo finansavimui prevencijos tikslais[68] (6-oji Pinigų plovimo prevencijos Direktyva). Siūlomame Reglamente ir Direktyvoje, numatomi platūs įgaliojimai dalintis informacija tarp kovą su finansiniais nusikaltimais vykdančių subjektų, kurie reikšmingai paveiktų visą dalinimosi informacija reguliacinę aplinką.

6-os Direktyvos 18 str. numatoma, kad FŽP turi būti suteikta tiesioginė ar netiesioginė prieiga prie teisėsaugos informacijos.

Siūlomo Reglamento, perduotoje svarstyti Europos Tarybai versijoje[69], finansų įstaigoms, ir valstybės institucijoms bendradarbiaujančioms kovoje su finansiniais nusikaltimais *(*angl. *private-private partnerships ir public-private partnerships*) siūloma leisti:

1) dalintis informacija, nukrypstant nuo draudimo atskleisti informaciją nuostatų (54 3a str.);
2) dalintis deramo kliento patikrinimo metu surinkta informacija finansų įstaigoms tarpusavyje (55 str. 5p.);
3) dalintis deramo kliento patikrinimo metu surinkta informacija finansų įstaigoms su kompetentingomis valstybės institucijomis (55 str. 7p.).

Siūlomame Reglamente, kartu su teise dalintis informacija, įtvirtinamos ir sąlygos kada leidžiami informacijos mainai: duomenys, kuriais dalinamasi turi kelti įtarimų, finansų įstaigos klientai turi būti informuoti, kad jų duomenimis gali būti dalinamasi, turi būti dalinamasi tik tvarkingais ir atnaujintais asmens duomenimis, o tam naudojami saugūs perdavimo kanalai. Valstybės duomenų apsaugos pareigūnams turi būti suteikta prieiga prie tokių dalinimosi duomenimis platformų. Bet visos šios duomenų apsaugos priemonės labiau veikia techniniame lygmenyje, neatsakant į pagrindinį klausimą, ar toks dalijimasis duomenimis ir esmės nepažeidžia teisės į privatumą ir asmens duomenų apsaugą. Todėl, sekančioje dalyje supažindinama su teise į privatumą ir asmens duomenų apsaugą, analizuojama kokie reikalavimai taikomi asmens duomenis finansinių nusikaltimų prevencijos tikslais tvarkymui, ką apie tai sako Europos Duomenų Apsaugos Valdyba (*angl. European Data Protection Board,* toliau EDPB), ir kokia galima teismų pozicija.

Apibendrinat, finansų įstaigose atliekamų finansinių operacijų įrašai yra svarbiausias finansinių nusikaltimų tyrimo šaltinis, todėl finansų įstaigoms patikėtas ypatingas vaidmuo kovoje

[68]Pasiūlymas, Europos Parlamento ir Tarybos Direktyva, 2021 m. liepos 20d., „Dėl mechanizmų, kuriuos turi įdiegti valstybės narės finansų sistemos naudojimo pinigų plovimui ar terorizmo finansavimui prevencijos tikslais, kuria panaikinama Direktyva (ES) 2015/84, EUR-LEX, žiūrėta 2024-01-26, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52021PC0423

[69] Pasiūlymas, Europos Parlamento ir Tarybos Reglamentas 2021 m. liepos 20d., „Dėl finansų sistemos naudojimo pinigų plovimui ar terorizmo finansavimui prevencijos“, Tarpinstitucinė versija Tarybos svarstymui, 15517/22, 2022m. gruodžio 5d., https://data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf

su finansiniais nusikaltimais. Kartu su finansų įstaigomis, kovą su finansiniais nusikaltimais vykdo specialiai tam įsteigti finansinės žvalgybos padaliniai ir teisėsaugos institucijos. Kilus įtarimams finansiniu nusikaltimu, finansų įstaigos perduoda STR FŽP, kurie savo ruožtu atlieka analizę ir perduoda informaciją teisėsaugos institucijoms tolimesnio tyrimo vykdymui. Finansų įstaigos tarpusavyje nesikeičia informacija apie klientus ir kilusius įtarimus. Informacijos mainai tarp FŽP ir FŽP ar teisėsaugos institucijų, veikiančių skirtingose jurisdikcijose yra komplikuoti dėl skirtingo FŽP statuso valstybėse narėse. Teisėsaugos institucijos tai pat neturi tiesioginės prieigos prie visų įtariamojo sąskaitų, visose finansų įstaigose. Dėl šių priežasčių, nei finansų įstaigos, nei FŽP neturi plataus, visapusio vaizdo ir negali aptikti finansinių nusikaltimų, vykdomų pasitelkiant platų finansinių įstaigų tinklą. Kylant abejonėms, dėl dabartinio reguliavimo efektyvumo kovoje su finansiniais nusikaltimais, siekiama sukurti bendradarbiavimo modelius, kurie leistų finansų įstaigoms keistis informacija tarpusavyje, ir FŽP bei teisėsaugos institucijoms surinkti informaciją iš finansų įstaigų savo pačių iniciatyva, net jei neužpildomas STR. Įgyvendinus bendradarbiavimo modelius, kovą su finansiniais nusikaltimais vykdantiems subjektams būtų suteikiami platūs įgaliojimai dalintis asmens duomenimis, todėl turi būti apsvarstoma kokį poveikį teisei į privatumą ir asmens duomenų apsaugą turėtų šie pokyčiai.

2. TEISĖ Į PRIVATUMĄ IR ASMENS DUOMENŲ APSAUGĄ

Tradiciškai, kliento privatumo apsauga laikoma didele vertybe finansų sektoriuje, o Banko paslapties įsipareigojimas - pagrindinis banko ir kliento santykių įsipareigojimas, užtikrinantis finansinės informacijos konfidencialumą[70]. Kita vertus, 2003 m. paskelbus FATF rekomendacijas, valstybėms numatyta pareiga užtikrinti, kad Banko paslapties nuostatos neturėtų trukdyti FATF rekomendacijų įgyvendinimui[71]. Taigi, finansų įstaigoms nustatytas įpareigojimas vykdyti finansinių nusikaltimų prevenciją, sugriovė tradicines finansinės informacijos konfidencialumo prielaidas. Dėl to, įstatymo leidėjui ir finansų įstaigoms teko sunkus uždavinys, susijęs su dviejų interesų – asmens teisės į privatumą bei visuomenės kolektyvinio intereso – konkurencija[72]. Poreikis užtikrinti, kad finansų sistemoje necirkuliuotų nusikalstamu būdų įgytos lėšos ir poreikis užtikrinti asmens teisę į privatumą, neturėtų būti suvokiamas kaip būtinybė, pasirinkti tarp vieno ir kito intereso. „Šie tikslai nėra vienas kitą paneigiantys ar prieštaraujantys, o vienas kitą papildantys[73]“, ir gali veikti kartu demokratinėje visuomenėje. Tinkamo balanso suradimas tarp kovos su finansiniais nusikaltimais ir asmens duomenų apsaugos yra ir pagrindinis uždavinys, vystant privataus ir valstybinio sektoriaus, bei privataus sektoriaus tarpusavio keitimosi informacija modelius[74]. Todėl, šioje dalyje atskleidžiama teisės į privatumą ir asmens duomenų apsaugą sąvoka, analizuojama kokį balansą tarp kovos su finansiniais nusikaltimais ir asmens duomenų apsaugos reikalauja užtikrinti pirminiai ir antriniai teisės šaltiniai, kokios nuostatos sukurtos teismų precedentais ir privalomos teisinės galios neturinčiais teisės šaltinais (toliau įvardijamais *soft law* terminu).

2.1 Teisės į privatumą ir asmens duomenų apsaugą sąvoka ir raida

Teisė į privatumą, arba teisė į privataus gyvenimo apsaugą yra pamatinė žmogaus teisė. Nėra priimta universalios sąvokos šiai teisei apibrėžti, bet teisės esmė gali būti apibūdinama kaip „minties laisvė, savo kūno valdymas, vienatvė namuose, asmeninės informacijos kontrolė, laisvė

[70] Kaiser, *supra note,* 10: 430.
[71] Financial Action Task Force (FATF), *FATF 40 Recommendations*, (2003), 4p., https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202003
[72] Markevičius, *supra note,* 15: 189-190.
[73] Financial Action Task Force (FATF), *supra note*, 6: 3.
[74] Bank for International Settlements (BIS), *supra note,* 55: 22.

nuo stebėjimo, savo reputacijos apsauga ir apsauga nuo kratų ir tardymų“[75] . Arba „ne daugiau, bet ir nemažiau negu, asmens laisvė pačiam pasirinkti laiką, aplinkybes, o svarbiausią apimtį, kuria jo įsitikinimais, tikėjimu, elgesiu ir nuomone būtų galima dalintis, ar atskleisti kitiems“[76].

Moderni teisės į privatumą koncepcija apima ir apsaugą nuo valstybės kišimosi į asmenų privatų gyvenimą. Tai pat, iš teisė į privatumą apibrėžimo išplaukia ir asmens teisė kontroliuoti, kas gali matyti jo asmeninę informaciją. Šioje vietoje teisė į privatumą persidengia su teise į asmens duomenų apsaugą. E. Markevičiaus nuomone, „nors asmens duomenų apsaugos teisinis reguliavimas ir gali turėti kitų tikslų […], tačiau asmens duomenų apsaugos taisyklių taikymo pamatinis tikslas, visuomet yra asmens teisės į privatumą apsauga […], pažeidžiant asmens teisę į duomenų apsaugą, tuo pačiu pažeidžiama ir jo teisė į privatų gyvenimą, tačiau ne atvirkščiai”. Magistro baigiamajame darbe ir toliau bus laikomasi šios nuomonės, ir sąvokos teisė į privatumą ir teisė į asmens duomenų apsaugą vartojamos lygiagrečiai, kaip papildančios viena kitą.

Teisė į privatumą kildinama iš tokių ankstyvų principų kaip ryšių, susirašinėjimo ir laiškų slaptumas, kurie daugelyje valstybių pradėti saugoti apytikriai nuo XVII a[77]. Nors teisės į privatumą konceptas randamas daugelio jurisdikcijų teisės doktrinos pirmtakuose ir vystėsi veikiamas tarptautinių gairių, direktyvų, projektų, bet per laiką, reikalavimai skirtingose valstybėse išsivystė skirtingai, atspindint jų istorinę ir kultūrinę patirtį, skirtingas teisės sistemas ir skirtingai taikomas teisės normas[78]. Vienose valstybėse ši teisė yra įtvirtinta konstitucijoje (pavyzdžiui, 2009 m. ratifikavus Lisabonos sutartį, Europos Sąjungoje teisė į privatumą tapo pamatine teise), kitose valstybės privataus gyvenimo apsaugos principas atskleidžiamas teismų doktrinoje, (JAV, Jungtinė Karalystė). Tai pat, yra ir valstybių, kurių teisėje aiškiai nenumatyta privataus gyvenimo apsauga. Šioje vietoje svarbu pažymėti, kad privatumo apsaugos skirtumai tarp valstybių labai apsunkina arba padaro neįmanomą tarptautinį keitimąsi informacija, nes informacija turėtų būti perduodama tik tokiai valstybei, kuri taiko aukštesnį arba vienodą asmens duomenų apsaugos lygį, kaip ir perduodančioji valstybė[79].

Šių dienų konceptą atitinkanti teisės į privatumą ir asmens duomenų apsaugą sąvoka tarptautinėje teisėje įtvirtinta Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 str., (toliau Konvencija), o Europos Sąjungos pirminiuose teisės šaltiniuose – Europos Sąjungos Pagrindinių teisių Chartijos 7 ir 8 str., (toliau Chartija). Antriniuose Europos Sąjungos teisės

[75]Daniel J. Solove, *Understanding Privacy*, Harvard University Press, (2009), 2 cituota iš Birutė Pranevičienė, „Limiting of the right to privacy in the context of protection of national security“, JURISPRUDENCIJA 18, 4 (2011):1613, https://ojs.mruni.eu/ojs/jurisprudence/article/view/96/90

[76]Oscar M. Ruebhausen, Orville. M.; Brim, „Privacy and Behavioral Research“, *Columbia Law Review*, 65 (1965): 1184 cituota iš *ibid*.

[77] Diggelmann, Oliver, Cleis N. Maria, How the Right to Privacy Became a Human Right (2014), 442 cituota iš Kaiser, *supra note,* 10: 210.

[78] Financial Action Task Force (FATF), *supra note*, 6: 7.

[79] Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679, *supra note,* 38: 63 konstatuojama dalis.

šaltiniuose, teisę į privatumą ir asmens duomenų apsaugą reglamentuoja, 2016 m. iki tol galiojusią Direktyvą 95/46/EB pakeitęs, BDAR, vadinamas griežčiausiu teisės į privatumą ir asmens duomenų apsaugą įstatymų rinkiniu pasaulyje[80], ir 2019 m. Tarybos pamatinį sprendimą – 2008/977/TVR pakeitusi LED Direktyva.

2.2 Teisė į privatumą ir asmens duomenų apsaugą pirminiuose teisės šaltiniuose

Nors ir konstitucinio pobūdžio, teisė į privatumą ir asmens duomenų apsaugą nėra absoliuti, ir gali būti suvaržyta (bet nepažeista) tam tikra apimti, esant įstatyme numatytoms sąlygoms. Teisės į privatumą ir asmens duomenų apsaugą suvaržymas laikomas teisėtu, kai kumuliatyviai tenkinamos Chartijoje nustatytos sąlygos: „bet koks šios Chartijos pripažintų teisių ir laisvių įgyvendinimo apribojimas turi būti numatytas įstatymo ir nekeisti šių teisių ir laisvių esmės. Remiantis proporcingumo principu, apribojimai galimi tik tuo atveju, kai jie būtini ir tikrai atitinka Sąjungos pripažintus bendrus interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti“[81]. Konvencijos formuluotė yra labai panaši – „numatytomis sąlygomis Valstybės institucijos neturi teisės apriboti naudojimosi šiomis teisėmis, išskyrus įstatymų nustatytus atvejus ir, kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės saugos ar šalies ekonominės gerovės interesams, siekiant užkirsti kelią viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti“[82].

Iš Chartijos teksto išskiriami 5 kriterijai[83], kuriuos turi atitikti teisėtas teisės į privatumą ir asmens duomenų apsaugą apribojimas:

1) priemonės, suvaržančios Chartijos saugomų pamatinių teisių įgyvendinimą turi būti aiškiai ir tiksliai apibrėžtos ir įtvirtintos įstatymais, tam kad asmenys, kurių teisės ribojamos, turėtų galimybę susipažinti ir numatyti galimas pasekmes. Europos Žmogaus Teisių Teismas (toliau EŽTT), aiškindamas Konvencijoje įtvirtintą teisių apribojimo numatant įstatymais sąlygą, pažymi, kad pirmiausia reikalaujama jog numatyta priemonė turėtų pagrindą vidaus teisėje. Antra, kad ši nacionalinė teisė turi būti prieinama atitinkamam asmeniui. Trečia atitinkam asmeniui turi būti suteikta galimybė numatyti nacionalinėje teisėje įtvirtintos

[80] Ben, Wolford, *What is GDPR, the EU's new data protection law?*, GDPR EU, žiūrėta 2024-01-26. https://gdpr.eu/what-is-gdpr/

[81] „Europos Sąjungos pagrindinių teisių Chartija“, 2000m. publikuota 2012-10-26, 52 str., EUR-LEX, žiūrėta 2024-01-26, https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:12012P/TXT

[82] European Convention on Human Rights, 1950, Last reviewed on 24/03/2017, 8 str,., EUR-LEX, žiūrėta 2024-01-26, https://www.echr.coe.int/documents/d/echr/convention_ENG

[83] European Data Protection Supervisor, „Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data”, 2019 m. gruodžio 19d., 6-8, https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf

priemonės pasekmes jam. Ir ketvirta – bet kokia nacionalinėje teisėje įtvirtinta priemonė turi būti suderinama su teisinės valstybės principu[84]. Analogiškai toks išaiškinimas pritaikomas ir Chartijos nuostatoms;

2) suvaržymu nekeičiama teisių ir laisvių esmė. Tai reiškia, kad negalima nustatyti tokių suvaržymų, dėl kurių teisė netektų savo turinio ir asmuo nebegalėtų ja pasinaudoti. Ši sąlyga nerandama Konvencijoje ir buvo išplėtota būtent Europos Sąjungos Teisingumo Teismo (toliau ESTT) praktikoje, tačiau pati teisių ir laisvių esmės sąvoka plačiai neatskleista ESTT jurisprudencijoje. Daugiau dėl teisių ir laisvių esmės pasisakė Vokietijos Konstitucinis Teismas, reikalaudamas, kad įstatymų leidėjas saugotų visuomenės privatumą, ne tik įvertinant atskirų priemonių teisėtumą, bet visą teisinę aplinką tos pačios priemonės vykdymo atžvilgiu[85];

3) teisėkūros priemonė yra tinkama, kai tikrai atitinka Sąjungos svarbius bendruosius interesus, arba yra būtina kitų teisėms ir laisvėms apsaugoti. Kovos su finansiniais nusikaltimais, kaip Sąjungos bendrojo viešojo intereso, klausimas neanalizuojamas plačiau šio magistro baigiamojo darbo apimtyje ir laikomasi nuomonės, kad kova su finansiniais nusikaltimais neabejotinai yra svarbus Sąjungos bendrasis interesas. Kaip ir nurodo FATF – „pinigų plovimo ir teroristų finansavimo prevencija tarnauja svarbiems nacionalinio saugumo ir viešojo intereso tikslams [...][86], ir BDAR įžanginė dalis „ [...] visos valstybės narės pripažįsta, kad kova su pinigų plovimu ir teroristų finansavimu yra svarbus viešasis interesas [...]“[87];

4) priemonė yra tikrai būtina ir mažiausiai suvaržanti, kai teisėtam tikslui pasiekti galima rinktis iš kelių tinkamų priemonių;

5) priemonė yra proporcinga ir ja nustatomas teisingas balansas tarp konkuruojančių teisių, kartu taikant ir atitinkamas apsaugos priemones.

4 ir 5 kriterijai yra artimai susiję vienas su kitu, nes būtinumas yra išankstinė proporcingumo sąlyga. Jei teisėkūros priemonė neatitinka būtinumo kriterijaus, proporcingumas nebevertinamas. Būtinumo kriterijus reiškia, kad turi būti vertinamas priemonės tinkamumas tikslui, kurio ja siekiama, ir tokia priemonė turi būti mažiausiai suvaržanti iš visų galimų pasirinkimų pasiekti tam pačiam tikslui. Tik, kai priemonė tenkina visus 4 aukščiau išvardintus kriterijus gali būti atliekamas jos proporcingumo vertinimas. Proporcingumo testas įprastai apima įvertinimą, kokios pamatinės teisės apsaugos priemonės turėtų būti nustatomos kartu su teisę

[84] Europos Žmogaus Teisių Teismas, „Case of Heino v. Finland“, 56720/09, 2011 m. vasario 15 d., 36, HUDOC, žiūrėta 2024-01-26, https://hudoc.echr.coe.int/eng?i=001-103394
[85] BVerfG, 1 BvR 256/08 (2010) cituota iš Kaiser, *supra note,* 10: 424.
[86] Financial Action Task Force (FATF), *Private sector information sharing*, (Paris, 2017), 4, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf
[87] Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679, *supra note*, 38: 42 konstatuojamoji dalis.

suvaržančia priemone, siekiant sumažinti riziką, kylančią pamatinės teisės apsaugai iki „priimtino“ proporcingo lygio. LR Konstitucinio teismo doktrinoje proporcingumo principas „ reiškia, kad teisės aktuose numatytos priemonės turi atitikti teisėtus ir visuomenei svarbius tikslus, kad šios priemonės turi būti būtinos minėtiems tikslams pasiekti ir neturi varžyti asmens teisių ir laisvių akivaizdžiai labiau, negu reikia šiems tikslams pasiekti[88]“.

2.3 Teisė į privatumą ir asmens duomenų apsaugą antriniuose teisės šaltiniuose

4-os Pinigų plovimo prevencijos Direktyvos 41 str. 1d. nustato, kad duomenų tvarkymui kovoje su finansiniais nusikaltimais, finansų įstaigos turi taikyti BDAR.

