Vilniaus universiteto Teisės fakulteto
Baudžiamosios justicijos katedra

Gabijos Panomariovaitės
V kurso baudžiamosios justicijos
studijų šakos studentės

Magistro darbas

Tarptautinis bendradarbiavimas tiriant kibernetinius nusikaltimus

International Cooperation in Cybercrime Investigation

Vadovas: Asist. Dr. Justas Namavičius
Recenzentas: Lekt. Darius Prapiestis

Vilnius
2024

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojama tarptautinio bendradarbiavimo svarba ir sunkumai kovojant su nusikaltimais kibernetinėje erdvėje, aptariant tiek bendrą tarptautinio baudžiamojo bendradarbiavimo sistemą Europos Sąjungoje ir Lietuvoje, tiek ir specifinius kibernetinių nusikaltimų keliamus iššūkius bei jų tyrimo ypatumus. Darbe įvertinami elektroninių įrodymų gavimo būdai pasitelkiant tarptautinį bendradarbiavimą ir analizuojama tokių duomenų gavimo problematika, tačiau ypatingas dėmesys skiriamas naujam 2023 m. Europos Sąjungos elektroninių įrodymų teisės aktų paketui ir su juo susijusiems iššūkiams. Šis darbas siekia įvertinti, ar naujasis teisės aktų paketas padės efektyviau kovoti su kibernetiniais nusikaltimais.

Pagrindiniai žodžiai: kibernetiniai nusikaltimai, tarptautinis bendradarbiavimas, elektroniniai įrodymai, elektroniniai duomenys, Europos Sąjunga, skaitmeninių paslaugų teikėjai.

This paper analyses the importance and difficulties of international cooperation in the fight against cybercrime, discussing both the general framework of international criminal cooperation in the European Union and Lithuania, as well as the specific challenges and peculiarities of cybercrime investigation. The work assesses the ways of obtaining electronic evidence through international cooperation and analyses the problems of obtaining such data, but pays particular attention to the new 2023 European Union electronic evidence legislative package and the challenges related to it. This paper seeks to assess whether the new package will contribute to a more effective fight against cybercrime.

Key words: cybercrime, international cooperation, electronic evidence, electronic data, European Union, digital service providers.

TURINYS

ĮŽANGA

Nagrinėjamos temos aktualumas. Modernėjant visuomenei ir atsirandant naujoms technologijoms, mūsų gyvenimas vis labiau persipina su skaitmeninėmis technologijomis. Atrodo, kad mūsų kasdienybė persikelia į kibernetinę erdvę, padedama technologijų, kurios supaprastina ir pagreitina įprastines užduotis, darbą ir bendravimą. Tačiau prie šios naujos realybės prisitaiko ir nusikalstamumas. Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos duomenimis Lietuvoje 2023 m. užregistruotos 45 151 nusikalstamos veikos, iš kurių 3887 nusikalstamos veikos, arba 8,6 proc., padarytos kibernetinėje erdvėje (Informatikos ir ryšių departamentas, 2024). Nusikaltimai įgauna ne tik naują erdvę, tačiau ir naują pobūdį, kuris lemia daugybę iššūkių teisėsaugos institucijoms tiriant kibernetinius nusikaltimus. Vienas iš jų, yra tai, kad nusikaltimai padaryti naudojant kibernetinę erdvę peržengia vienos valstybės jurisdikcijos ribas. Dėl šios priežasties, tiriant tokio pobūdžio nusikaltimus reikia pasitelkti tarptautinį bendradarbiavimą, ypatingai siekiant gauti duomenis, kurie vėliau gali būti pripažįstami įrodymais, esančius kitoje valstybėje. Europos Taryba ir Europos Parlamentas, po penkerių metų trukusių derybų, 2023 m. liepą galiausiai priėmė teisės aktų paketą (Reglamentas (ES) 2023/1543 ir Direktyva (ES) 2023/1544) skirtą elektroninių įrodymų rinkimui, palengvinant ir pagreitinant tarptautinį bendradarbiavimą šiuo klausimu. Atsižvelgiant į tai, šis naujasis teisinis reglamentavimas bus taikomas nuo 2026 m