2.3.1 Finansiniai duomenys kaip specialių kategorijų duomenys

Kaip ir minėta 1.1 sk. įgyvendinant pinigų sekimo principą kovoje su finansiniais nusikaltimais, renkami finansinių operacijų duomenys. Pagal BDAR, tokie duomenys priskiriami specialių kategorijų asmens duomenims, nes asmens finansinių operacijų įrašai atskleidžia jautrias asmens gyvenimo detales, kaip seksualinė orientacija, sveikatos būklė, politiniai, religiniai įsitikinimai ir kt., taip leidžiant iš labai arti pažvelgti į kasdienį asmens gyvenimą ir įpročius. Piktnaudžiavimas tokiais duomenimis ir pakankamų garantijų nebuvimas gali turėti itin neigiamų pasekmių asmeniui, kurio duomenys renkami[89]. Dėl šios priežasties, specialių kategorijų asmens duomenų tvarkymas yra draudžiamas, išskyrus BDAR 9 str. 2d. įtvirtintas išimtis. Šioje vietoje BDAR artimai atkartoja Chartijos tekstą, nustatant, kad specialių kategorijų asmens duomenų tvarkymas galimas jei „tvarkyti duomenis būtina dėl svarbaus viešojo intereso priežasčių, remiantis Sąjungos arba valstybės narės teise, kurie turi būti proporcingi tikslui, kurio siekiama, nepažeisti esminių teisės į duomenų apsaugą nuostatų ir kuriuose turi būti numatytos tinkamos ir konkrečios duomenų subjekto pagrindinių teisių ir interesų apsaugos priemonės[90]“.

Analizuojant keitimosi informacija tarp finansų įstaigų ir privataus bei valstybinio sektoriaus bendradarbiavimo iniciatyvas BDAR kontekste, tikslinga suprasti, kad finansinių nusikaltimų prevencijos tikslais tvarkomi duomenys gali būti išskirti į duomenis iki įtarimų kilimo (*angl. pre-suspicion*) ir duomenis kilus įtarimams (*angl. post-suspicion*). BDAR reikalavimai taikomų duomenų iki įtarimų kilimo tvarkymui, skiriasi nuo reikalavimų, taikomų duomenų kilus

[88] Lietuvos Respublikos Konstitucinis Teismas, „Oficialiosios Konstitucinės Doktrinos nuostatos, 2014-2016, Vilnius, 2017, žiūrėta 2024-04-28. https://lrkt.lt/data/public/uploads/2017/06/doktrinos-papildymas-2014-2016.pdf
[89] Financial Action Task Force (FATF), *supra note*, 6: 3.
[90] Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679, *supra note*, 38: 9str., 2d., g punktas.

įtarimui tvarkymo. Atskaitos tašku įtarimų kilimui laikomas STR perdavimas FŽP, nes perduodant STR pareiškiami įtarimai atskleistos tapatybės asmeniui. Nusikalstamos veiklos duomenims priskiriami ir duomenys apimantys dar nepatvirtintus įtarimus nusikalstama veika[91], todėl duomenys kilus įtarimams patenka į antrą BDAR numatytą specialių duomenų kategoriją – asmens duomenys apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas (BDAR 10 str.). Vadovaujantis BDAR 10 str., „tokie duomenys gali būti tvarkomi „tik prižiūrint valdžios institucijai arba kai duomenų tvarkymas leidžiamas Sąjungos arba valstybės narės teise, kurioje nustatytos tinkamos duomenų subjektų teisių ir laisvių apsaugos priemonės“[92].

2.3.2 BDAR principai kovoje su finansiniais nusikaltimais

Finansų įstaiga, privalo asmens duomenis, finansinių nusikaltimų prevencijos tikslais, tvarkyti tokiu būdu, kad nebūtų pažeidžiami BDAR 5 str. įtvirtinti principai ir iš jų kylančios duomenų subjektų teisės. Mokslinėje literatūroje kyla diskusijų, dėl kovos su finansiniais nusikaltimais teisinio reguliavimo atitikties tikslo apribojimo ir duomenų kiekio mažinimo principams.

Tikslo ribojimo principas „yra pagrindinis duomenų apsaugos principas, sukurtas siekiant nustatyti nurodytu tikslu surinktų asmens duomenų tvarkymo ir tolesnio jų naudojimo kitais tikslais ribas. „[...] Surinkus duomenis, jų negalima toliau tvarkyti su šiais tikslais nesuderinamu būdu“[93]. Išreiškiamas susirūpinimas, kad tikslo ribojimo principas gali būti pažeidžiamas įgyvendinant privataus ir valstybinio sektoriaus bendradarbiavimo per duomenų apsikeitimo platformas modelį[94]. Pavyzdžiui, jei prie platformos prisijungusios finansų įstaigos pasidalintų iš teisėsaugos gauta informacija finansų įstaigos grupės duomenų bazėse, siekdamos vėliau panaudoti šią informaciją kliento rizikos nustatymui. Kai asmenys negali numatyti, kokiu tikslu bus naudojami apie juos surinkti duomenys, pažeidžiamas pirmasis Chartijoje numatytas kriterijus. Šiuo atveju, „teisėsauga neturėtų būti laikoma nurodytu, aiškiu ir teisėtu tikslu“[95]. Finansų įstaigų ir teisėsaugos bendradarbiavimui būtinos teisinės priemonės, užtikrinančios, kad

[91] *What is criminal offence data?* Information Commissioner's Office, žiūrėta 2024-01-25. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/criminal-offence-data/what-is-criminal-offence-data
[92] Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679, *supra note*, 38: 10 str.
[93] Article 29 Data protection Working Party, „Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data“, 2015 m. gruodžio 1d., 6, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf
[94] European Data Protection Supervisor, „Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing“, 2020 m. liepos 23d, 46p., https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf
[95] Article 29 Data protection Working Party, *op. cit.*, 6.

duomenys renkami komerciniais tikslais, vėliau nebūtų naudojami teisėsaugos tikslais ir atvirkščiai. Pagal iki BDAR galiojusios Direktyvos 95/46/EC 29 str. įsteigta patariamoji Darbo grupė teisės į privatumą ir asmens duomenų apsaugą srityje (angl. *Article 29 Working Party*) toliau WP29) pabrėžia, kad finansų įstaigų bendradarbiavimas su teisėsaugos institucijomis kartu siekiant nustatyto tikslo turėtų būti apribotas iki to, kas tikrai būtina[96], taip mažinant duomenų kuriais apsikeičiama kiekį, o kartu ir valdant tų pačių duomenų naudojimo kitiems tikslams riziką.

Duomenų kiekio mažinimo principas teigia, kad asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi. Remdamasis šiuo principu, finansų įstaiga turi griežtai apriboti tvarkomus duomenis ir tvarkyti tik tą informaciją, kuri tiesiogiai būtina kovai su finansiniais nusikaltimais[97]. Kaip ir minėta 1.3 sk. už netinkamą finansinių nusikaltimų prevencijos įgyvendinimą, finansų įstaigoms gresia didelės baudos, todėl finansų įstaigos yra linkusios verčiau daryti daugiau, nei daryti mažiau, ir dažnu atveju vadovaujasi nuostata, kad daugiau asmens duomenų užtikriną efektyvesnę kovą su finansiniais nusikaltimais. Perteklinis duomenų rinkimas kovoje su finansiniais nusikaltimais nėra naujas reiškinys. Dar 2011m., WP29 iškėlė finansų įstaigų renkamų duomenų būtino reikalingumo klausimą[98]. Tačiau, pirmiausia, tai taikytina finansų įstaigų naudojamam kliento pažinimo procesui. Atsiribojant nuo pastarojo klausimo problematikos ir vertinat tik keitimosi duomenimis tarp finansų įstaigų tarpusavyje ir su teisėsaugos institucijoms modelius, duomenų kiekio mažinimo principo įgyvendinimas, reikalauja nustatyti tikslias duomenų kategorijas ir pateikti jas nacionalinės asmens duomenų apsaugos institucijos (angl. *Data protection authority*, toliau DPA) įvertinimui, tam, kad nebūtų pažeidžiamas proporcingumo principas, peržengiant būtinojo reikalingumo ribas.

Be aukščiau įvardintų principų, BDAR kodifikuoja ir daugybę kitų duomenų subjekto teisių išvedamų iš pagrindinių principų. Duomenimis iki įtarimų kilimo taikoma teisė į informaciją ir teisė susipažinti su asmens duomenimis (BDAR 13,14 ir 15 str.), teisė reikalauti ištaisyti duomenis (BDAR 16 str.), ir teisė „būti pamirštam“.

2.3.3 BDAR ir asmens duomenys kilus įtarimams

Svarbu, kad finansinių nusikaltimų tikslais tvarkant duomenis kilus įtarimui, nebegali būti užtikrinami BDAR 5 str. įtvirtinti principai ir iš jų kylančios duomenų subjektų teisės, nes

[96] Article 29 Data protection Working Party, *supra note*, 92: 2.
[97] European Union Agency for Fundamental Rights and Council of Europe, „Handbook on European Data Protection Law“, 2018 edition, 125, cituota iš Laurinaitis, *supra note* 16: 406.
[98] Article 29 Data protection Working Party, „Opinion 14/2011on data protection issues related to the prevention of money laundering and terrorist financing: Annex the working party on the protection of individuals with regard to the processing of personal data“, 2011 m. birželio 13d., 20, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en_annex.pdf

„įsijungia“ draudimas atskleisti informaciją (angl. *tipping off*), tam, kad nebūtų sukliudyta teisėsaugos tyrimui[99]. Tokiu atveju, finansų įstaigos remiasi BDAR 23 str., kuris numato, kad BDAR 5 str. įtvirtinti principai ir iš jų kylančios duomenų subjektų teisės gali būti apribotos, kai tokiu apribojimu gerbiama pagrindinių teisių ir laisvių esmė ir jis demokratinėje visuomenėje yra būtina ir proporcinga priemonė siekiant užtikrinti nacionalinį saugumą, nusikalstamų veikų prevenciją, tyrimą ar nustatymą (BDAR 23 str. a ir d d.). Šioje vietoje BDAR gryžta prie Chartijos teksto. Bet, jei duomenimis kilus įtarimų nebetaikoma BDAR apsauga, ar tai reiškia, kad tokie duomenys tampa saugomi tik pamatinių Chartijoje įtvirtintų principų? Šį klausimą supa teisinis neužtikrintumas. Pavyzdžiui V. Ferrari, teigia, kad duomenų tvarkymas kilus įtarimams nepatenka į vakuumą, o taikoma LED[100], nes finansų įstaiga laikoma kompetentinga institucija, kuriai pagal valstybės narės teisę pavesta vykdyti viešosios valdžios funkcijas[101]. Tačiau W. Maxwell, prieštarauja argumentuodamas, kad teoriškai finansų įstaiga gali tapti kompetentinga institucija pagal LED, bet tam reikėtų perduoti įgaliojimus veikti valstybės vardu[102]. Vykdant finansinių nusikaltimų prevenciją, finansų įstaigos tokių įgaliojimų neturi. Dar daugiau teisinio netikrumo atsiranda prisimenant, kad ne visose valstybėse narėse FŽP turi teisėsaugos institucijos statusą (1.2.2 poskyris) ir gali taikyti LED. Vadinasi, jei duomenimis kilus įtarimų, pagal BDAR 23 str. išimtį netaikoma BDAR apsauga, o LED taikymo sąlygos nėra iki galo aiškios, toliau vertinant poveikį teisei į privatumą ir asmens duomenų apsaugą keičiantis duomenimis kilus įtarimų, reikėtų vadovautis pirminio teisės šaltinio – Chartijos nuostatomis.

2.3.4 Teisėtas pagrindas tvarkyti asmens duomenis

BDAR nustato, kad asmens duomenys gali būti tvarkomi tik esant vienam iš 6 str. įtvirtintų pagrindų.

Kurį pagrindą tvarkant asmens duomenis finansinių nusikaltimų prevencijos tikslais tinkamiausia taikyti finansų įstaigoms yra diskutuotinas klausimas, nes finansinių nusikaltimų prevencija, savo pobūdžiu, dalinai atitinka 3 pagrindus.

Tvarkyti duomenis būtina:

1) kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė (BDAR 6 str., c d.)
2) siekiant atlikti užduotį, vykdomą viešojo intereso labui (BDAR 6 str., e d.)
3) siekiant teisėtų finansų įstaigos interesų – teisėtas interesas (BDAR 6 str., f d.).

[99] Europos Parlamento ir Tarybos Direktyva (ES) 2015/849, *supra note*, 31: 39 str.
[100] Ferrari, *supra note*, 11: 526.
[101] Europos Parlamento ir Tarybos direktyva (ES) 2016/680, *supra note,* 39: 3str. 7d. b p.
[102] Maxwell, *supra note*, 12: 11.

Magistro baigiamajam darbe, atsiribojama nuo tinkamiausio teisėto tvarkymo pagrindo vertinimo, ir klausimas analizuojamas tik tokia apimtimi, kiek tai reikšminga apsikeičiant duomenimis finansiniams nusikaltimams tirti. Toliau laikysime, kad tinkamiausias pagrindas finansų įstaigos tvarkyti asmens duomenis, vykdant finansinių nusikaltimų prevenciją, yra teisinė prievolė[103]. Beje, nėra esminių skirtumų ar asmens duomenys tvarkomi remiantis teisine prievole, ar viešojo intereso labui, nes abu pagrindai turi būti įtvirtinti įstatymu. Tai reiškia, kad įstatyme nustatomos aiškios ir griežtos taisyklės, atitinkančios būtinumo ir proporcingumo kriterijus. Tačiau, kai asmens duomenys tvarkomi teisėto intereso pagrindu, BDAR atsiranda takoskyra nuo teisinės prievolės, ar viešojo intereso pagrindų, ir priemonių proporcingumo ir būtinumo įvertinimo našta pereina duomenų valdytojui[104].

Dabartiniame kovos su finansiniais nusikaltimais reguliavime nekyla neaiškumų dėl teisėto duomenų tvarkymo pagrindo, tačiau įgyvendinant keitimosi informacija tarp finansų įstaigų ir su teisėsauga modelius, duomenų tvarkymo pagrindas, kuriuo įprastai remiasi finansų įstaiga rinkdama klientų duomenis ar perduodama juos teisėsaugos institucijoms, tampa nebetinkamas**.** Kai finansų įstaiga keičiasi duomenimis tarpusavyje, ar gauna duomenis iš teisėsaugos, jei toks reikalavimas nėra įtvirtintas nacionalinėje teisėje, vienintelis tinkamas pagrindas duomenų apdorojimui yra teisėtas interesas (BDAR 6 str., f d.).

WP29 paskelbtoje nuomonėje dėl teisėto intereso kaip duomenų tvarkymo pagrindo taikymo, sakoma, kad BDAR 6str. f d. taikoma „ [...] kai duomenų valdytojas [...] siekia intereso, kuris atitinka bendrąjį visuomenės interesą [..]. Tai apima tokias situacijas, kai duomenų valdytojas nevykdo konkrečių teisinių įsipareigojimų, nustatytų įstatymuose ir kituose teisės aktuose, [bet perduodamas duomenis] padeda teisėsaugai arba privačioms suinteresuotoms šalims kovoti su neteisėta veikla, pvz., pinigų plovimu“[105]. Finansų įstaigų iniciatyva keistis duomenimis tarpusavyje kyla iš savanoriškų paskaitų, todėl tvarkant asmens duomenis turėtų būti remiamasi tik teisėto intereso pagrindu. Tačiau, kaip minėta šio skyrelio pradžioje, pakeičiant duomenų tvarkymo pagrindą iš teisinės prievolės į teisėtą interesą, finansų įstaigoms kyla pareiga pačioms įvertinti keitimosi duomenimis proporcingumą ir būtinumą. Į interesų balanso derinimo pareigos perkėlimą finansų įstaigoms turėtų būti žiūrima labai kritiškai, žinant, kad naujausia teismų praktika parodo, kad ši užduotis ne visada tinkamai atliekama net įstatymų leidėjo (žr. 2.4.1). Dėl šios priežasties, valstybės narės, kuriose vystomos keitimosi duomenimis privačiame sektoriuje

[103] Maxwell, *supra note*, 12: 12-15.
[104] *Ibid.,* 14.
[105] Article 29 Data protection Working Party, „Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC“. 2014m. balandžio 9d., 28, https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf

iniciatyvos, skuba reglamentuoti informacijos mainus nacionalinės teisėje (plačiau 3-iame sk.). Tačiau, siūlomose teisės aktų pakeitimuose, kurie leistų finansų įstaigoms dalintis informacija tarpusavyje, neįtvirtinama pareiga dalintis, o tik tokia galimybė. To neužtenka, kad finansų įstaigos dalindamosi duomenimis tarpusavyje, galėtų remtis ne teisėto intereso, o teisinės pareigos pagrindu, taip pareigą vertinti nustatytų priemonių proporcingumą perduodant įstatymo leidėjui. WP29 sako, kad taikydamas teisinę prievolę, duomenų valdytojas turi neturėti pasirinkimo, ar vykdyti įstatymuose numatytą įsipareigojimą[106]. Įstatymuose numatyta teisinė prievolė, neturėtų duomenų valdytojui suteikti diskrecijos, kaip ji turėtų būti įgyvendinta. Kol kas, keitimosi informacija tarp finansų įstaigų ir su teisėsaugos institucijomis modeliai konstruojami tik savanoriškais pagrindais, tai reiškia, kad perduodamos asmens duomenis, finansų įstaigos turi įvertinti ar toks perdavimas yra būtinas ir proporcingas.

Vertinant, ar keitimosi informaciją tarp finansų įstaigų ir su teisėsauga modeliai nepažeidžia teisės į privatumą ir asmens duomenų apsaugą, neužtenka BDAR analizės, nes BDAR nukreipia į Chartijoje įtvirtintus principus. Kaip ir minėta anksčiau, Chartijoje įtvirtintos teisės gali būti suvaržomos tik tokia apimtimi, kuri yra proporcinga siekiamam tikslui. Todėl, prieš leidžiant naujas iniciatyvas dalintis duomenimis tarp finansų įstaigų ir su teisėsauga ir rengiant tai įgalinančias įstatymo pataisas, turi būti įvertintas kovos su finansiniais nusikaltimais priemonių proporcingumas. Kaip ir teigia EŽTT, „[.. valstybė, atliekanti „pionierės“ vaidmenį, [...] prisiima ypatingą atsakomybę už tinkamos pusiausvyros radimą[107]“. Tačiau, įstatymų leidėjui dažnai nepavyksta nustatyti tinkamos interesų pusiausvyros, todėl tinkamo balanso nustatymo pareiga iš esmės paliekama teismų kompetencijai[108]. Todėl vertinant, ar galimybė finansų įstaigoms keistis informacija tarpusavyje ir su teisėsaugos institucijoms nepažeidžia teisės į privatumą ir asmens duomenų apsaugą, būtina atsižvelgti į esant panašioms faktinėms aplinkybėms priimtus teismų sprendimus.

2.4 Asmens duomenų apsauga kovoje su finansiniais nusikaltimais: teismų praktika

2.4.1 Aiškumo reikalavimas

ESTT akcentuoja teisės į privatumą ir asmens duomenų apsaugą svarbą[109]. Tačiau, iki šiol vienintelė byla, kurioje teismas vertino teisės į privatumą ir asmens duomenų apsaugą suvaržymą

[106] Article 29 Data protection Working Party, *supra note*, 98: 6.
[107] Žmogaus Teisių Teismas, „Case of S. and Marper v. The United Kingdom“, 30562/04, 30566/04, 2008 m. gruodžio 4 d, 112, HUDOC, žiūrėta 2024-01-26, https://hudoc.echr.coe.int/fre?i=001-90051
[108] Kaiser, *supra note* 10: 260.
[109] Kaiser, *supra note* 10: 260.

kovojant su finansiniais nusikaltimais yra *WM and Sovim SA vs Luxembourg Business Registers*. Byloje spręstas klausimas, ar prieigos prie juridinio asmens galutinių naudos gavėjų nacionalinio registro suteikimas plačiajai visuomenei nepažeidžia asmenų, esančių naudos gavėjais, teisių į asmens duomenų apsaugą. Sujungtose bylose C-37/20 IR C-601/20 ESTT nustatė, kad 5 Pinigų plovimo prevencijos Direktyvos nuostata, dėl prieigos prie juridinių asmenų tikrųjų savininkų duomenų suteikimo plačiajai visuomenei, yra negaliojanti, nes materialinėje teisės normoje naudojamas žodis „bent“ (asmenys [...] gauna bent tokią informaciją: tikrojo savininko vardą ir pavardę, gimimo metus [...])[110] neatitinka aiškumo ir tikslumo reikalavimo[111]. Taip pažeidžiamas pirmasis Chartijoje įtvirtintas kriterijus – „priemonės suvaržančios Chartijos saugomų pamatinių teisių įgyvendinimą turi būti aiškiai ir tiksliai apibrėžtos ir įtvirtintos įstatymais“[112].

Lietuvos teisėje, teisė į privatumą ir asmens duomenų apsaugą tai pat pasirodė itin saugoma kovos su finansiniais nusikaltimais akivaizdoje. 2022m. prezidentas vetavo įstatymo pataisą, kuria buvo siekiama suteikti galimybę mokėjimo paslaugų teikėjams tvarkyti specialių kategorijų asmens duomenis vykdant sukčiavimo, atliekant mokėjimus, prevenciją, tyrimą ir nustatymą. Prezidentas pabrėžia, kad „esminė žmogaus teisė į duomenų apsaugą turi būti užtikrinta[113]“, o įstatymas, kuriame nėra pateikta aiškaus ir baigtinio sąrašo kriterijų, „kas laikytina [...] sukčiavimo atliekant mokėjimus prevencija tyrimu ir nustatymu, neatitinka konstitucinio proporcingumo principo“, „pagal kurį asmens teisių ir laisvių įstatymų negalima riboti labiau, negu reikia teisėtiems ir visuomenei svarbiems tikslams pasiekti“[114]. Iš to išplaukia, kad ginant konstitucines teises, įtvirtinti įstatymu būtina tik tai, kas minimaliai būtina[115]“. Be to, prezidentas pabrėžia, kad būdama ES nare, Lietuva negali priimti įstatymo su plačiais, beprecedenčiais duomenų tvarkymo įgaliojimais[116].

---

[110] Europos Parlamento ir Tarybos direktyva (ES) 2018/843, *supra note*, 43: 30 str. 5 d., c p.
[111] Europos Sąjungos Teisingumo Teismas, „Sprendimas Sujungtose bylose WM (C-37/20) ir Sovim SA (C-601/20) prieš Luxembourg Business Registers“, 2022 m. lapkričio 22d, 82 p., InfoCuria, žiūrėta 2024-01-27, https://curia.europa.eu/juris/document/document.jsf?text=&docid=268059&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=311534
[112] Europos Sąjungos pagrindinių teisių Chartija, *supra note*, 81: 52 str.
[113] *Prezidento veto: žmogaus privatus gyvenimas turi būti apsaugotas tinkamai reguliuojant asmens duomenų tvarkymą*, 2022 m. lapkričio 17 d, Lietuvos Respublikos Prezidentas, žiūrėta 2024-01-27, https://www.lrp.lt/lt/prezidento-veto-zmogaus-privatus-gyvenimas-turi-buti-apsaugotas-tinkamai-reguliuojant-asmens-duomenu-tvarkyma/39475
[114] Lietuvos Respublikos Prezidento Dekretas, „Dėl Lietuvos Respublikos Mokėjimų įstatymo NR. VIII-1370 2, 3, 54, 76 straipsnių ir priedo pakeitimo įstatymo NR.XIV-1478 grąžinimo Lietuvos Respublikos Seimui pakartotinai svarstyti“, 2022 m. lapkričio 17 d, 1 str. 9 p., INFOLEX, žiūrėta 2024-01-27, https://www.infolex.lt/ta/810191
[115] *Seimas pritarė Respublikos Prezidento veto dėl Mokėjimų įstatymo pataisų*, Lietuvos Respublikos Seimas, žiūrėta 2024-01-27, https://www.lrs.lt/sip/portal.show?p_r=35403&p_k=1&p_t=283020
[116] Prezidento veto, *supra note*: 113.

2.4.2 Masinis sekimas

Grįžtant prie *WM and Sovim SA vs. Luxembourg Business Registers* bylos, ESTT pasako, kad nors kova su finansiniais nusikaltimais yra bendrojo intereso tikslas, kuriuo galima pateisinti net ir didelius Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymus, bet dėl galimybės bet kuriam plačiosios visuomenės atstovui susipažinti su informacija apie tikruosius savininkus suteikiami pranašumai kovoje su finansiniais nusikaltimais negali kompensuoti daug didesnio teisės į privatumą ir asmens duomenų apsaugą suvaržymo[117] (netenkinamas proporcingumo kriterijus).

Tiesa, šioje byloje vertintas asmens duomenų atskleidimas plačiajai visuomenei, o ESTT pažymėjo, kad kova su finansiniais nusikaltimas visų pirma yra finansų įstaigų ir FŽP kompetencija[118]. Ši pastaba leidžia manyti, kad platesnio mąsto įsikišimas į privataus gyvenimo sferą būtų priimtinas, kai kovos su finansiniais nusikaltimais priemones taiko kompetentingos institucijos. Kadangi, kovos su finansiniais nusikaltimais priemonių proporcingumas, kai priemones taiko kompetentingos institucijos, nebuvo nagrinėtas teisme, vertinant priemonių proporcingumą remiamasi bylomis, nagrinėtomis esant panašioms faktinėms aplinkybėms.

Digital Rights of Ireland byloje ESTT nagrinėjo Direktyvos 2006/24 galiojimą. Direktyva buvo nustatyta pareiga viešai prieinamiems elektroninių ryšių paslaugų ar viešųjų ryšių tinklų teikėjams saugoti visų vartotojų telekomunikacijų duomenis nuo 6 mėn. iki 2m., siekiant, kad duomenys būtų prieinami sunkių nusikaltimų, tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslu. ESTT konstatavo, kad minėta Direktyva yra negaliojanti, nes bendrai taikoma visiems asmenims ir visoms elektroninio ryšio priemonėms, bei visiems srauto duomenims visiškai jų nediferencijuojant, nenumatant kokių nors ribojimų ar išimčių pagal kovos su sunkiais nusikaltimais tikslo kriterijų[119], net tiems asmenims, kurie neatitinka jokių požymių, leidžiančių manyti, kad jų elgesys gali būti, nors netiesiogiai, ar tolimai, susijęs su sunkiais nusikaltimais[120]. Taip sudaromas plataus masto ir ypač didelis Chartijos teisių apribojimas, kuris nėra tiksliai reglamentuotas nuostatomis, leidžiančiomis užtikrinti, kad iš tiesų neviršijama tai, kas yra griežtai

[117] Europos Sąjungos Teisingumo Teismas, *supra note*, 111: 83.
[118] *Ibid.*
[119] Europos Sąjungos Teisingumo Teismas, „Sprendimas Sujungtose bylose Digital Rights Ireland Ltd (C-293/12) prieš Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Airiją,The Attorney General, ir Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl ir kt“, 2014 m. balandžio 8d, 57p., EUR-LEX, žiūrėta 2024-01-27, https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62012CJ0293
[120] *Ibid*., 58 p.

būtina[121], o asmeniui sukeliamas nepaaiškinamas pojūtis, jog yra stebimas[122]. Analogiškai, kovos su finansiniais nusikaltimais prevencijos priemonės taikomos visiems asmenims be išimties, neturint pirminių įtarimų konkretaus asmens atžvilgiu. Tiesa, būtų galima argumentuoti, kad rizika grįstas požiūris reikalauja klientus skirtyti į rizikos kategorijas, bet to nepakanka, nes rizikos kategorijos iš esmės nustato, tik, ar deramo kliento patikrinimo metu turi būti atliekamas sustiprintas kliento patikrinimas. Finansų įstaigos atlieka visų be išimties finansinių operacijų stebėjimą, neatsižvelgiant kokia kliento rizika nustatyta pirminio vertinimo metu. Atsižvelgiant į tai, kad finansinių įstaigų paslaugomis naudojasi 96,4 % populiacijos euro zonoje[123], nuolatinis finansinių operacijų stebėjimas gali būti prilyginamas masiniam sekimui. V. Ferrari apibūdina kovos su finansiniais nusikaltimais tikslu vykdomą masinį sekimą kaip „ stebėjimu pagrįstus teisėsaugos tinklus, sukurtus finansinių duomenų bazėse“[124]. Galimybė finansų įstaigoms dalintis informacija tarpusavyje ir su teisėsaugos institucijomis, numanomai dar labiau padidintų masinio sekimo mąstą, o asmuo gali jaustis nuolat stebimas ne tik finansų įstaigos, kurios paslaugomis naudojasi, bet ir viso finansų įstaigų tinklo ir teisėsaugos.

Keliais metais vėliau, vėl kreiptasi į ESTT su prašymu priimti prejudicinį sprendimą sujungtose bylose *Tele2 Sverige AB* ir *Secretary of State for the Home Department* iš esmės prašant išaiškinti, kokia apimti taikomas sprendimas byloje *Digital Rights of Ireland*, dėl teisėsaugos institucijų prieigos prie saugomų duomenų. Šioje byloje ESTT konstatavo, kad „draudžiami nacionalinės teisės aktai, kuriuose kovos su nusikalstamumu tikslais numatyta pareiga bendrai, nediferencijuojant saugoti visus, su visais abonentais ir registruotais naudotojais susijusius srauto ir vietos nustatymo duomenis, perduodamus bet kokia elektroninio ryšio priemone[125]“. O „kalbant apie kovą su nusikalstamumu, iš principo, prieiga teisėsaugos institucijoms gali būti suteikta tik prie asmenų, kurie įtariami planuojantys sunkų nusikaltimą, jį darantys arba padarę, arba vienaip

[121] Europos Sąjungos Teisingumo Teismas, „Sprendimas Sujungtose bylose Digital Rights Ireland Ltd (C-293/12) prieš Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Airiją,The Attorney General, ir Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl ir kt“, 2014 m. balandžio 8d, 65p., EUR-LEX, žiūrėta 2024-01-27, https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62012CJ0293

[122] Generalinio Advokato Išvada, „Sujungtose bylose Digital Rights Ireland Ltd (C-293/12) prieš Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Airiją, The Attorney General, ir Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl ir kt“, 2013 m. gruodžio 12d, 52 p., InfoCuria, žiūrėta 2024-01-27, https://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=LT&mode=req&dir=&occ=first&part=1&cid=315665

[123] Miguel Ampudia, Michael Ehrmann, „Financial inclusion: what’s it worth?“, ECB Working Paper, 1990 (2017), 3, https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1990.en.pdf

[124] Ferrari, *supra note*, 11: 525

[125] Europos Sąjungos Teisingumo Teismas, „Sprendimas Sujungtose bylose Tele2 Sverige AB (C 203/15) prieš Post och telestyrelsen Secretary of State for the Home Department (C 698/15) prieš Tom Watson, Peter Brice, Geoffrey Lewis“, 2016 m. gruodžio 21 d., 112p., InfoCuria, žiūrėta 2024-01-27, https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=5995909

ar kitaip dalyvavę jį darant“[126]. Perkeliant šį teismo sprendimą į dalinimosi duomenimis tarp finansų įstaigų ir su teisėsauga modelį, reikia pasižymėti, kad teisėsaugai negali būti suteikiama prieiga prie finansų įstaigų turimų asmens duomenų iki įtarimų kilimo.

Vokietijos Konstitucinis teismas, dar anksčiau sprendęs iš tos pačios Direktyvos kilusį klausimą dėl telekomunikacijų duomenų rinkimo, nesant konkretaus pagrindo, pabrėžė, kad duomenų apie klientus, ar vartotojus saugojimas be pakankamo pagrindo įtarti, neturėtų būti laikomas norma, o priimtinas tik kaip siaura išimtis iš taisyklės, kuria galima pasinaudoti tik esant būtinybei[127]. Grindžiant šiuo sprendimu, tai pat turėtų būti keliamas klausimas, ar dalinimasis duomenimis iki įtarimų kilimo, net kai teisėsaugai nesuteikiama prieiga, o tai vyksta tik finansų įstaigų lygmenyje, gali būti laikomas proporcingu.

Masinio sekimo problema gali būti neutralizuojama tik susiaurinant stebimų asmenų ratą, pagrįsta įtartinumo kriterijumi. Tačiau, čia susiduriama su kita problema. Pirma, įtarimas yra daugiau, nei tuščias svarstymas, bet neatitinka faktinių, įrodymais pagrįstų žinių[128]. Nors iš reguliuojamo sektoriaus darbuotojų, vykdančių finansinių nusikaltimų prevenciją, tikimasi didesnių, nei įprasta profesinių gebėjimų, pagrįstai atskirti įtarimų keliančias operacijas. Jie „pirmiausia turi išaiškinti, kas yra įprasta kliento veikla, kad galėtų pasakyti, kas yra neįprasta“[129]. Tam reikia rinkti asmens duomenis ir stebėti vykdomas operacijas. Taigi, kol finansinių operacijų visuotinis stebėjimas, vykdant finansinių nusikaltimų prevenciją, yra būtina priemonė, nesant mažiau varžančių alternatyvų, keitimasis informacija tarp finansų įstaigų ir su teisėsaugos institucijomis gali būti ir nepateisintas kaip būtinas.

2.5 Soft law: EDPB rekomendacijos

Reaguodama į siūlomą Reglamentą ir Direktyvą (žr. 1.3.4), EDPB paskelbė dvi nuomones ir laišką Europos Parlamentui ir Tarybai, kuriame įspėjo dėl dalijimosi duomenimis.

Keitimasis informacija tarp finansų įstaigų

---

[126] Europos Sąjungos Teisingumo Teismas, „Sprendimas Sujungtose bylose Tele2 Sverige AB (C 203/15) prieš Post och telestyrelsen Secretary of State for the Home Department (C 698/15) prieš Tom Watson, Peter Brice, Geoffrey Lewis“, 2016 m. gruodžio 21 d., 119p., InfoCuria, žiūrėta 2024-01-27, https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=5995909

[127] Vokietijos Konstitucinis Teismas, „Headnotes to the Judgment of the First Senate“, 2010 m. kovo 2d. 1BvR 256, 263, 586/08, 206 p., žiūrėta 2024-01-27, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html

[128] Mark Dennis, *The measure of last resort: some things you need to know about the law of arrest*, Forbes Chambers, 2011, 2, https://criminalcpd.net.au/wp-content/uploads/2016/09/Arrest_paper__The_Measure_of_Last_Resort__June_2011.pdf

[129] Marius Laurinaitis, Darius Štitilis, ir Egidijus Verenius, „Asmens duomenų kiekio mažinimo principo įgyvendinimas finansų įstaigose“, JURISPRUDENCIJA, 27, 2 (2020): 397, https://ojs.mruni.eu/ojs/jurisprudence/article/view/6365/5325

Pasak EDBP, siūlomo Reglamento 55 str. 5p., kuris leistų finansų įstaigoms tarpusavyje dalintis informacija (angl. *private-private partnership*), reikštų labai didelį asmens duomenų apdorojimo mąstą, kuris sukeltų masinį stebėjimą, atliekamą privačių subjektų. Dėl to, tokios priemonės proporcingumas yra labai abejotinas[130].

Keitimasis teisėsaugos informacija su FŽP

Vertinant dalinimąsi informacija su FŽP, Europos duomenų apsaugos priežiūros pareigūnas (angl. *European Data Protection Supervisor*), toliau EDPS, mano, kad 6-osios Pinigų plovimo prevencijos Direktyvos[131] 18 str., FŽP suteikiamos itin platūs įgaliojimai prieigai prie teisėsaugos informacijos, pirmiausia nesuderinami su administraciniu FŽP statusu, o tai pat ir neatitinkantys proporcingumo principo. EDBP pabrėžia, kad informacija perduodama FŽP turi būti apribota iki būtinojo reikalingumo ir siejama tik su FŽP Sąjungoje patikėtais operatyvinės ir strateginės analizės uždaviniais. Kai tuo metu, siūlomu įstatymo pakeitimu, aiškia neapibrėžiama, kokiomis asmens duomenų kategorijomis leidžiama dalintis, nurodant platų, nebaigtinį sąrašą, kuris įtraukia tiesioginę ir netiesioginę prieigą prie teisėsaugos informacijos[132].

Keitimasis informacija su teisėsaugos institucijomis

Vertindama Reglamento 55 str. 7p., siūlomą galimybę teisėsaugos institucijoms keistis operatyvine informacija su finansų įstaigomis (angl. *public-private partnerships*), EDPB išreiškė susirūpinimą, kad tai būtų „labai rizikingas precedentas, vertinant iš duomenų apsaugos perspektyvos“[133]. Informacijos perdavimo valstybės institucijoms ribojimas yra labai svarbus teisės į privatumą ir asmens duomenų apsaugą turinio aspektas, suteikiantis asmeniui apsaugą nuo perdėto valstybės kišimosi į privatų gyvenimą. Įstatymais įtvirtinta galimybė ne tik surinkti informaciją iš finansų įstaigų, kai asmuo įtarimas padaręs nusikalstamą veiką, bet ir nurodyti finansų įstaigoms stebėti asmenį, kartu perduodant operatyvinę informaciją, tam tikra apimtimi reikštų teisėsaugos pareigų perdavimą privačiam sektoriui. EDPB šiuo klausimu laikosi pozicijos, kad „bet kokiomis aplinkybėmis, tiesiogiai ar netiesiogiai, privačiam sektoriui neturi būti patikėtos teisėsaugos užduotys“[134]. Teisėsaugos informacijos perdavimas finansų įstaigoms, analogiškai kaip ir dalinimosi informacija finansų įstaigoms tarpusavyje atveju, paskatintų atskyrimą nuo

[130] European Data Protection Board, „Letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations“, 2023 m. kovo 28d., Briuselis, 3, žiūrėta 2024-01-27. https://edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0015_aml_cft_ep_en.pdf

[131] Pasiūlymas, Europos Parlamento ir Tarybos Direktyva, *supra note,* 68: 18 str.

[132] Data Protection Supervisor, „Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals“, 2021 m. rugsėjo 22d., 11, https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf

[133] European Data Protection Board, *op.cit.,* 3.

[134] European Data Protection Supervisor, „Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC“, 2017 m. vasario 2d., 61 p., https://www.parlament.gv.at/dokument/XXV/EU/131392/imfname_10692002.pdf

finansų sistemos. „Todėl EDPB nuomone, sunkiai tikėtina tokia priemonė atitinka būtinumo ir proporcingumo kriterijus“ [135].

Tai pat, išreiškiamas susirūpinimas, kad pradėjus dalintis duomenimis tarp finansų įstaigų ir su teisėsaugos institucijomis, labai sustiprėtų rizikos minimizavimo praktika (angl. *de-risking)* [136]. Rizikos minimizavimas yra reiškinys, kai finansų įstaigos atsisako teikti paslaugas asmeniui, nes jis kelia per daug rizikos, palyginti su gaunama nauda. Tokios praktikos pasekmė yra finansinė atskirtis, kurią patiria asmuo „išmestas“ iš finansų sistemos. Finansinė atskirtis siejama su didele socialinės atskirties rizika ir gali sukelti nepasitikėjimą tiek valstybe, tiek finansų įstaigomis[137]. EBA (European Banking Authority) įspėja, kad rizikos minimizavimas, ypač nesant įsitesėjusio teismo sprendimo asmens atžvilgiu, prieštarauja bendriems ES tikslams, gali iškraipyti konkurenciją vieningoje rinkoje ir neigiamai paveikti valstybių narių finansų sistemos stabilumą[138]. Dėmesys į finansinės atskirties problemą ypač pakrypo 2024m., kai Jungtinės Karalystės Aukščiausiasis Teismas atsisakė nagrinėti ieškinį, kuriame ieškovas kaltina finansų įstaigą atsisakius teikti jam paslaugas, nesant pagrįstų įrodymų ir siekia, atstatyti asmens reputaciją[139]. Jungtinės Karalystės Aukščiausiasis Teismas savo sprendimą motyvavo tuo, kad bylinėjimosi metu šalių patirtos išlaidos, neatsvertų ieškovo gaunamos naudos, nes jis nepatyrė finansinių nuostolių, o „išmetimo“ iš finansų sistemos atvejus (angl. *de-banking*) turėtų nagrinėti ne teismas, o finansinių paslaugų priežiūros institucija[140].

Apibendrinant, teisė į privatumą ir asmens duomenų apsaugą, kovojant su finansiniais nusikaltimais gali būti apribota. Chartija nustato sąlygas tokiam teisės suvaržymui, išlaikant tinkamą balansą tarp dviejų skirtingų interesų. Pamatinės Chartijos nuostatos perkeltos ir į antrinį teisės šaltinį – BDAR, kuriuo, atlikdamos finansinių nusikaltimų prevenciją remiasi finansų įstaigos. Pagal BDAR, finansinių operacijų duomenys gali būti tvarkomi tik tam tikslui, kuriam yra surinkti ir tik tokia apimtimi, kiek būtina siekiant nustatyto tikslo. Duomenims kilus įtarimui, vadovaujantis BDAR 23 str. išimtimi, tam tikros BDAR nuostatos, gali būti netaikomos. Todėl, kuriant keitimosi informacija tarp finansų įstaigų ir su teisėsaugos institucijomis modelius, kurie

[135] European Data Protection, *supra note,* 130: 3.
[136] Financial Action Task Force (FATF), *supra note*, 6: 48.
[137] Bank for International Settlements (BIS), *supra note,* 55: 19.
[138] European Banking Authority, „Opinion of the European Banking Authority on ‘de-risking’“, 2022 m. sausio 5d., 4, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-irsking.pdf
[139] „Revolut calls on High Court to throw out lawsuit over account closure“. *Financial Times*. 2024 m. sausio 18d. https://www.ft.com/content/8763fa89-4269-4286-91d1-678cb71cde12
[140] https://riskandcompliance.freshfields.com/post/102j1zz/de-banking-claim-against-revolut-struck-out-as-an-abuse-of-process

nepažeistų teisės į privatumą ir asmens duomenų apsaugą, iš esmės turi būti kliaujamasi Chartijoje nustatytais principais.

Kai asmens duomenys tvarkomi teisinės prievolės, ar viešojo intereso pagrindu, pareiga nustatyti priemonių proporcingumą tenka įstatymo leidėjui. Bet, jei asmens duomenys tvarkomi teisėto intereso pagrindu, o taip ir yra keitimosi informacija tarp finansų įstaigų ir su teisėsaugos institucijomis modeliuose, pareiga išlaikyti interesų balansą tenka pačiai finansų įstaigai. Šis aspektas yra problematiškas, nes teismas, net įstatymo leidėjo teisės aktuose įtvirtintas priemones gali pripažinti neatitinkančias proporcingumo kriterijaus.

Neabejojama, kad dėl kovos su finansiniais nusikaltimais svarbos, galima pateisinti ir didelio mąsto teisės į privatumą ir asmens duomenų apsaugą suvaržymus, tačiau priemonės turi būti aiškiai numatytos įstatyme, nepaliekant diskrecijos finansų įstaigai veikti savo nuožiūra. Tai pat, teismas nepateisina ir masinio sekimo (plataus mąsto duomenų rinkimo, nesant išimčių ar nesant pirminių įtarimų). Masinis sekimas būdingas kovai su finansiniais nusikaltimais, o platesnės galimybės keistis duomenis, dar labiau paskatintų šį reiškinį. Todėl, keitimasis asmens duomenimis iki įtarimų kilimo, neatitinka proporcingumo principo.

Pateikdama nuomonę, dėl ES siūlomų kovą su finansiniais nusikaltimais reguliuojančių teisės aktų pakeitimų, EDPB abejoja ar priemonės, leidžiančios keistis informacija tarp finansų įstaigų, FŽP gauti informaciją iš teisėsaugos ir teisėsaugai perduoti operatyvinę informaciją finansų įstaigoms, gali būti laikomos proporcingomis. Taikant išvardintas priemones, asmuo, be teisėto pagrindo (nesant įsitesėjusio teismo sprendimo), gali patirti finansinę atskirtį. O tai gali sukelti nepasitikėjimą valstybe ir finansų įstaigomis.

Prisimenant, kad pokyčiai leidžiantys platesnes galimybes keistis informacija tarp kovą su finansiniais nusikaltimais vykdančių subjektų yra būtini, norint efektyviai kovoti su šiais nusikaltimais, ir žinant, kokie reikalavimai kyla siekiant nepažeisti teisės į privatumą ir asmens duomenų apsaugą, keičiantis šia informacija, 3-ame skyriuje analizuojami, keitimosi informacija ir tarp finansų įstaigų ir su teisėsauga modeliai, kuriuos jau taiko/ruošiasi taikyti keletas valstybių.

3. KEITMOSI INFORMACIJA MODELIAI

Įstatymo leidėjui delsiant reglamentuoti keitimosi informacija tvarką, pradėta keistis informacija savanoriškais pagrindais. Keliose valstybėse narėse privatus sektorius sujungė jėgas ir ėmėsi iniciatyvos, sukurti keitimosi informacija modelius ir technines platformas. Privataus sektoriaus iniciatyvų kilimas rodo pasiryžimą išeiti iš įstatymais nustatytų minimalių atitikties ribų, siekiant ne tik formaliai laikytis įstatymo, bet ir efektyviai kovoti su finansiniais nusikaltimais[141]. Apytikriai 2019-2022m. pradėti taikyti modeliai jau pademonstravo pirmuosius sėkmingus rezultatus kovoje su finansiniais nusikaltimais. Atlikta keletas išsamių studijų, parodančių, kad dalinimosi informacija tarp finansų įstaigų modeliai leidžia apdoroti daugiau duomenų, aptikti finansinių nusikaltimų grandinę, kuri nebūtų matoma izoliuotai veikiant vienai finansų įstaigai, pašalina nereikalingą dubliavimą, mažina finansų įstaigoms tenkančią atitikties naštą, ir leidžia FŽP perduoti kokybiškesnę informaciją, kas galiausiai nulemtų neteisėtų būdu įgytų lėšų eliminavimą iš finansų sistemos ir konfiskavimą[142]. Tačiau, modelių suderinimo su asmens duomenų apsaugos reikalavimais klausimas nėra iki galo išspręstas. Šiame skyriuje analizuojami pasirinkti modeliai, į analizę įtrauktos ES valstybės ir trečiosios šalys, siekiant palyginti, galimybes keistis informacija kovojant su finansiniais nusikaltimais ES narėse ir kitose valstybėse. Pirmoje skyriaus dalyje analizuojami keitimosi informacija tarp finansų įstaigų modeliai, o antroje – keitimosi su teisėsauga.

3.1 Keitimosi informacija tarp finansų įstaigų modeliai

3.1.1 TMNL Olandijoje

Informacijos mainų modelių pradininke ES galima laikyti Olandiją. 2020m., 5 Olandijoje veikiantys bankai susijungė ir įkūrė *Transactie Monitoring Nederland B.V.* (toliau TMNL). TMNL yra „debesų“ platforma, kurioje talpinami prie platformos prisijungusiose finansų įstaigose atliekamų operacijų duomenys. Oficialioje interneto svetainėje TMNL pristatoma kaip platforma, sujungianti skirtingų finansų įstaigų operacijų duomenis ir randanti prasmingus ryšius tarp jų. Analizuodami šiuos ryšius, finansų įstaigų specialistai, įgauna naujų įžvalgų apie galimai vykdomus finansinius nusikaltimus. Platformos pagalba aptinkamos neįprastos operacijos ir

[141] Vogel, *supra note* 9: 6.
[142] Bank for International Settlements (BIS), *supra note,* 55; Financial Action Task Force (FATF), *supra note*, 6; Future of Financial Intelligence Sharing (FFIS) research program, *supra note* 8.

atskleidžiamos naujos taktikos, kurios kitu atveju galėtų likti nepastebėtos[143]. Platformoje esantys duomenys yra pseudominizuoti. Pseudomenizavimas tai asmens duomenų anonimizavimo būdas, kai asmenį galinti identifikuoti informacija pakeičiama unikaliu identifikatoriumi, ir gali būti konvertuojama atgal į identifikuoti asmenį leidžiančius duomenis, tik turint šifravimo raktą. Tai reiškia, kad identifikuoti asmenį, dėl kurio gautas įspėjimas, gali tik finansų įstaiga, susijusi su to asmens vykdomomis finansinėmis operacijomis. Kai pagal įvestus algoritmus stebėdama finansines operacijas, dirbtinio intelekto pagalba, platforma aptinka galimo finansinio nusikaltimo požymių, visos su ta finansine operacija susijusios finansų įstaigos gauna įspėjimą. Įspėjimus, finansų įstaigos, peržiūri savarankiškai, ir nepriklausomai nuo kitų nusprendžia, ar pildyti STR. Platformoje neatskleidžiama, ar kitos finansų įstaigos pateikė STR.

Dėl asmens duomenų apsaugos keliamų reikalavimų, teisinėje aplinkoje vyraujantis neužtikrintumas yra viena pagrindinių kliūčių sparčiam duomenų keitimosi modelių vystymui[144]. Siekiant, kad šis iššūkis netrukdytų toliau plėtoti TMNL, o finansų įstaigoms nekiltų abejonių dėl asmens duomenų perdavimo teisėtumo, Olandijoje suskubta keisti nacionalinę teisę, įtvirtinant finansų įstaigoms pareigą dalintis duomenimis tarpusavyje. Inicijuotose Olandijos pinigų plovimo prevencijos ir terorizmo finansavimo prevencijos įstatymo (oland. *de Wet ter voorkoming van witwassen en financieren van terrorisme*) pakeitimuose, numatyta, kad:

1) finansų įstaiga imasi pagrįstų priemonių įsitikinti, ar kitoje finansų įstaigoje nebuvo atsisakyta teikti paslaugų klientui, ir jei taip, kokios buvo atsisakymo priežastys;
2) paklausimą gavusi finansų įstaiga nedelsdama informuoja apie nustatytą kliento riziką, priemones, kurių ėmėsi šiai rizikai valdyti, arba paslaugų nutraukimo/atsisakymo teikti aplinkybes;
3) pradėdama dalykinius santykius su klientu, finansų įstaiga informuoja klientą apie savo pareigą perduoti/rinkti informaciją iš kitos finansų įstaigos[145].

Įstatymo pakeitimas išpildo pirmąją Chartijos nuostatą, reikalaujančią, kad bet koks teisės suvaržymas turi būti numatytas įstatymo. Tai pat, išsprendžiamas teisėto pagrindo pagal BDAR klausimas, nes dalijimuisi duomenimis iš savanoriško pereinant į reikalaujamą įstatymu, teisėtu pagrindu tampa teisinės pareigos vykdymas. Našta vertinti priemonių proporcingumą tenka įstatymo leidėjui, o ne pačiai finansų įstaigai (žr. 2.3.4).

---

[143] *What does TMNL do?*, Transactie Monitoring Nederland, žiūrėta 2024-02-21, https://tmnl.nl/en/about-tmnl/tmnl-in-brief/

[144] Financial Action Task Force (FATF), *supra note*, 6: 44.

[145] Tweede Kamer der Staten-Generaal 2022-2023, 36 228 Nr.2, ,, Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme in verband met het verbod op contante betalingen voor goederen vanaf 3.000 euro en het uitbreiden van de mogelijkheden voor informatie-uitwisseling ten behoeve van de poortwachtersfunctie (Wet plan van aanpak witwassen)“, 3b, Tweede Kamer, žiūrėta 2023-02-22. https://www.tweedekamer.nl/downloads/document?id=2022D43319

Naudojant TMNL, finansų įstaigos dalijasi duomenis iki įtarimų kilimo (angl. *pre-suspicion*). Dalinimasis tokias duomenimis gali būti pripažintas neproporcingai varžantis teisę į privatumą ir asmens duomenų apsaugą, dėl jam būdingo masinio sekimo (žr. 2.4.2). Vertindama siūlomus įstatymo pakeitimus DPA priėjo išvadą, kad nėra pagrįsto ryšio tarp priemonių tikslo ir teisės į privatumą ir asmens duomenų apsaugą suvaržymo, todėl keitimasis informacija tarp finansų įstaigų neatitinka proporcingumo principo[146]. DPA motyvuoja savo išvadą pirma tuo, kad nebuvo įvertintos kitos mažiau varžančios alternatyvos, antra, kad priemonių veiksmingumas yra ribotas.

DPA pažymi, kad neaišku, kodėl naudojantis „juoduoju sąrašu“, finansų įstaiga negali pasiekti tokių pačių rezultatų kaip naudojantis TMNL platforma[147]. „Juodasis sąrašas“ tai centriniame išoriniame registre talpinami duomenys apie klientus, kuriems buvo atsisakyta teikti paslaugas dėl keliamos rizikos. Klausimas, ar naudojantis „juoduoju sąrašu“ pasiekiami rezultatai gali būti prilyginami keitimosi informacija modeliu pasiekiamais rezultatais. „Juodasis sąrašas“ padeda finansų įstaigai aptikti, kad klientas kelia riziką, tačiau naudojantis tik juo, nebūtų atrastos finansinių nusikaltimų schemos už vienos finansų įstaigos ribų, taip, kaip tai galima atlikti sutelkiant finansų įstaigų duomenis vienoje platformoje.

Kita DPA išsakyta pastaba dėl riboto priemonių veiksmingumo aiškinama tuo, kad jei duomenimis keičiamasi tik tarp prie platformos prisijungusių finansų įstaigų, arba tik vienos valstybės teritorijoje, tokia priemonė nepadės pasiekti trokštamų pokyčių kovoje su finansiniais nusikaltimais, nes duomenų mainams išlieka būdingas izoliuotas vaizdas. Tiesa, šia pastaba neatsižvelgiamą į tai, kad modelis veikia kaip pilotinė programa. Gavus projekto rezultatus ir įsitikinus modelio veikimo sėkme, modelį būtų galima pradėti taikyti, prisijungiant ir finansų įstaigoms iš kitų valstybių.

Nors DPA išsakyti argumentai nesustabdė iniciatyvos ir įstatymo pakeitimo projektas perduotas svarstyti Olandijos Atstovų rūmams, ESTT priėmus sprendimą *WM and Sovim SA vs. Luxembourg Business Registers* byloje, Olandijoje nuspręsta sustabdyti platesnių galimybių dalintis duomenimis tarp finansų įstaigų ir su teisėsauga suteikimą ir nepriimti naujų iniciatyvų, nes dalijimosi informacija teisinis pagrindas yra politiškai kontraversiškas ir reikalauja tolimesnių diskusijų[148].

[146] *Netherlands: AP advises on draft bill to amend Money Laundering Action Plan Act*, OneTrust Data Guidance, žiūrėta 2024-02-22, https://www.dataguidance.com/news/netherlands-ap-advises-draft-bill-amend-money
[147] Autoriteit Persoonsgegevens, „ Advies consultatieversie voorstel voor de wet plan van aanpak witwassen“, 2020 kovo 10d, 2-3, https://autoriteitpersoonsgegevens.nl/uploads/imported/advies_wet_plan_van_aanpak_witwassen.pdf
[148] *News update Financial Regulatory,* Hauthoff, žiūrėta 2024-02-21, https://www.houthoff.com/insights/news-update/dutch-government's-aml-policy-agenda-and-fine-for-collective-licence-holder

3.1.2 AML Bridge Estijoje

Keliais mėnesiais vėliau nei Olandijoje, Estijoje inicijuotas AML Bridge projektas dalinimuisi informacija finansinių nusikaltimų prevencijos tikslu. Projekto iniciatoriai buvo 4 didžiausi Estijos bankai, sujungę jėgas su Reguliavimo technologijų (RegTech, angl. *regulatory technology*) įmone. Nuo pat pradžių, į projektą įtrauktas Estijos reguliatorius, DPA ir FŽP. Skirtingai nei TMNL, AML Bridge yra sukurtas dalintis duomenimis kilus įtarimams. Naudodamos AML Bridge finansų įstaigos tarpusavyje dalinasi operatyvia informacija ir gali vykdyti bendrus tyrimus. Pažymėtina tai, kad keitimasis informacija AML Bridge platformoje, be tradicinių finansinių nusikaltimų, apima ir keitimąsi informacija dėl sukčiavimo ir tarptautinių sankcijų pažeidimo. Platformos pagrindą sudaro pranešimų mechanizmas, kai nustačius finansinio nusikaltimo požymių, siejamu su konkrečiu IBAN numeriu, finansų įstaigos palieka pranešimą, kurį gali matyti kitos prie AML Bridge prisijungusios finansų įstaigos, kai jose vykdoma operacija, naudojant tą patį IBAN numerį[149]. Susirašinėjimas tarp platformos narių yra užšifruotas, norint iššifruoti pranešimus reikalingas raktas, kurį turi tik finansų įstaigos, todėl asmens duomenys yra neprieinami platformos tiekėjui, ar bet kuriai kitai suinteresuotai šaliai[150].

Autorės žiniomis, nėra duomenų, kad Estijos DPA būtų nepalankiai vertinusi keitimosi informacija modelio kūrimą (kaip tai nutiko Olandijoje). Galbūt todėl, kad keitimosi informacija modeliu sukūrimui Estijoje jau ilgai vyrauja palanki teisinė-reguliacinė aplinka. Tai paaiškinama valstybės požiūriu į kovos su finansiniais nusikaltimais svarbą. Bankinis sektorius Estijoje anksčiau yra įsivėlęs į pinigų plovimo skandalus, neigiamai paveikdamas valstybės reputaciją kovos su finansiniais nusikaltimais atžvilgiu, todėl nepalankios finansiniams nusikaltimams aplinkos kūrimas yra politinis prioritetas Estijoje[151]. Galimybė finansų įstaigoms bendradarbiauti tarpusavyje pinigų plovimo ir teroristų finansavimo prevencijos tikslais numatyta dar 2017m., perkeliant 4-ąją Pinigų Plovimo prevencijos Direktyvą į nacionalinę teisę. Estijos pinigų plovimo ir teroristų finansavimo prevencijos įstatyme (est. *Rahapesu ja terrorismi rahastamise tõkestamise seadus*) įtvirtinta kad:

1) įpareigoti subjektai gali bendradarbiauti tarpusavyje pinigų plovimo ir teroristų finansavimo prevencijos tikslu, perduodami jiems prieinamą informaciją ir atsakydami į kitų finansų įstaigų paklausimus per protingą terminą, laikydamiesi pareigų ir apribojimų kylančių iš kitų teisės aktų;

[149] SALV, *AML Bridge – building the new standard in AML/CTF*, White Paper, 2021, 7, https://salv.com/uploads/AML-Bridge-Estonia.pdf
[150] Financial Action Task Force (FATF), *supra note*, 6: 37.
[151] „Crypto bears the brunt of Estonia's war against dirty money", *Politico*, 2022-03-11, žiūrėta 2023-03-03, https://www.politico.eu/article/crypto-finance-estonia-dirty-money/

2) įpareigoti subjektai, prireikus, gali keistis informacija, kuri buvo surinkta deramo klientų patikrinimo metu, nepaisydami banko, verslo, profesinės paslapties, ar bet kokio kito konfidencialumo įsipareigojimo, jei tokiu keitimusi nepažeidžiamas geros valios principas[152].

Po AML Bridge projekto iniciavimo priimtos tik įstatymo pataisos, leidžiančios finansų įstaigoms keistis informacija, ne tik pinigų plovimo ir teroristų finansavimo, bet ir sukčiavimo prevencijos ir tarptautinių sankcijų įgyvendinimo tikslais.

Skirtingai nei Olandijoje, Estijoje įstatymo leidėjas nuėjo kiek kitu keliu ir įstatymuose finansų įstaigoms neįtvirtino pareigos, o tik galimybę keistis informacija tarpusavyje. Kai keitimasis yra savanoriškas, tinkamas teisėtas pagrindas tvarkyti asmens duomenis yra teisėtas interesas, tai reiškia pareiga vertinti taikomų priemonių proporcingumą paliekama pačioms finansų įstaigoms (žr. 2.3.4). Estijos įstatyme plačias galimybes keistis informacija riboja geros valios principo taikymas. Finansų įstaigos kiekvieną kartą teikdamos prašymus gauti informaciją ir perduodamos informaciją turėtų įvertinti, kiek toks prašymas yra būtinas ir atitinka vieną iš tikslų, kuriais leidžiama keistis informacija. Taip, visa atsakomybė, už galimus teisės į privatumą ir asmens duomenų apsaugą pažeidimus perkeliama finansų įstaigai.

Nors pradėjus naudoti AML Bridge jau pasiekta žymių rezultatų – ,,dešimt Estijos bankų inicijavo beveik 1 200 bendrų tyrimų pinigų plovimo, sukčiavimo ir tarptautinių sankcijų pažeidimo atvejuose, o nusikaltėlių kontroliuojamų sąskaitų nepasiekė milijonai eurų[153], pastebima jog interesų balanso svarstyklės Estijoje, politiniu sprendimu, pakrypo į kovos su finansiniais nusikaltimais pusę. Tokiomis aplinkybėmis, lieka neatsakytas klausimas ar Estijos modelis, teisės į privatumą ir asmens duomenų apsaugą požiūriu, yra tinkamas tik kol jo nevertino teismas?

3.1.3 Įstatymo pataisos Lietuvoje

Kylančios iniciatyvos ir naujas požiūris į kovą su finansiniais nusikaltimais neliko nuošalyje ir Lietuvoje. Tiesa, skirtingai nuo Olandijos, Lietuvoje pradedama ne nuo platformos kūrimo, o nuo įstatymo pataisų. Pasak Pinigų plovimo kompetencijų centro, duomenų keitimosi platforma galėtų būti sekantis žingsnis[154]. 2021m., ,,Pinigų plovimo kompetencijų centro ekspertų darbo grupė parengė Pinigų plovimo ir teroristų finansavimo prevencijos įstatymo pakeitimus,

[152] Riigikogu, ,,Rahapesu ja terrorismi rahastamise tõkestamise seadus“, 2017-11-27, 16 str. 2d., Riigi Teataja, žiūrėta 2024-02-22, https://www.riigiteataja.ee/en/eli/502122020004/consolide
[153] SALV, *supra note*, 149: 1.
[154] Struktūruotas interviu su Pinigų plovimo prevencijos kompetencijų centro teisėkūros iniciatyvų ir metodikos grupės koordinatore Greta Geneliene.

įteisinančius galimybę, finansų įstaigoms keistis informacija tarpusavyje“[155]. 2023-12-01 priimtas nutarimas, LR Seimui perduoti svarstyti įstatymo pakeitimo projekto variantą, kuris apima ne tik keitimąsi informacija kovoje su tradiciniais finansiniais nusikaltimais, kaip pinigų plovimas, teroristų finansavimas ir mokesčių slėpimas, bet ir sukčiavimą bei tarptautines sankcijas. 2024m. balandžio 18d. LR Seimas priėmė įstatymo pakeitimus: Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas papildyti 15^1 straipsniu.

1) „Finansų įstaigos, siekdamos įgyvendinti [...] pinigų plovimo ir (ar) teroristų finansavimo, įskaitant ir tarptautinių finansinių sankcijų ir (ar) ribojamųjų priemonių netinkamo įgyvendinimo, prevencijos priemones, turi teisę keistis informacija apie klientą ir jo atstovą, kliento naudos gavėją, kliento, kuris yra juridinis asmuo, nuosavybės ir kontrolės struktūroje dalyvaujančius asmenis ir (ar) pinigines operacijas ar sandorius, kai joms kyla įtarimų dėl galimo pinigų plovimo ir (ar) teroristų finansavimo, įskaitant galimą tarptautinių finansinių sankcijų ir (ar) ribojamųjų priemonių netinkamą įgyvendinimą [...].
2) Finansų įstaigos asmens duomenis tvarko vadovaudamosi [BDAR] ir keičiasi tik ta informacija apie klientą ir jo atstovą, kliento naudos gavėją, kliento, kuris yra juridinis asmuo, nuosavybės ir kontrolės struktūroje dalyvaujančius asmenis ir (ar) pinigines operacijas ar sandorius, kuri yra būtina siekiant įgyvendinti [...] nurodytus tikslus[156]“.

Kaip ir Estijoje, Lietuvoje finansų įstaigos dalinasi informacija tik kilus įtarimams, o pareiga įvertinti taikomų priemonių proporcingumą perkeliama finansų įstaigoms, nes dalinimasis vyksta savanoriškais pagrindais (finansų įstaigos turi teisę, bet ne pareigą dalintis informacija). Vertindama įstatymo pakeitimus, Lietuvos DPA (Valstybinė duomenų apsaugos inspekcija) neturėjo kitų pastabų, tik pabrėžė, kad siūlomu teisės aktu būtina aiškiai nustatyti asmens duomenų tvarkymo ribas ir sąlygas[157]. Tenkinant aiškumo ir tikslumo reikalavimą, įstatymu įvardijamas baigtinis sąrašas duomenų, kuriais galima keistis. Tiesa, šis įstatymo papildymas savo tikslu yra labai panašus į 2022m. LR Prezidento vetuotą įstatymą, kuriuo siekta kovoti su sukčiavimu (žr. 2.4.1). Tai rodo, kad per pastaruosius kelis metus, Lietuvoje, kovos su finansiniais nusikaltimais svarbai skiriama daugiau dėmesio. Sekantis žingsnis Lietuvai, po šio įstatymo priėmimo, yra tinkamos keitimosi duomenimis platformos įdiegimas.

[155] Pinigų plovimo prevencijos kompetencijų centras, Metinė ataskaita, 2021, 4, https://amlcenter.lt/wp-content/uploads/2022/08/PPPKC-Metine-veiklos-ataskaita-2021m..pdf
[156] „Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo Nr. VIII-275 2, 9, 10, 11, 15, 16, 21, 22, 23, 25, 29, 36, 39, 40, 48, 49 straipsnių pakeitimo ir Įstatymo papildymo 15-1, 15-2, 46-1 straipsniais įstatymas“, *supra note*, 17: 15^1str.
[157] Valstybinė duomenų apsaugos inspekcija, 2023-08-09, Nr. 2R (3.2.Mr.), „Dėl Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo ir susijusių įstatymų projektų“, TAIS, žiūrėta 2023-11-17, https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/6d9063a036af11eeb4b9a076396dcf81?positionInSearchResults=1&searchModelUUID=3106598b-305d-41f0-aaa1-448d37092fee

3.1.4 COSMIC Singapūre

Skirtingai nei ES valstybėse, Singapūre, keitimosi duomenimis tarp finansų įstaigų modelio ir platformos iniciatoriai buvo ne privatus sektorius, o Singapūro prudencinės priežiūros institucija. 2021 m. pradėjusi veikti COSMIC platforma sukurta taip, kad su finansiniais nusikaltimais nuo pat platformos veikimo pradžios būtų kovojama itin plačiu spektru. Visų pirma, be keitimosi informacija tarp finansų įstaigų, platforma apima ir keitimąsi informacija su teisėsauga, nes Singapūro FŽP turi tiesioginę prieigą prie COSMIC platformos ir gali naudotis platformoje esančia informacija atlikdamas savo analizę[158]. Be to, COSMIC platformoje dalinamasi ir duomenimis iki įtarimų kilimo ir duomenimis kilus įtarimams.

Keitimosi informacija loginė seka COSMIC platformoje sukonstruota taip, kad finansų įstaigoms nustatoma pareiga *prašyti, suteikti* arba *įspėti* priklausoma nuo to, koks rizikos lygis nustatomas atliekant deramą kliento patikrinimą.

1) *Prašyti.* Kai atliekant kliento patikrinimą finansų įstaiga pastebi rizikos požymių, , tačiau šie pastebėjimai nėra pakankami pareikšti įtarimą, finansų įstaiga, per COSMIC platformą gali kreiptis į kitas finansų įstaigas, kurios yra susijusios su tuo pačiu kliento, ar jo vykdomomis operacijomis.
2) *Suteikti*. Kai atliekant kliento rizikos vertinimą, finansų įstaiga pastebi požymių, rodančių didesnę kliento įsitraukimo į finansinius nusikaltimus riziką, nei pirmuoju atveju, finansų įstaiga turi veikti aktyviai ir informuoti kitas su klientu, ar jo vykdoma operacija susijusiais finansų įstaigas COSMIC platformoje.
3) *Įspėti.* Kai kliento veikla finansų įstaigoje įvertinama kaip labai rizikinga ir finansų įstaiga pasirenka pildyti STR ir nutraukti dalykinius santykius su klientu, finansų įstaiga turi užpildyti įspėjimą COSMIC platformoje. Įspėjimas matomas COSMIC platformos „juodajame sąraše“.

Platformai tik pradėjus veikti finansų įstaigos keičiasi duomenimis savanoriškai, tačiau planuojama, kad pareiga atsakyti į kitų finansų įstaigų prašymus, suteikti informaciją apie nustatytą aukštesnę riziką ir įspėti, kai supildomas STR ir nutraukiami santykiai, ateityje bus privaloma[159]. Už netinkamą naudojimąsi platformą ir pranešimų neteikimą nustačius riziką, finansų įstaigai bus skiriamos baudos.

Atsiribojant nuo išsamios teisę į privatumą ir asmens duomenų apsaugą saugančių teisės aktų Singapūre analizės, pastebėtina, kad bendrais bruožais Singapūro Asmens duomenų apsaugos įstatymas (angl. *Personal Data Protection Act*) panašus į BDAR. Jam tai pat būdingas

[158] Future of Financial Intelligence Sharing (FFIS) research program, *supra note* 8: 47.
[159] Financial Action Task Force (FATF), *supra note*, 6: 23.

eksteritorinis taikymas, be asmens sutikimo duomenis galima tvarkyti esant teisėtam interesui, jautrių asmens duomenų kategorijos neišskiriamos, bet teisiškai neįpareigojantys išaiškinimai rekomenduoja duomenų tvarkytojui atsižvelgti į tai, ar tvarkomi specialių kategorijų duomenys[160]. Iki COSMIC platformos sukūrimo, finansų įstaigoms kaip ir ES buvo leidžiama keistis informacija tik su tai pačiai grupei priklausančiomis kitomis finansų įstaigomis. Tačiau Singapūro asmens duomenų apsaugos įstatyme numatyta, kad kiti įstatymai gali turėti viršenybę prieš asmens duomenų apsaugos reikalavimus, todėl Singapūro Centrinis Bankas atlieka finansinių paslaugų ir rinkų įstatymo pataisas, siekiant reglamentuoti COSMIC platformos veikimą. Aiškinant keitimosi informacija COSMIC platformoje ribas, vertinamas ne asmens duomenų, o konfidencialios informacijos atskleidimas. Dalintis konfidencialia informacija leidžiama tik kovos su pinigų plovimo ir teroristų finansavimu tikslais ir tik modelio *įspėti, suteikti, prašyti* ribose. Pažeidus šias dalinimosi informacija nuostatas, finansų įstaigai skiriamos baudos. Tai pat, ketinama įstatymais numatyti apsaugą nuo civilinės atsakomybės už bet kokius konfidencialumo pareigos pažeidimus jei finansų įstaiga veikė atsargiai, rūpestingai ir gera valia.

3.1.5 Patriotinis Aktas, sekcija 314(b) JAV

Įstatymas leidžiantis finansų įstaigoms dalintis informacija tarpusavyje Jungtinėse Amerikos Valstijose (toliau JAV) priimtas dar 2001m. JAV Patriotinio Akto sekcijoje 314(b) numatyta, kad „[..] finansų įstaigos ar kiti įpareigoti subjektai gali dalintis informacija tarpusavyje, kai ši informacija apima fizinius, juridinius asmenis organizacijas ir valstybes įtariamus teroristų finansavimų ar pinigų plovimu. Finansų įstaiga perduodama ir gaudama informaciją pinigų plovimo ir teroristų finansavimo prevencijos tikslais, neatsako už konfidencialios informacijos atskleidimą pagal jokį kitą JAV teisės aktą, kitų valstybių teisės aktą [..], bet kokį teisinį susitarimą, asmeniui, kuris yra konfidencialios informacijos atskleidimo subjektas arba asmeniui, kurio tapatybė tai pat nustatoma atskleidžiant informaciją, išskyrus, kai toks informacijos perdavimas [..] pažeistų kitas Patriotinio Akto nuostatas“ [161].

Taigi Sekcija 314(b) numato „saugų uostą“ nuo civilinės atsakomybės, finansų įstaigoms savanoriškai dalinantis informacija siekiant nustatyti galimą pinigų plovimą ar teroristų finansavimą[162]. Tiesa, šis įstatymas taikomas tik finansų įstaigoms ir kitiems įpareigotiems

[160] DLA Piper, *Data Protection Laws of the World. Singapore*, žiūrėta 2023-12-20, https://www.dlapiperdataprotection.com/index.html?t=law&c=SG

[161] „Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001, 115 STAT, 272 Public Law 107–56—OCT. 26, 2001, sec. 314(b), žiūrėta 2024-02-22. https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[162] FinCEN, *Section 314(b) Fact Sheet*, 2020-12, 1, https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

subjektams prisijungusiems prie JAV FŽP – FinCEN (angl. *Financial Crime Enforcement Network*) valdomos kovos su pinigų plovimu ir teroristų finansavimu programos.

Norėdama dalintis informacija, taikant „saugaus uosto“ apsaugą, finansų įstaiga turi:

1) užregistruoti FinCEN ir išreikšti norą keistis informacija su kitomis finansų įstaigomis ir įpareigotais subjektais,
2) atskleisdama informacija privalo patikrinti, ar priimančioji įstaiga tai pat yra FinCEN tinklo narė,
3) gali keistis tik informacija kovos su finansiniais nusikaltimais tikslu,
4) turi įdiegusi pakankamas priemones ir procesus apsaugoti informacijos saugumą ir konfidencialumą atsakydama į užklausas ir jas teikdama[163].

FinCEN nenustato, ar keičiantis duomenimis turi būti naudojamas koks nors technologinis sprendimas, kaip apsikeitimo duomenimis platforma. Apsikeitimas informacija gali vykti net žodžiu ar raštu, jei finansų įstaiga sugeba užtikrinti informacijos saugumą ir konfidencialumą. Be to, valstybinės institucijos, įskaitant ir pačią FinCEN nėra įtraukiamos ir negali matyti informacijos, kuria dalinamasis, kol neužpildomas STR[164].

Nors JAV Patriotinis Aktas priimtas jau daugiau nei 20 metų, bet didžiąją dali šio laiko nepadaryta proveržio dalintis informacija. 2020m. FinCEN pateikiamoje statistikoje nurodoma, kad 2019m. pab. prie informacijos dalinimosi taikant Sekcijos 314(b) modelį buvo prisijungę 7000 finansų įstaigų, ar kitų įpareigotų subjektų, o su nuoroda į Sekciją 314(b) užpildyta 15 861 STR. Visgi, tai yra maži skaičiai lyginant su visais JAV veikiančių įpareigotų subjektų skaičiumi. FinCEN programoje dalyvauja tik kiek daugiau nei 12% įpareigotų subjektų ir vos 0.6% STR yra užpildomi su nuoroda į 314(b) Sekciją[165]. Viena iš vangaus dalyvavimo programoje priežasčių yra teisinis neužtikrintumas kokia informacija leidžiama dalintis. Pagal anksčiau pateiktus FinCEN išaiškinimus, buvo manoma, kad dalintis informacija galima tik kai finansų įstaigoje vykdoma operacija įtraukia lėšas įtariamas nusikalstama kilme, ar skirtas nusikaltimui vykdyti. 2020 m. FinCEN pateikė dar vieną išaiškinimą, kuriame atsakyta į klausimus, stabdžiusius finansų įstaigas nuo dalinimosi informacija. Dalindamosi informacija, finansų įstaigos neturi turėti tikslių žinių, kad kliento veikla susijusi su pinigų plovimu ar teroristų finansavimu, užtenka turėti pagrįstą pagrindą (įtarimą) apie galimą finansinių nusikaltimų vykdymą[166]. Tai pat, buvo manoma, kad

[163] Federal Deposit Insurance Corporation, *Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity*, 2023, FFIEC BSA/AML Examination Manual, 6, https://www.fdic.gov/news/financial-institution-letters/2023/fil23040e.pdf
[164] Financial Action Task Force (FATF), *supra note*, 56: 35.
[165] Jim, Richards, *314(b) Information Sharing – a Valuable, but Underutilized Tool*, 2020, RegTech Consulting, https://regtechconsulting.net/aml-regulations-and-enforcement-actions/314b-information-sharing-a-valuable-but-underutilized-tool/
[166] *FinCEN Expands Section 314(b) Information Sharing Safe Harbor*, Debevoise & Plimpton, 2020, 2, žiūrėta 2024-03-03. https://www.debevoise.com/insights/publications/2020/12/fincen-expands-section-314b-information

informacija galima dalintis, tik kai finansų įstaigoje vykdoma finansinė operacija. Naujausiame FinCEN išaiškinime nurodoma, kad galima dalintis ir informacija apie pavyzdžiui, bandymą sudaryti sandorį arba bandymą paskatinti kitus sudaryti sandorį. Tai pat, buvo išaiškinti, kad dalinimasis informacija pinigų plovimo prevencijos tikslais apima ne tik pinigų plovimą tiesiogiai, bet ir kitus su pinigų plovimu siejamus finansinius nusikaltimus (angl. *predicate offenses*), tai reiškia, kad galima dalintis informacija ir sukčiavimo, korupcijos ir kt. finansinių nusikaltimų atveju[167]. Po pakartotinio FinCEN išaiškinimo tikimasi proveržio dalyvaujant programoje, tačiau naujausia statistika dar nėra prieinama.

Vertinat kiek JAV sukurtas keitimosi duomenimis tarp finansų įstaigų modelis atitinka reikalavimus keliamus asmens duomenų apsaugai, turime pastebėti, kad dėl istoriškai susiklosčiusių aplinkybių, interesų balansas tarp teisės į privatumą ir kovos su finansiniais nusikaltimais, skatinant vyriausybei, smarkiai pakrypo į pastarosios pusę, po tokių įvykių kaip 9/11 išpuolis. Net gali būti sakoma, kad per pastaruosius 50 metų JAV, finansinio privatumo apsauga buvo tiesiog panaikinta[168]. JAV ir ES požiūris į privatumo apsaugą jau seniai išskyrė ir tolsta vienas nuo kito įgaunant pagreitį. Kartu išskiria ir požiūris į asmens duomenis kovoje su finansiniais nusikaltimais. JAV būdinga rinkti ypač didelius asmens duomenų kiekius juos analizuojant mažiau, kai tuo tarpu ES renkama mažiau duomenų, bet daugiau dėmesio skiriama išsamiai analizei[169]. Natūralu, kad vyraujant skirtingai teisinei-reguliacinei aplinkai JAV nekyla tų pačių problemų dėl teisės į privatumą ir asmens duomenų apsaugą reikalavimų, kurios kyla keičiantis informacija ES.

3.1.6 Duomenų keitimosi tarp finansų įstaigų modelių lyginamoji analizė

Tarpusavyje lyginant ES valstybių narių keitimosi informacija tarp finansų įstaigų modelius (žr. 1 priedas), galima pasakyti, kad modeliai, kuriuose keičiamasi duomenimis kilus įtarimams (Lietuva ir Estija) įgyvendinami lengviau (nesulaukė DPA pastabų), nei modeliai keičiantis duomenimis iki įtarimų kilimo (Olandija). Taip yra todėl, keitimasis duomenis po įtarimų kilimo, nesukelia masinio sekimo reiškinio, teismų, dažnu atveju, pripažįstamo kaip per didele apimtimi varžančio teisę į privatumą ir asmens duomenų apsaugą (žr. 2.4.2 sk.). Tačiau, siejant su 2-me sk. atlikta teisės į privatumą ir asmens duomenų apsaugą analize, keitimosi

[167] FinCEN, *supra note,* 162: 3.
[168] Nicolas, Anthony, „The Right to Financial Privacy: Crafting a Better Framework for Financial Privacy in the Digital Age“, *Policy Analysis* no. 945, (Washington, DC, 2023), 15, https://www.cato.org/sites/cato.org/files/2023-04/policy-analysis-945.pdf
[169] *Encouraging Public-Private Partnerships to Fight Financial Crime*, Atlantic Council, (Washington, DC, 2012), 9, https://www.files.ethz.ch/isn/155412/AC-TR%20Financial%20Crime%20Report%20-%20Final.pdf

duomenimis kilus įtarimui modeliuose, lieka svarbių neatsakytų klausimų, dėl asmens duomenų apsaugos reikalavimų.

1) Įstatymų leidėjas, finansų įstaigai, įtvirtina galimybę, o ne prievolę keistis duomenimis. Kai apsikeitimas asmens duomenimis yra savanoriškas, teisėtas pagrindas tvarkyti asmens duomenis pagal BDAR yra teisėtas interesas ir finansų įstaigoms kyla pareiga pačioms įvertinti keitimosi duomenimis proporcingumą ir būtinumą kiekvienu atveju (žr. 2.3.4 sk.). Dėl tenkančios atsakomybės ir gresiančių baudų, tokiu atveju, finansų įstaigų gali vengti naudotis galimybę keistis duomenimis.
2) Dalinantis duomenimis kilus įtarimams gali būti taikoma BDAR 23 str. išimtis, leidžianti neužtikrinti tam tikrų BDAR principų. Modeliuose neatsakyta į klausimą, būdingą visam kovos su finansiniais nusikaltimais reguliavimui. Koks teisės aktas saugo teisę į privatumą ir asmens duomenų apsaugą, kai BDAR dalinai nebetaikomas? (žr. 2.3.3).

Lyginant ES modelius su trečiųjų šalių modeliais (žr. 1 priedas), pastebėtina, kad ES modelių kūrimą dažniausiai inicijuoja pačios finansų įstaigos, kai tuo tarpu trečiosiose šalyse modelius kuria valstybės institucijos. Iš to sprendžiama, kad trečiosiose šalyse į kovoje su finansiniais nusikaltimais taikomų priemonių gerinimą žvelgiama kaip į valstybės, o ne tik finansų įstaigų, kurioms priskirtas „vartų saugotojų“ vaidmuo, uždavinį. Teisėsaugos ar kt. valstybės institucijų įtraukimas yra centrinis platformos veikimo elementas[170]. Singapūro modelis įdomus tuo, kad vienoje platformoje bandoma sujungti ir privataus-privataus ir privataus-valstybinio sektoriaus bendradarbiavimą; teisėsauga aktyviai įtraukiama į modelį. Svarbu, kad Singapūro modelyje dominuoja privalomas taikymas, tai rodo tvirtą įstatymų leidėjo užmojį kovoti su finansiniais nusikaltimais, nepaliekant išlygų. JAV modelis patrauklus paprastu įgyvendinimu ir itin plačiu spektru finansinių nusikaltimų, kuriuos galima tirti naudojant tą patį modelį, tačiau dėl skirtingai taikomų asmens duomenų apsaugos reikalavimų, JAV modelis yra nepritaikomas ES.

Svarbu paminėti, kad veikiančiuose modeliuose netinkamai įgyvendinus asmens duomenų apsaugai keliavimus reikalavimus, atsiranda ir kitos rizikos, siejamos su nepakankama teisės į privatumą apsauga. Tai *de-risking* praktikos ir iš jų kylanti finansinės atskirties grėsmė, bei informacijos nutekinimo rizika.

Finansinė atskirtis. Finansinė atskirtis, kylanti, kai finansų įstaigos nutraukia santykius su klientu yra sudėtingas klausimas, kuris negali būti paliekamas spręsti pačioms finansų įstaigoms, dėl rimtų pasekmių asmeniui (žr. 2.5) Finansų įstaiga turi užtikrintai žinoti, ar finansinė atskirtis, ar sustiprinta stebėsena yra įstatymo leidėjo valia tinkama ir pageidaujama priemonė, jei taip, kokiomis aplinkybėmis ir kokiam nustatytam rizikos lygiui galima taikyti sprendimą

[170] Future of Financial Intelligence Sharing (FFIS) research program, *supra note* 8: 18.

nutraukti santykius, atsižvelgiant į tai kai įtarimai pareiškiami ne teisminio proceso metu[171]. Olandijos ir JAV modelis sukurtas taip, kad viena finansų įstaiga neturėtų atskleisti kitoms finansų įstaigoms, jei priima sprendimą nutraukti santykius su klientu. Singapūro modelyje ši informacija prieinama kitoms finansų įstaigoms, tačiau draudžiama nutraukti santykius su klientu, neatlikus išsamaus, individualaus kliento vertinimo įstaigos viduje. Estijos modelyje netaikomos jokios kontrolės priemonės valdyti *de-risking* praktikai.

Informacijos nutekinimas. Anksčiau minėta, kad duomenų iki įtarimų kilimo ir duomenų kilus įtarimams takoskyra yra STR perdavimas (žr. 2.3.1). Kai užpildomas STR finansų įstaigai draudžiama atskleisti šį faktą klientui ir tretiesiems asmenims[172]. Draudimo tikslas išvengti bet kokio galimo trukdymo teisėsaugos tyrimui, kai įspėtas įtariamasis sunaikina įkalčius. FATF, (2022) duomenimis, kai kurie iniciatyvų dalyviai jautėsi neužtikrinti, ar informacijos atskleidimas kitai finansų įstaigai nelaikomas informacijos nutekinimu trečiajai šaliai. Be papildomų gairių iš įstatymo leidėjo, uždavinys dalinantis informacija nepažeisti draudimo atskleisti informaciją pasirodė keliantis iššūkių[173]. Visuose platformose (išskyrus JAV) duomenys yra šifruojami, ir atskleidžiami tik turint šifravimo raktą, tai apsaugo nuo duomenų nutekinimo trečiajai šaliai. Tai, kad kitos finansų įstaigos žino STR užpildymo faktą, iš esmės, nėra problema, nes visoms finansų įstaigoms taikomi konfidencialumo reikalavimai ir už informacijos nutekinimą skiriamos baudos. Tiesa, daugelyje modelių pasirenkama nuslėpti STR užpildymo faktą, saugantis labiau nuo *de-risking* problemos. Kyla klausimas, ar praktikoje gali pasitaikyti situacijų, kai vienai finansų įstaiga atskleidus duomenis, kita įstaiga atskleis duomenis klientui, ar trečiajai šaliai ar pan. nežinodama, kad duomenis perdavusioje finansų įstaigoje buvo užpildytas STR, ir ar tokiu atveju duomenis perdavusi, ar gavus finansų įstaiga galėtų būti laikoma atsakinga už informacijos nutekinimą? Autorės nuomone, platformų, kuriuose keičiamasi duomenimis kilus įtarimų, dalyviai turi aiškiai suprasti, kad kai keičiamasi duomenimis tarp finansų įstaigų, riba, nuo kurios duomenys turi būti laikomi duomenimis kilus įtarimų ir pradedamas taikyti draudimas atskleisti informaciją, yra nebe STR perdavimas, o pats apsikeitimas informacija su kita finansų įstaiga, kai įtarimai išreiškiami už finansų įstaigos, kurioje jie kilo ribų. Papildomos gairės iš įstatymo leidėjo padėtų užtikrinti, kad visos finansų įstaigos laikytųsi šios nuostatos.

[171] Future of Financial Intelligence Sharing (FFIS) research program, *supra note* 8: 76-77.
[172] Europos Parlamento ir Tarybos Direktyva (ES) 2015/849, *supra note*, 31: 39 str. 1d.
[173] Financial Action Task Force (FATF), *supra note*, 6: 46.

3.2 Keitimasis informacija su teisėsauga

Apie keitimąsi informacija tarp privataus ir valstybinio sektoriaus pradėta galvoti anksčiau, nei apie 3.1 sk. analizuotą keitimąsi informacija privačiame sektoriuje. Po 2015 ir 2016 m. teroristinių išpuolių Paryžiuje ir Briuselyje, daugiau nei 20 valstybių nusprendė išvysti kovos su finansiniais nusikaltimais modelius, suvienijančius teisėsaugą, reguliatorius ir finansų įstaigas siekiant bendro tikslo – aptikti ir užkirsti kelią finansiniams nusikaltimams[174]. Privataus ir valstybinio sektoriaus bendradarbiavimas paprastai apima keitimąsi strategine ir/arba taktine informacija. Strateginis bendradarbiavimo metu, kovą su finansiniais nusikaltimais vykdančios institucijos keičiasi tipologijomis, naujomis žiniomis apie nusikaltėlių veikimo būdus, aktualias grėsmes ir pan. Toks apsikeitimas informacija nedaro jokio poveikio teisei į privatumą ir asmens duomenų apsaugą, todėl toliau šiame magistro baigiamajame darbe nenagrinėjamas.

Keitimasis taktine informacija reiškia operatyvinės teisėsaugos informacijos perdavimą finansų įstaigoms, prašant vykdyti įtariamųjų, ar kitų dominančių asmenų, finansinio elgesio stebėseną. Paprastai dalijantis tokia informacija, pasidalijama „teisėsaugos taikinių“ asmens duomenimis, todėl neišvengiamai kyla klausimų dėl teisės į privatumą ir asmens duomenų apsaugą užtikrinimo. Iš kovos su finansiniais nusikaltimais perspektyvos, keitimasis informacija tarp teisėsaugos ir finansų įstaigų yra naudingas abiem pusėms: finansų įstaigos paremia teisėsaugos institucijas jų vykdomuose ikiteisminiuose tyrimuose, o teisėsaugos institucijos padeda finansų įstaigoms vykdyti finansinių nusikaltimų prevenciją, nes pačioms finansų įstaigoms trūksta kriminalistinės patirties, nustatant finansinių nusikaltimų atvejus. Iš teisės privatumą ir asmens duomenų apsaugą perspektyvos, kyla klausimas, ar privačiam sektoriui, t.y. finansų įstaigoms, gali būti patikėtos teisėsaugos užduotys?

Dr. Benjamin Vogel pastebi, kad vyrauja du skirtingi požiūriai, į finansų įstaigoms priskiriamą tikslą, kovoje su finansiniais nusikaltimais. Vienu požiūriu, sutelkiamas dėmesys į įpareigotųjų subjektų, kaip „vartų saugotojų“, vaidmenį. Akcentuojamas tikslas – užkirsti kelią nusikalstamu būdu įgyto turto patekimui į teisėtą ekonomiką[175]. Kitas požiūris siejamas su *follow the money* tyrimo metodo pritaikymu, valstybei kovojant su finansiniais nusikaltimais. Finansų įstaigos matomos kaip finansinės žvalgybos šaltinis ir pasitelkiamos, kaip instrumentas valstybės vykdomam stebėjimui[176]. Keitimosi informacija tarp finansų įstaigų ir teisėsaugos modeliai atliepia, būtent, į antrojo požiūrio tikslus.

---

[174] Nick, J., Maxwell, David, Artingstall, „The Role of Financial Information-Sharing Partnerships in the Disruption of Crime“, Occasional Paper, 2017, Royal United Services Institute, X, https://static.rusi.org/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwwell_artingstall_web_4.2.pdf

[175] Vogel, *supra note,* 9: 11.

[176] *Ibid.*

3.2.1 Keitimosi informacija su teisėsauga modeliai

Patriotinis Aktas, sekcija 314(a) JAV. JAV, dalinimasis operatyvine-taktine informacija su finansų įstaigomis leidžiamas nuo 2001m. pagal Patriotinio Akto, Sekcijos 114 (a) dalį, kur numatyta, kad „[...] specialiu reguliatoriaus ar teisėsaugos institucijų prašymu gali būti dalinamasi informacija apie asmenis, įmones, organizacijas įsitraukusiais į teroristinę ar pinigų plovimo veiklą, [...] esant įtarimui, grindžiamam patikimais įrodymais. [...]. Finansų įstaiga turi paskirti atsakingą asmenį/-is, kuris priimtų informaciją iš teisėsaugos ir stebėtų sekamų subjektų finansines operacijas. Tai pat, numatytas apribojimas, kad iš teisėsaugos gauta informacija, finansų įstaigoje, negali būti panaudota jokiu kitu tikslu, išskyrus nustatyti raportuotiną veiklą“[177]. 2015m., FinCEN nusprendė patobulinti keitimosi informaciją mechanizmą, labiau jį priartinant prie konkrečių tyrimų ir reguliuojant prašomos informacijos srautą. Kas 6 savaites, FinCEN, glaudžiai bendradarbiaujant su teisėsauga, kviečia tikslines finansų įstaigas į susitikimus, kur paprašoma surinkti informaciją konkretiems tyrimams. Per metus taip atliekama apie 10 tyrimų[178].

JMLIT, Jungtinėje Karalystėje. JMLIT modelis sukurtas ir teisinė bazė jam priimta Jungtinei Karalystei dar būnant ES nare, 2014m., nors rimtesnis dėmesys į keitimosi informacija su teisėsauga modelių potencialą kovoti su finansiniais nusikaltimais, Europoje atkreiptas po 2015m. teroristinių išpuolių. JMLIT modelio tikslas – padėti finansų įstaigoms ir su finansiniais nusikaltimais kovojančiomis valstybinėms institucijomis apsikeisti duomenimis, palengvinant joms tenkančias žvalgybos ir analizės užduotis. JMLIT struktūroje veikia operatyvinė grupė, kurioje dalinamasi operatyvine informacija apie veiką, susijusią su finansiniais nusikaltimais. Grupė susideda iš teisėsaugos, FŽP ir finansų įstaigų atstovų. Teisinė bazė informacijos mainams yra *Crime and Courts Act 2013*, 7 sekcijoje įtvirtinta galimybė .„atskleisti informaciją teisėsaugai, jei toks atskleidimas vykdomas siekiant tikslų, reikalingų teisėsaugos funkcijoms atlikti[179]“. Per pirmuosius veikimo metus, po pilotinės versijos testavimo (2016-2017m.), naudojant JMLIT atlikti ikiteisminiai tyrimai, kurių metu areštuota 7 mln. svarų sterlingų įtariamai nusikalstamu būdų įgytų lėšų[180].

Fintell Alliance Olandijoje. 2019m., Olandijos FŽP (administracinio tipo) sujungė teisėsaugą ir finansų įstaigas Fintell Alliance iniciatyvai. Dalinimuisi taktine operatyvine informacija paskirta viena platforma. Metai po iniciatyvos pradžios, teisėsaugos prašymu, FŽP

[177] USA Patriot Act, *supra note,* 161: sec. 314(a).
[178] Maxwell, Artingstall, *supra note*, 175: 15.
[179] „Crime and Courts Act 2013“, 2013 c.22, sec. 7. Legislation.gov.uk, žiūrėta 2024-03-03. https://www.legislation.gov.uk/ukpga/2013/22/section/7
[180] Maxwell, Artingstall, *op. cit*., 175.

pasidalino informacija su Fintell Alliance platformoje dalyvaujančiais bankais ir atliko jungtinę analizę, kurios metu pavyko aptikti ryšius ir sąsajas, atkleidusias itin didelio mąsto pinigų plovimo tinklą, bei įspėti kitas finansų įstaigas, aptarnaujančias su tinklo nariais siejamas sąskaitas, imtis prevencinių priemonių[181].

SAMLIT Švedijoje. 2020m. 5 didžiausi Švedijos bankai pradėjo bendradarbiauti su teisėsauga pinigų plovimo prevencijos ir teroristų finansavimų srityje, siekdami efektyviau dalintis informacija. SAMLIT suskirstyta į tris darbo grupes. Viena grupė keičiasi taktine-operatyvine informacija, kita grupė rūpinasi kovos su finansiniais nusikaltimais strategija, trečia grupė sprendžia teisinius klausimus. Kiekvienoje grupėje dalyvauja ir FŽP. Finansų įstaigos su operatyvine grupe keičiasi informacija susijusia su konkrečiais įtariamaisiais, prieš kuriuos vykdoma kriminalinė žvalgyba. Per du metus nuo SAMLIT iniciatyvos pradžios, su finansų įstaigų pagalba, sėkmingai surinkti įrodymai 9 bylose ir pradėti teisminiai procesai[182].

Lyginant keitimosi informacija su teisėsauga modelius tarpusavyje (žr. 2 priedas), visuose nagrinėtose keitimosi informacija modeliuose dalyvauja ne tik teisėsaugos institucijos ir finansų įstaigos, bet ir FŽP, neatsižvelgiant į jų statusą. Tai reiškia, kad šie modeliai apjungia visas kovos su finansiniais nusikaltimais grandis. Visi nagrinėti modeliai, pasiekė reikšmingų rezultatų kovoje su finansiniais nusikaltimais. ES veikiantys modeliai yra labai panašūs savo struktūra, sekant JK modeliu, kuris buvo pirmasis ES dar iki *Brexit*. Pastebima, kad ES modelių veikimas nėra sureguliuotas įstatymais, kai tuo tarpu trečiosiose šalyse, keitimasis informacija tarp finansų įstaigų ir teisėsaugos, numatytas įstatymo. Tai pat, trečiosiose šalyse prie modelio prijungtos visos finansų įstaigos, kai dalyvavimas ES yra savanoriškas.

3.2.2 Keitimosi informacija su teisėsauga modeliai ir asmens duomenų apsauga

Įgyvendinant keitimosi informacija su teisėsauga modelius, finansų įstaigos išeina iš joms priskirtų „vartų saugotojų“ ribų, ir tampa žvalgybinės informacijos rinkimo šaltiniu. EDPB nepritaria operatyvinių teisėsaugos duomenų dalinimuisi su FŽP ir finansų įstaigomis. Nes FŽP ir finansų įstaigų įsitraukimas į ikiteisminius tyrimus, viršija Sąjungoje jiems patikėtas užduotis – vykdant finansinių nusikaltimų prevenciją, saugoti teisėtą ekonomiką, nuo nusikalstamu būdu įgytų lėšų patekimo (žr. 2.5). Nepaisant to, keitimosi informacija modeliai, ES ir toliau veikia,

[181] Financial Action Task Force (FATF), Anti-money laundering and counter-terrorist financing measures – The Netherlands, (Paris, 2022), 59, https://www.fatf-gafi.org/en/publications/mutualevaluations/documents/mer-netherlands-2022.html

[182] The Swedish police Authority, *The Financial Intelligence Unit Annual Report 2022*, 2023, 22, https://polisen.se/siteassets/dokument/polisens-arsredovisning/fipos-arsrapport/financial-intelligence-unit-annual-report-2022.pdf

savanoriško dalinimosi principu, atnešdami teigiamų rezultatų kovoje su finansiniais nusikaltimais.

Tai nėra pirmas kartas, kada EDPB nuomonė paliekama nuošalyje, siekiant rezultatų kovoje su finansiniais nusikaltimais. 2016m., siekiant stiprinti FŽP ir teisėsaugos bendradarbiavimą, FŽP keitimosi informacija tinklas FIU.net buvo perkeltas administruoti Europolui. 2017-2018m. pranešime EDPS įspėjo apie iššūkius, kylančius dėl asmens duomenų apsaugos[183]. Tąkart, į tai nebuvo atsižvelgta. Metais vėliau, EDPS paskelbė, kad Europolui neturėtų būti leidžiama tvarkyti duomenis apie asmenis, kurie pagal nacionalinius baudžiamuosius įstatymus nepriskiriami „įtariamiesiems“. Europolo bendradarbiavimo valdyba kreipėsi į priežiūros pareigūną, prašydama pateikti nuomonę, išaiškinančią Europolo įgaliojimus. Nustatyta, kad pagal ES, ar nacionalinę teisę, nėra vieningai suderinto sąvokos „įtariamasis“ apibrėžimo ir FIU.net veikimas Europole buvo galutinai sustabdytas[184].

Tam, kad istorija nepasikartotų, reikalingas teisinis aiškumas ir nedviprasmiškas įstatymo leidėjo sprendimas, keitimosi informacija modelių ateities Sąjungoje klausimu. Panašu, kad modelius įgyvendinančiose valstybėse neoficialiai (neįtvirtinta įstatymais) einama prie dalies teisėsaugos pareigų perdavimo privačiam sektoriui. Susiklosčiusią situaciją labai tiksliai apibūdina mintis, kad „kai valstybėse neoficialiai pripažįstama ir esamos teisinės sistemos trūkumams ištaisyti neoficialiai naudojama savanoriška praktika, tai paprastai rodo, kad anksčiau ar vėliau reikės tobulinti teisinę sistemą“[185].

Apibendrinant, dalinimosi informacija tarp finansų įstaigų modeliai pademonstravo sėkmingus rezultatus kovoje su finansiniais nusikaltimais. Nagrinėtų ES valstybių nacionalinėje teisėje, buvo įtvirtinta galimybė finansų įstaigoms dalintis informacija tarpusavyje, kilus įtarimams. Tačiau „mūšis“ dėl teisės į privatumą užtikrinimo neaplenkė ir šių iniciatyvų[186]. Pavyzdžiui Olandijoje, kur keitimosi informacija modelis apima ir keitimaisi informacija iki įtarimų kilimo, įstatymo pakeitimų svarstymas sustabdytas po 2022 m. pab. paskelbto nuosprendžio *WM and Sovim SA vs. Luxembourg Business Registers* byloje.

Keitimasis duomenimis kilus įtarimams, tai pat nėra įtvirtintas harmonizuotai ES lygmeniu. Kol kas lieka neišspręstų klausimų, reikalaujančių aktyvaus įstatymų leidėjo įsikišimo:

---

[183] Mouzakiti, *supra note*, 19: 372.
[184] Jon Rees, Sanne, Wass, *GDPR clash leaves Europol banned from hosting financial crime computer network. S&P Global Market Intelligence,* 2020, žiūrėta 2024-03-03, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/gdp r-clash-leaves-europol-banned-from-hosting-financial-crime-computer-network-57121862
[185] Vogel, *supra note*, 9: 7.
[186] *Special Contributor Forecast: Data Privacy, Protection Challenges and Risk Management Concerns Will Lead AML Compliance Direction in 2023*, ACFCS, žiūrėta 2024-02-21, https://www.acfcs.org/acfcs-special-contributor-forecast-data-privacy-protection-challenges-and-risk-management-concerns-will-lead-aml-compliance-direction-in-2023

finansų įstaigoms perkeliama atsakomybė už interesų pusiausvyros išlaikymą; nenustatyta, koks duomenų apsaugos standartas taikomas, kai duomenimis kilus įtarimų nebetaikomas BDAR; neaiški yra įstatymų leidėjo valia, dėl įtarimų keliančių asmenų pašalinimo iš finansų sistemos (*de-risking*); nėra nuostatų, dėl tinkamo pareigos neatskleisti informacijos vykdymo.

Keičiantis duomenims tarp teisėsaugos institucijų ir finansų įstaigų, finansų įstaigoms perduodama dalis teisėsaugos pareigų. Taip, finansų įstaigos išeina iš tradiciškai joms priskiriamo „vartų saugotojų“ vaidmens ir tampa žvalgybinės informacijos rinkimo šaltiniu. Visose nagrinėtuose valstybėse, įgyvendinusiose keitimosi informacija tarp finansų įstaigų ir teisėsaugos modelius, pasiekta daug žadančių rezultatų, kovojant su finansiniais nusikaltimais. Nagrinėtuose ES valstybėse, skirtingai nei trečiosiose šalyse, modelių veikimas nėra sureguliuotas įstatymais, o finansų įstaigos jungiasi savanoriškais pagrindais. Savanoriškos praktikos taikymas signalizuoja apie reikalingus pokyčius įstatyminiame reguliavime. EDBP nepritaria teisėsaugos pareigų perdavimu privačiam sektoriui, nes taip valstybė galėtų perdėtai kištis į asmens gyvenimą.

.

IŠVADOS

1. Keitimosi informacija kovoje su finansiniais nusikaltimais ir asmens duomenų apsaugos reikalavimų analizėje atskleista, kad šių dienų finansinių nusikaltimų prevencijos sistema nebėra pakankama kovojant su finansiniais nusikaltimais. Tarp valstybių sienų ir finansų įstaigų sukonstruoti nusikaltėlių tinklai, gali būti išnarplioti tik kovą su finansiniais nusikaltimais įgyvendinantiems subjektams išeinant už įstaigos/valstybės ribų, efektyviai bendradarbiaujant ir keičiantis informacija visose, kovą su finansiniais nusikaltimais vykdančių institucijų grandyse. Šiai dienai, Europos Sąjungoje nėra vienodo reguliavimo, įteisinančio tokius informacijos mainus. Įstatymo leidėjui, vėluojant nustatyti bendrą politiką ir teisinę-reguliacinę aplinką, kai kuriuose valstybės narėse kilo privataus ir valstybinio sektoriaus savanoriškos iniciatyvos keistis duomenimis. Lygiagrečiai, ši tendencija stebima ir ES nepriklausančiose valstybėse, stambiuose pasaulio finansų centruose. Pradėti diegti keitimosi informacija modeliai jau pademonstravo sėkmingus rezultatus kovojant su finansiniais nusikaltimais. Tačiau, liko iki galo neišspręstų klausimų dėl pakankamo teisės į privatumą ir asmens duomenų apsaugą užtikrinimo.

2. Teisė į privatumą ir asmens duomenų apsaugą saugo nuo perdėto valstybės kišimosi į privatų asmenų gyvenimą. Tačiau, ši teisė nėra absoliuti ir gali būti suvaržyta. Tam, kad suvaržymas būtų teisėtas, kovoje su finansiniais nusikaltimais taikomos priemonės turi būti būtinai reikalingos šios kovos tikslams pasiekti. Masinis sekimas, kai kovos su finansiniais nusikaltimais priemonės taikomos visiems asmenims, jų nediferencijuojant (nesant įtarimų), ir teisėsaugos pareigų perdavimas privačiam sektoriui, kovojant su finansiniais nusikaltimais kelia svariausių abejonių, dėl suderinamumo su teise į privatumą ir asmens duomenų apsaugą.

3. *Dėl keitimosi informacija tarp finansų įstaigų (*angl. *private-private partnership).* Finansų įstaigos negali keistis informacija **iki įtarimų kilimo**, nes taikant kovos su finansiniais nusikaltimais priemonę bendrai visiems asmenims, jų nediferencijuojant, sukeliamas masinis sekimas, neproporcingai varžantis teisę į privatumą ir asmens duomenų apsaugą.

Finansų įstaigos gali keistis informacija **kilus įtarimams**, tačiau:

valstybės narės nacionalinėje teisėje turi būti įtvirtinta ne galimybė, o pareiga dalintis informacija, nes asmens duomenų perdavimo proporcingumo, saugant asmenes teisę į privatumą klausimas negali būti paliktas finansų įstaigos nuožiūrai, atsižvelgiant į tai, kad išlaikyti tinkamą balansą ne visada pavyksta net įstatymo leidėjui. Įstatymo leidėjas turi duoti aiškiais ir griežtas nuostatas kaip keičiantis informacija turi būti valdomos finansinės atskirties ir informacijos nutekinimo rizikos.

4. *Dėl keitimosi informacija tarp finansų įstaigų ir teisėsaugos (*angl. *private-private partnership)*. Keitimasis operatyvine informacija tarp teisėsaugos su finansų įstaigomis, kai teisėsauga nurodo finansų įstaigai stebėti įtariamųjų finansines operacijas sunkiai suderinimas su teise į privatumą ir asmens duomenų apsaugą, nes teisėsaugos pareigų perdavimas finansų įstaigoms viršija Sąjungoje joms patikėtas užduotis, o asmuo neapsaugomas nuo perdėto valstybės kišimosi į privatų gyvenimą. Vis dėl to, informacija būtų galima keistis, įstatymo leidėjui išreiškus aiškią poziciją, kad dabartinių kovos su finansiniais nusikaltimais priemonių nepakanka ir finansų įstaigos, išeidamos iš tradiciškai joms priskiriamo „vartų saugotojų“ vaidmens, tampa žvalgybinės informacijos rinkimo šaltiniu, o tokia priemonė yra būtinai reikalinga teisėsaugos funkcijoms atlikti (Jungtinės Karalystės modelis). Tai pat, saugant teisę į privatumą ir asmens duomenų apsaugą reikalingas diferencijavimas, todėl priemonė turėtų būti taikoma tik asmenims, prieš kuriuos vykdoma kriminalinė žvalgyba (Švedijos modelis).

PASIŪLYMAI

1. Keitimosi informacija tarp finansų įstaigų modelis turi būti kuriamas harmonizuotai ES lygmeniu, nustatant aiškius reikalavimus ir vienodą teisinę bazę visose valstybėse narėse. Harmonizuoto modelio sukūrimas leistų perduoti informacija tarp valstybių sienų, o finansų įstaigos turėtų tikslias ir aiškias nuostatas. Tai leistų plačiu mastu kovoti su finansiniais nusikaltimais.

2. Lietuvoje jau priimtas įstatymas leidžiantis finansų įstaigoms keistis informacija tarpusavyje ir sekantis etapas yra tinkamo duomenų keitimosi modelio/techninės platformos parengimas. Siūloma, vadovaujantis gerąją kitų šalių praktika, kontroliuoti finansinės atskirties ir informacijos nutekinimo rizikas. Finansų įstaigoms turėti būti neleista nutraukti santykių su klientu. remiantis kitos finansų įstaigos sprendimu (Singapūro modelio geroji praktika), o dalinantis informacija tarpusavyje turėtų būti taikomas analogiškas draudimas atskleisti informaciją, kaip ir STR perdavimo atveju. Tai pat, ateityje būtų verta įtvirtinti ne pareigą, o prievolę dalintis informacija nacionaliniuose įstatymuose, taip priemonės proporcingumo įvertinimo naštą iš finansų įstaigos perkeliant įstatymo leidėjui.

3. Lietuvoje taip pat būtų galima kurti darbo grupes iš teisėsaugos FŽP ir finansų įstaigų specialistų ir pradėti keistis taktine informacija tarp finansų įstaigų ir teisėsaugos, apsibrėžiant, kad tokia priemonė yra būtinai reikalinga teisėsaugos funkcijoms atlikti, ir apribojant taikymą tik asmenims, prieš kuriuos vykdoma kriminalinė žvalgyba.

LITERATŪROS SĄRAŠAS

Teisės aktai:

1. „European Convention on Human Rights“. 1950. Last reviewed on 24/03/2017. EUR-LEX. Žiūrėta 2024-01-26. https://www.echr.coe.int/documents/d/echr/convention_ENG
2. Europos Parlamento ir Tarybos Direktyva (ES) 2015/849 2015 m. gegužės 20d. „Dėl finansų sistemos naudojimo pinigu plovimui ar teroristu finansavimui prevencijos, kuria iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 ir panaikinama Europos Parlamento ir Tarybos direktyva 2005/60/EB bei Komisijos direktyva 2006/70/EB“. EUR-LEX. Žiūrėta 2023-01-26. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32015L0849
3. Europos Parlamento ir Tarybos Direktyva (ES) 2016/680. 2016 m. balandžio 27d. „ Dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR“. EUR-LEX. Žiūrėta 2023-01-26. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016L0680
4. Europos Parlamento ir Tarybos Direktyva (ES) 2018/843, 2018 m. gegužės 30d. „kuria iš dalies keičiama Direktyva (ES) 2015/849 Dėl finansų sistemos naudojimo pinigų plovimui ar teroristų finansavimui prevencijos ir iš dalies keičiamos Direktyvos 2009/138/EB ir 2013/36/ES“. EUR-LEX. Žiūrėta 2023-01-26. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32018L0843
5. Europos Parlamento ir Tarybos Direktyva (ES) 2019/1153, 2019 m. birželio 20d. „kuria nustatomos taisyklės dėl paprastesnio finansinės ir kitos informacijos naudojimo tam tikrų nusikalstamų veikų prevencijos, nustatymo, tyrimo ir baudžiamojo persekiojimo už jas tikslais ir kuria panaikinamas Tarybos sprendimas 2000/642/TVR“. EUR-LEX. Žiūrėta 2023-01-26. https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32019L1153
6. Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679, 2016 m. balandžio 27 d. „Dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“. EUR-LEX. Žiūrėta 2023-01-26. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex%3A32016R0679

7. „Europos Sąjungos pagrindinių teisių Chartija“. 2000m. Publikuota 2012-10-26. EUR-LEX. Žiūrėta 2024-01-26. https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX:12012P/TXT
8. „Crime and Courts Act 2013“. 2013 c.22. Legislation.gov.uk. Žiūrėta 2024-03-03. https://www.legislation.gov.uk/ukpga/2013/22/section/7
9. „Europos Sąjungos Sutartis“. 1957 m., suvestinė redakcija 2012-10-26. EUR-LEX. Žiūrėta 2023-01-26. https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=celex%3A12012E%2FTXT
10. „Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo Nr. VIII-275 2, 9, 10, 11, 15, 16, 21, 22, 23, 25, 29, 36, 39, 40, 48, 49 straipsnių pakeitimo ir Įstatymo papildymo 15-1, 15-2, 46-1 straipsniais įstatymas“, (TAR, 2024-04-25, Nr. 2024-07537). INFOLEX. Žiūrėta 2024-04-28. https://www-infolex-lt.skaitykla.mruni.eu/ta/941993#Xfcc32c158c44476a8f6b690995d3a024
11. Lietuvos Respublikos Prezidento Dekretas. „Dėl Lietuvos Respublikos Mokėjimų įstatymo NR. VIII-1370 2, 3, 54, 76 straipsnių ir priedo pakeitimo įstatymo NR.XIV-1478 grąžinimo Lietuvos Respublikos Seimui pakartotinai svarstyti“. 2022 m. lapkričio 17 d. INFOLEX. Žiūrėta 2024-01-27. https://www.infolex.lt/ta/810191
12. Riigikogu. „Rahapesu ja terrorismi rahastamise tõkestamise seadus“. 2017-11-27. Riigi Teataja. Žiūrėta 2024-02-22. https://www.riigiteataja.ee/en/eli/502122020004/consolide
13. „Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001”. 115 STAT, 272 Public Law 107–56—OCT. 26, 2001. Žiūrėta 2024-02-22. https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

***Soft law*:**

14. Article 29 Data protection Working Party. „Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data“. 2015 m. gruodžio 1d. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf
15. Article 29 Data protection Working Party. „Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC“. 2014m. balandžio 9d. https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate-interests/files/20141126_overview_relating_to_consultation_on_opinion_legitimate_interest_.pdf

16. Article 29 Data protection Working Party. „Opinion 14/2011on data protection issues related to the prevention of money laundering and terrorist financing: Annex the working party on the protection of individuals with regard to the processing of personal data“. 2011 m. birželio 13d. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp186_en_annex.pdf
17. Autoriteit Persoonsgegevens. „ Advies consultatieversie voorstel voor de wet plan van aanpak witwassen“. 2020 kovo 10d. https://autoriteitpersoonsgegevens.nl/uploads/imported/advies_wet_plan_van_aanpak_witwassen.pdf
18. European Banking Authority. „Opinion of the European Banking Authority on 'de-risking'“. 2022 m. sausio 5d. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf
19. European Data Protection Board. „Letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations“. 2023 m. kovo 28d. Briuselis. Žiūrėta 2024-01-27. https://edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0015_aml_cft_ep_en.pdf
20. European Data Protection Supervisor. „ Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC“. 2017 m. vasario 2d. https://www.parlament.gv.at/dokument/XXV/EU/131392/imfname_10692002.pdf
21. European Data Protection Supervisor. „Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data“. 2019 m. gruodžio 19d. https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf
22. European Data Protection Supervisor. „Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals“. 2021 m. rugsėjo 22d. https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf
23. European Data Protection Supervisor. „Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing“. 2020 m. liepos 23d. https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf
24. Financial Action Task Force (FATF). *FATF 40 Recommendations*. (2003). https://www.fatf-gafi.org/content/dam/fatfgafi/recommendations/FATF%20Recommendations%202003.pdf

25. Financial Action Task Force (FATF). *Anti-money laundering and counter-terrorist financing measures – The Netherlands*. Paris, 2022. https://www.fatf-gafi.org/en/publications/mutualevaluations/documents/mer-netherlands-2022.html
26. Financial Action Task Force (FATF). *International standards on combating money laundering and the financing of terrorism & proliferation.* Paris, 2023. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
27. Financial Action Task Force (FATF). *Partnering in the fight against financial crime data protection, technology and private sector information sharing.* Paris, 2022. https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html
28. Financial Action Task Force (FATF). *Private sector information sharing.* Paris, 2017. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf
29. Valstybinė duomenų apsaugos inspekcija. 2023-08-09, Nr. 2R (3.2.Mr.). „Dėl Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymo ir susijusių įstatymų projektų“. TAIS. Žiūrėta 2023-11-17. https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/6d9063a036af11eeb4b9a076396dcf81?positionInSearchResults=1&searchModelUUID=3106598b-305d-41f0-aaa1-448d37092fee

Teisės aktų projektai:

30. Pasiūlymas. Europos Parlamento ir Tarybos Direktyva, 2021 m. liepos 20d. „Dėl mechanizmų, kuriuos turi įdiegti valstybės narės finansų sistemos naudojimo pinigų plovimui ar terorizmo finansavimui prevencijos tikslais, kuria panaikinama Direktyva (ES) 2015/84. EUR-LEX. Žiūrėta 2024-01-26. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423
31. Pasiūlymas. Europos Parlamento ir Tarybos Reglamentas 2021 m. liepos 20d. „Dėl finansų sistemos naudojimo pinigų plovimui ar terorizmo finansavimui prevencijos“. Tarpinstitucinė versija Tarybos svarstymui. 15517/22. 2022m. gruodžio 5d. Žiūrėta 2024-01-26. https:// data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf
32. Tweede Kamer der Staten-Generaal 2022-2023, 36 228 Nr.2 „ Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme in verband met het verbod op contante betalingen voor goederen vanaf 3.000 euro en het uitbreiden van de mogelijkheden voor informatie-uitwisseling ten behoeve van de poortwachtersfunctie (Wet plan van aanpak witwassen)“. Tweede Kamer. Žiūrėta 2023-02-22. https://www.tweedekamer.nl/downloads/document?id=2022D43319

Teismų praktika:

33. Europos Sąjungos Teisingumo Teismas. „Sprendimas Sujungtose bylose WM (C-37/20) ir Sovim SA (C-601/20) prieš Luxembourg Business Registers“. 2022 m. lapkričio 22d. InfoCuria. Žiūrėta 2024-01-27. https://curia.europa.eu/juris/document/document.jsf?text=&docid=268059&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=311534
34. Europos Sąjungos Teisingumo Teismas. „Sprendimas Sujungtose bylose Tele2 Sverige AB (C 203/15) prieš Post och telestyrelsen Secretary of State for the Home Department (C 698/15) prieš Tom Watson, Peter Brice, Geoffrey Lewis“. 2016 m. gruodžio 21 d. InfoCuria. Žiūrėta 2024-01-27. https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=5995909
35. Europos Sąjungos Teisingumo Teismas. „Sprendimas Sujungtose bylose Digital Rights Ireland Ltd (C-293/12) prieš Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Airiją,The Attorney General, ir Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl ir kt“. 2014 m. balandžio 8d. EUR-LEX. Žiūrėta 2024-01-27. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62012CJ0293
36. Europos Žmogaus Teisių Teismas. „Case of Heino v. Finland“. 56720/09. 2011 m. vasario 15 d. HUDOC. Žiūrėta 2024-01-26. https://hudoc.echr.coe.int/eng?i=001-103394
37. Europos Žmogaus Teisių Teismas. „Case of S. and Marper v. The United Kingdom“, 30562/04, 30566/04. 2008 m. gruodžio 4 d. HUDOC. Žiūrėta 2024-01-26. https://hudoc.echr.coe.int/fre?i=001-90051
38. Generalinio Advokato Išvada. „Sujungtose bylose Digital Rights Ireland Ltd (C-293/12) prieš Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Airiją,The Attorney General, ir Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl ir kt“. 2013 m. gruodžio 12d. InfoCuria. Žiūrėta 2024-01-27. https://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=LT&mode=req&dir=&occ=first&part=1&cid=315665
39. Generalinio Advokato Išvada. „Sujungtose bylose WM (C-37/20) ir Sovim SA (C-601/20) prieš Luxembourg Business Registers“. 2022 m. sausio 20d. InfoCuria. Žiūrėta 2024-01-27. https://curia.europa.eu/juris/document/document.jsf?text=&docid=252461&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=5995909

40. Lietuvos Respublikos Konstitucinis Teismas. „Oficialiosios Konstitucinės Doktrinos nuostatos. 2014-2016. Vilnius, 2017. Žiūrėta 2024-04-28. https://lrkt.lt/data/public/uploads/2017/06/doktrinos-papildymas-2014-2016.pdf
41. Vokietijos Konstitucinis Teismas. „Headnotes to the Judgment of the First Senate“. 2010 m. kovo 2d. 1BvR 256, 263, 586/08. Žiūrėta 2024-01-27. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html

Mokslinės publikacijos:

42. Anthony, Nicolas. „The Right to Financial Privacy: Crafting a Better Framework for Financial Privacy in the Digital Age“. Policy Analysis no. 945 (2023). Cato Institute, Washington, DC. https://www.cato.org/sites/cato.org/files/2023-04/policy-analysis-945.pdf
43. Ampudia, Miguel, Ehrmann Michael. „Financial inclusion: what's it worth?“ *ECB Working Paper*, 1990 (2017). https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1990.en. pdf
44. Bank for International Settlements (BIS). *Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders*. 2023. https://www.bis.org/publ/othp66.htm
45. Brewczynska, Magdalena. „Financial Intelligence Units: Reflections on the applicable data protection legal framework“. *Computer Law and Security Review*, 43 (2021). https://doi.org/10.1016/j.clsr.2021.105612
46. Centre for European Policy Studies (CEPS). *Anti-money laundering in the EU time to get serious.* Briuselis, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805607
47. Dennis, Mark.*The measure of last resort: some things you need to know about the law of arrest*. Forbes Chambers, 2011. https://criminalcpd.net.au/wp-content/uploads/2016/09/Arrest_paper__The_Measure_of_Last_Resort__June_2011.pdf
48. *Encouraging Public-Private Partnerships to Fight Financial Crime*. Atlantic Council. 2012. Washington DC. https://www.files.ethz.ch/isn/155412/AC-TR%20Financial%20Crime%20Report%20-%20Final.pdf
49. EPP Group. *How to combat organised crime in the European Union*. 2022. https://www.eppgroup.eu/newsroom/publications/epp-group-position-paper-on-how-to-combat-organised-crime-in-the-european-union
50. European Banking Federation. Lifting the spell of dirty money: blueprint for an effective EU framework to fight money laundering. 2020. https://www.ebf.eu/wp-content/uploads/2020/03/EBF-Blueprint-for-an-effective-EU-framework-to-fight-money-laundering-Lifting-the-Spell-of-Dirty-Money-.pdf

51. Europos Komisija. „On the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing“. Commission staff working document. Briuselis, 2022. https://finance.ec.europa.eu/system/files/2022-10/221028-staff-working-document-aml-public-private-partnerships_en.pdf
52. Europos Komisija. *Accompanying the document Proposal for a Directive of the European Parliament and of the Council on laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA*. Commission staff working document. Strasbūras, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0114
53. Ferrari, Valeria. „Crosshatching Privacy: Financial Intermediaries' Data Practices between Law Enforcement and Data Economy“. *European Data Protection Law Review (EDPL)* 6, 4 (2020): 522-535. https://doi.org/10.21552/edpl/2020/4/8
54. Future of Financial Intelligence Sharing (FFIS) research program. „Lessons in private-private financial information sharing to detect and disrupt crime”. A Survey and Policy Discussion Paper, 2022. Royal United Services Institute. https://www.future-fis.com/uploads/3/7/9/4/3794525/rusi_ffis_survey_and_policy_discussion_paper_-_lessons_in_private-private_financial_information_sharing_to_detect_crime.pdf
55. INTERPOL General Secretariat. *Interpol's financial crime and anti-corruption centre (IFCACC)*. Lyon, 2022. https://www.interpol.int/content/download/17283/file/IFCACC_Project%20sheet_EN01.pdf
56. Kaiser, Carolina. „Privacy and identity issues in financial transactions : the proportionality of the European Anti-Money laundering legislation“. PhD Thesis, University of Groningen, 2018. https://research.rug.nl/en/publications/privacy-and-identity-issues-in-financial-transactions-the-proport
57. Kemsley, Dean, Kemsley, A. Sean ir Morgan, T. Frank. „Tax evasion on lawful income: is it a form of money laundering?“ *Journal of Financial Crime* 31, 1 (2023): 33-43. https://doi.org/10.1108/JFC-11-2022-0268
58. Kyriakos-Saad, Nadim, Esposito, Gianluca, ir Schwarz, Nadine. The Incestuous Relationship Between Corruption and Money Laundering. *Revue internationale de droit pénal* 83, 1–2 (2012): 161–172. https://www.cairn.info/revue-internationale-de-droit-penal-2012-1-page-161.htm
59. Laurinaitis Marius., Štitilis, Darius ir Verenius Egidijus. „Asmens duomenų kiekio mažinimo principo įgyvendinimas finansų įstaigose“. *JURISPRUDENCIJA*, 27, 2 (2020): 389–410. https://ojs.mruni.eu/ojs/jurisprudence/article/view/6365/5325

60. Markevičius Edgaras. „Asmens duomenų perdavimo elektroninėje erdvėje tarp Europos Sąjungos ir Jungtinių Amerikos Valstijų teisinės problemos“. Daktaro disertacija, Mykolo Romerio universitetas, 2022. https://www.mruni.eu/wp-content/uploads/2022/08/Edgaras-Markevicius_MRUweb.pdf
61. Maxwell J., Nick, Artingstall, David. „The Role of Financial Information-Sharing Partnerships in the Disruption of Crime“. Occasional Paper, 2017. Royal United Services Institute. https://static.rusi.org/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwwell_artingstall_web_4.2.pdf
62. Maxwell, Winston. *The GDPR and private sector measures to detect criminal activity*. Paris, 2021. https://hal.archives-ouvertes.fr/hal-03316259
63. McNaughton, J. Katarzyna. „The variability and clustering of Financial Intelligence Units (FIUs) – A comparative analysis of national models of FIUs in selected western and eastern (post-Soviet) countries“. *Journal of Economic Criminology*, 2, (2023). https://doi.org/10.1016/j.jeconc.2023.100036
64. Mouzakiti, Foivi. „Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive“. *New Journal of European Criminal Law* 11, 3 (2020): 351–374. https://doi.org/10.1177/2032284420943303
65. Naylor, R. Tom. *Follow-the-money methods in crime control policy*. Toronto, 1999. https://www.ncjrs.gov/nathanson/washout.html
66. Pasley, Robert. S. „Privacy Rights v. Anti-Money Laundering Enforcement“. *North Carolina Banking Institute* 6, 1 (2022): 147-226. http://scholarship.law.unc.edu/ncbi/vol6/iss1/7
67. Pavlidis, George. „Financial information in the context of anti-money laundering: Broadening the access of law enforcement and facilitating information exchanges“. *Journal of Money Laundering Control*, 23, 2, (2020): 369–378. https://doi.org/10.1108/JMLC-10-2019-0081
68. Pranevičienė, Birutė. Limiting of the right to privacy in the context of protection of national security“. *JURISPRUDENCIJA* 18, 4 (2011):1609-1622. https://ojs.mruni.eu/ojs/jurisprudence/article/view/96/90
69. Quintel, Teresa. „Data protection rules applicable to Financial Intelligence Units: still no clarity in sight“. *ERA Forum*, 23, 1 (2022): 53–74. https://doi.org/10.1007/s12027-021-00697-z

70. Richards, Jim. *314(b) Information Sharing – a Valuable, but Underutilized Tool*. 2020. RegTech Consulting. https://regtechconsulting.net/aml-regulations-and-enforcement-actions/314b-information-sharing-a-valuable-but-underutilized-tool/
71. Sinha, Gauri. „AML-CTF: a forced marriage post 9/11 and its effect on financial institutions“. *Journal of Money Laundering Control*, 16, 2 (2013): 142–158. https://doi.org/10.1108/13685201311318494
72. *Special Contributor Forecast: Data Privacy, Protection Challenges and Risk Management Concerns Will Lead AML Compliance Direction in 2023.* ACFCS. Žiūrėta 2024-02-21. https://www.acfcs.org/acfcs-special-contributor-forecast-data-privacy-protection-challenges-and-risk-management-concerns-will-lead-aml-compliance-direction-in-2023
73. Thony, Jean-Francois. *Use of Information Exchange in Criminal Matters to Combat Money Laundering and Financing of Terrorism*. IMF, 2007. https://www.elibrary.imf.org/display/book/9781589064874/ch001.xml
74. Vogel, Benjamin. „Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing“. *EUCRIM Forum* 1 (2022): 52-60. https://eucrim.eu/articles/potentials-and-limits-of-public-private-partnerships-against-money-laundering-and-terrorism-financing/
75. Rees, Jon, Wass, Sanne. *GDPR clash leaves Europol banned from hosting financial crime computer network*. S&P Global Market Intelligence. 2020. Žiūrėta 2024-03-03. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/gdpr-clash-leaves-europol-banned-from-hosting-financial-crime-computer-network-57121862
76. Wolford, Ben. *What is GDPR, the EU's new data protection law?* GDPR EU. Žiūrėta 2024-01-26. https://gdpr.eu/what-is-gdpr/
77. World Economic Forum. *The Role and Responsibilities of Gatekeepers in the Fight against Illicit Financial Flows: A Unifying Framework*. 2021. https://www3.weforum.org/docs/WEF_Gatekeepers_A_Unifying_Framework_2021.pdf

Kiti šaltiniai:

78. Anti-money laundering: Council and Parliament strike deal on stricter rules. Coucil of EU press releases. 2024-01-18. https://www.consilium.europa.eu/en/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules/
79. „Crypto bears the brunt of Estonia's war against dirty money“. *Politico*. 2022-03-11. Žiūrėta 2023-03-03. https://www.politico.eu/article/crypto-finance-estonia-dirty-money/
80. DLA Piper. *Data Protection Laws of the World. Singapore.* Žiūrėta. 2023-12-20. https://www.dlapiperdataprotection.com/index.html?t=law&c=SG

81. Federal Deposit Insurance Corporation. *Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity*. 2023. FFIEC BSA/AML Examination Manual. https://www.fdic.gov/news/financial-institution-letters/2023/fil23040e.pdf
82. *FinCEN Expands Section 314(b) Information Sharing Safe Harbor*. Debevoise & Plimpton. 2020. Žiūrėta 2024-03-03. https://www.debevoise.com/insights/publications/2020/12/fincen-expands-section-314b-information
83. FinCEN. *Section 314(b) Fact Sheet.* 2020-12. https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf
84. „History of Anti-Money Laundering (AML) Laws“. Sigma360. Žiūrėta 2023-01-27. https://www.sigma360.com/knowledge-center/history-of-aml-laws
85. *Netherlands: AP advises on draft bill to amend Money Laundering Action Plan Act*. OneTrust DataGuidance. Žiūrėta 2024-02-22. https://www.dataguidance.com/news/netherlands-ap-advises-draft-bill-amend-money
86. *News update Financial Regulatory.* Hauthoff. Žiūrėta 2024-02-21. https://www.houthoff.com/insights/news-update/dutch-government's-aml-policy-agenda-and-fine-for-collective-licence-holder
87. Pinigų plovimo prevencijos kompetencijų centras. Metinė ataskaita, 2021. https://amlcenter.lt/wp-content/uploads/2022/08/PPPKC-Metine-veiklos-ataskaita-2021m..pdf
88. *Prezidento veto: žmogaus privatus gyvenimas turi būti apsaugotas tinkamai reguliuojant asmens duomenų tvarkymą*. 2022 m. lapkričio 17 d. Lietuvos Respublikos Prezidentas. Žiūrėta 2024-01-27. https://www.lrp.lt/lt/prezidento-veto-zmogaus-privatus-gyvenimas-turi-buti-apsaugotas-tinkamai-reguliuojant-asmens-duomenu-tvarkyma/39475
89. „Revolut calls on High Court to throw out lawsuit over account closure“. *Financial Times*. 2024 m. sausio 18d. https://www.ft.com/content/8763fa89-4269-4286-91d1-678cb71cde12
90. SALV. *AML Bridge – building the new standard in AML/CTF*. White Paper, 2021. https://salv.com/uploads/AML-Bridge-Estonia.pdf
91. *Seimas pritarė Respublikos Prezidento veto dėl Mokėjimų įstatymo pataisų*. Lietuvos Respublikos Seimas. Žiūrėta 2024-01-27. https://www.lrs.lt/sip/portal.show?p_r=35403&p_k=1&p_t=283020
92. The Swedish police Auhority. *The Financial Intelligence Unit Annual Report 2022*. 2023. https://polisen.se/siteassets/dokument/polisens-arsredovisning/fipos-arsrapport/financial-intelligence-unit-annual-report-2022.pdf
93. „Using financial information for preventing, detecting, investigating and prosecuting criminal offences“. Summaries of EU Legislation. Žiūrėta 2024-02-21. https://eur-

lex.europa.eu/EN/legal-content/summary/using-financial-information-for-preventing-detecting-investigating-and-prosecuting-criminal-offences.html

94. *What does TMNL do*? Transactie Monitoring Nederland. Žiūrėta 2024-02-21. https://tmnl.nl/en/about-tmnl/tmnl-in-brief/
95. *What is criminal offence data?* Information Commissioner's Office. Žiūrėta 2024-01-25. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/criminal-offence-data/what-is-criminal-offence-data/

ANOTACIJA

Magistro baigiamajame darbe analizuojamos naujausios iniciatyvos, keistis informacija tarp kovą su finansiniais nusikaltimais vykdančių institucijų, dviem atskirais atvejais: kai finansų įstaigos keičiasi informacija tarpusavyje (angl. *private-private partnership*), kai teisėsauga perduoda operatyvinę informaciją finansų įstaigoms (angl. *public-private partnership*). Vertinamas šių iniciatyvų suderinamumas su teise į privatumą ir asmens duomenų apsaugą.

Prieinama išvados, kad šių dienų finansinių nusikaltimų prevencijos sistema nebėra pakankama kovojant su finansiniais nusikaltimais, o keitimasis informacija gali reikšmingai pagerinti susidariusią situaciją. Pagal Europos Sąjungoje įtvirtintą teisės į privatumą ir asmens duomenų apsaugą teisinį reguliavimą, keitimasis informacija kovoje su finansiniais nusikaltimais, tarp finansų įstaigų ir su teisėsauga, iš esmės, yra galimas, su tam tikromis išlygomis.

Reikšminiai žodžiai: kova su finansiniais nusikaltimais, keitimasis informacija, teisė į privatumą ir asmens duomenų apsaugą.

ANNOTATION

Master thesis analyses the new initiatives of information sharing in fighting financial crimes. Analysis contains two types of information sharing: where financial institutions exchange information with each other (*private-private partnership*) and where law enforcement exchanges operational information with financial institutions (*public-private partnership*). Analysis provides assessment of the new initiatives' compliance with the right to privacy and data protection law.

Concluded that current regulatory framework in financial crime prevention is not effective enough to fight financial crimes, where information exchanges may be seen as a paradigm shift. European Union legislative framework of privacy and data protection law provides possibility to exchange information between financial institutions and law enforcement with financial institutions under certain conditions.

Keywords: fighting with financial crimes, information exchange, the right to privacy and data protection.

SANTRAUKA

KEITIMASIS INFORMACIJA KOVOJE SU FINANSINIAIS NUSIKALTIMAIS IR ASMENS DUOMENŲ APSAUGOS REIKALAVIMAI

Magistro baigiamasis darbas

Nepaisant ilgus metus dedamų pastangų, kova su finansiniais nusikaltimais nėra efektyvi, nes nusikaltėliai nepaiso valstybių sienų ir kuria schemas, pasitelkdami platų finansų įstaigų tinklą. Tuo tarpu, kovą su finansiniais nusikaltimais vykdančių institucijų pusėje matomas tik fragmentuotas finansinių nusikaltimų tinklų vaizdas, kuris gali būti sudėliojamas tik peržengiant dabartiniu teisiniu reguliavimu nustatytas dalinimosi informacija ribas. Susiklosčius tokiai situacijai, informacijos mainai tarp kovą su finansiniais nusikaltimais vykdančių tampa kritiškai svarbūs kovoje su finansiniais nusikaltimais.

Šiai dienai Europos Sąjungoje nėra reguliavimo, įteisinančio tokius informacijos mainus. Įstatymo leidėjui, vėluojant nustatyti bendrą politiką ir teisinę-reguliacinę aplinką, kai kuriuose valstybės narėse kilo privataus ir valstybinio sektoriaus savanoriškos iniciatyvos keistis duomenimis. Lygiagrečiai ši tendencija stebima ir ES nepriklausančiose valstybėse, stambiuose pasaulio finansų centruose. Pradėti diegti keitimosi informacija modeliai jau pademonstravo sėkmingus rezultatus kovojant su finansiniais nusikaltimais, tačiau nebuvo iki įvertinti iš teisės į privatumą ir asmens duomenų apsaugą perspektyvos. Magistro baigiamajame darbe lygiagrečiai analizuojami du apsikeitimo informacija tipai: keitimasis informacija tarp finansų įstaigų (angl. *private-private partnership*), ir keitimasis informacija tarp teisėsaugos ir finansų įstaigų, kai teisėsauga dalinasi operatyvine informacija (angl. *public-private partnership)*. Iškeltas ginamasis teiginys, kad keitimosi informacija tarp finansų įstaigų modeliai yra būtinai reikalinga priemonė kovoje su finansiniais nusikaltimais ir gali būti suderinami su teise į privatumą ir asmens duomenų apsaugą, išlaikant interesų balansą.

Pirmojoje magistro baigiamojo darbo dalyje, atskleidžiama kokiomis aplinkybėmis kūrėsi kovą su finansiniais nusikaltimais vykdančios institucijos, kokie uždaviniai joms patikėti ir kaip keičiamasi informacija pagal dabartinį teisinį reguliavimą, kartu atskleidžiant ir kodėl keitimasis informacija kovoje su finansiniais nusikaltimais nėra pakankamas užtikrinti šios kovos efektyvumui ir kokius pokyčius siūlo įstatymų leidėjas.

Antroje dalyje, gilinamasi į teisės į privatumą ir asmens duomenų apsaugą teisinį reguliavimą, analizuojama, kokius reikalavimus keitimuisi duomenimis kovoje su finansiniais

nusikaltimais nustato pirminiai ir antriniai teisės šaltiniai, kaip keitimąsi informacija kovoje su finansiniais nusikaltimais vertina teismai ir už asmens duomenų apsaugą atsakingos ES institucijos.

Trečiojoje dalyje, apžvelgiami keitimosi informacija tarp finansų įstaigų (angl. *private-private partnership*), ir keitimosi informacija tarp teisėsaugos ir finansų įstaigų, kai teisėsauga dalinasi operatyvine informacija (angl. *public-private partnership),* modeliai ES ir trečiosiose šalyse, atliekamas jų suderinamumo su teise į privatumą ir asmens duomenų apsaugą vertinimas.

Prieinama išvados, kad pagal Europos Sąjungoje įtvirtintą teisės į privatumą ir asmens duomenų apsaugą teisinį reguliavimą, keitimasis informacija kovoje su finansiniais nusikaltimais, tarp finansų įstaigų ir su teisėsauga, iš esmės, yra galimas, su tam tikromis išlygoms.

SUMMARY

INFORMATION EXCHANGES IN FIGHTING FINANCIAL CRIMES AND THE LAW OF PRIVACY AND DATA PROTECTION

Master thesis

Regardless vast efforts to fight financial crimes, this fight has proven to be ineffective as criminals do not stop at state borders and use the net of multiple financial institutions to launder their illegal gains. Meanwhile, financial crimes fighting institutions have only fragmented picture of financial crime net, possible to complete only if overstepping the lines of current legal framework of information exchanges. On given circumstances, information exchanges among institutions dedicated to fight financial crime becomes crucial in fighting financial crime.

Current European Union legal framework does not allow required information exchanges. While Regulator lags to set common policy and law on this matter, voluntary private and government sectors initiatives to exchange information have arisen in some member states and third countries – the world's leading global finance centres. Launched information exchanges models have already shown its capacity in fighting financial crimes, nevertheless the full-scale evaluation of information exchanges models' implications to the right of privacy and data protections was left behind. Master thesis simultaneously analyse two types of information exchanges: financial institutions exchange of information with each other (*private-private partnership*) and law enforcement exchanges of operational information with financial institutions (*public-private partnership*). The defence thesis states that information exchanges is strictly necessary measure in financial crimes fighting and compatible with the right to privacy and data protection law while keeping the right balance of interests.

First part of master thesis reviews how the regulatory framework of financial crimes prevention has been developed, what tasks were entrusted to financial crime fighting subjects, and what are the limits for information exchanges under current legislative framework. Moreover, analysis explains why current fight against financial crimes measures are not effective enough and what are the new law proposals.

Second part reviews the right of privacy and data protection law, analysing requirements arising from primarily and secondary sources of law, courts jurisprudence and EU institutions responsible for the data protection opinions on the matter of data exchange in fighting financial crimes.

Third part analyses information exchange models between financial institutions (*private-private partnership*), and information exchange models between law enforcement and financial institutions, where law enforcement shares operational information (*public-private partnership)* in EU and third countries, evaluates if those models are compliant with the right to privacy and data protection law.

Concluded, that exchange of information between financial institutions and law enforcement with financial institutions is possible under certain conditions.

PRIEDAI

Priedas Nr. 1. Duomenų keitimosi tarp finansų įstaigų modeliai[187]

Požymis / Valstybė	ES			Trečiosios šalys	
	Olandija	**Estija**	**Lietuva**	**Singapūras**	**JAV**
Iniciatyvos pradžia	2020 07	2020 10	2021 08	2021 10	2001
Platforma	TMNL	AML Bridge	dar nesvarstyta	COSMIC	nereikalaujama specialios platformos
Nacionalinė teisė	Inicijuojamas keitimas	Yra	Inicijuojamas keitimas	Inicijuojamas keitimas	Yra
DPA vertinimas	Abejojama dėl priemonės proporcingumo	Neprieštaravo iniciatyvai	Neprieštaravo iniciatyvai	Nėra kliūčių dėl asmens duomenų apsaugos reikalavimų.	Nėra kliūčių dėl asmens duomenų apsaugos reikalavimų.
Duomenų rūšis	Iki įtarimų kilimo	Kilus įtarimams	Kilus įtarimams	Iki ir po įtarimų kilimo	Iki ir po įtarimų kilimo
Dalyvavimas: savanoriškas ar privalomas	Privalomas (po TA pakeitimo)	Savanoriškas	Savanoriškas	Privalomas	Savanoriškas
Teisėtas duomenų tvarkymo pagrindas pagal BDAR	Teisinė pareiga. Už proporcingumą atsako įstatymo leidėjas	Teisėtas interesas. Už proporcingumą atsako FI	Teisėtas interesas. Už proporcingumą atsako FI		
Ar duomenys kaupiami centralizuotai?	Taip	Ne	Kol kas neapibrėžta	Taip	-
Keitimosi tikslas	PP ir TFP	PP, TFP, Sankcijos, sukčiavimas	PP, TFP, Sankcijos, sukčiavimas	PP ir TFP	Visi finansiniai nusikaltimai

[187] Sudaryta autorės

1 priedo tęsinys. Duomenų keitimosi tarp finansų įstaigų modeliai

Požymis / Valstybė	ES			Trečiosios šalys	
	Olandija	**Estija**	**Lietuva**	**Singapūras**	**JAV**
Iniciatoriai	Privatus sektorius	Privatus sektorius	Institucija vienijanti privatų ir valstybinį sektorių	Prudencinės priežiūros institucija	FŽP
Santykis su teisėsauga	Neturi prieigos	FŽP dalyvauja vystant iniciatyvą, bet prieigos neturi	Kol kas neapibrėžta	FŽP turi tiesioginę prieigą	FŽP koordinuoja modelį, bet prieigos neturi
Duomenys šifruojami	Taip	Taip	Kol kas neapibrėžta	Taip	Ne
Finansinės atskirties ir *de-risking* proceso valdymas	Kitos FI naudotojos negali nustatyti, ar kuri nors naudotoja FI nutraukė dalykinius santykius.	Nekontroliuojama, planuojama peržiūrėti jei būtų iškelta byla.	Kol kas neapibrėžta	Kitoms FI neleidžiama atmesti kliento remiantis vien tuo pagrindu, kad viena iš FI įtraukia klientą į „juodąjį sąrašą.	Kitos FI naudotojos negali nustatyti, ar kuri nors naudotoja FI nutraukė dalykinius santykius.
Santykis su STR perdavimu	Nežinoma, kad buvo užpildytas STR	Nežinoma, kad buvo užpildytas STR, yra galimybė pildyti jungtinį STR.	Kol kas neapibrėžta	Žinoma, kad buvo užpildytas STR.	Nežinoma, kad buvo užpildytas STR
Apsauga nuo civilinės atsakomybės	Nepatikslinta	Neatsako, jei veikė gera valia	Nepatikslinta	Neatsako, jei veikė gera valia	„saugus uostas“

Priedas Nr. 2 Keitimosi informacija tarp finansų įstaigų ir teisėsaugos modeliai[188]

Požymis / Valstybė	ES		Iki *Brexit*	Trečiosios šalys
	Olandija	**Švedija**	**Jungtinė Karalystė**	**JAV**
Iniciatyvos pradžia	2019	2020	2014	2001, 2018 - atnaujintas
Iniciatyva	Fintell Alliance	SAMLIT	JMLIT	Sekcija 314 (a)
Įtvirtinta nacionalinėje teisėje	Ne	Ne	Taip	Taip
Informacijos tipas	Strateginė ir taktinė	Strateginė ir taktinė	Strateginė ir taktinė	Taktinė
FŽP dalyvavimas	Taip	Taip	Taip	Taip
FI dalyvavimas	Savanoriškas	Savanoriškas	Privalomas	Savanoriškas

[188] Sudaryta autorės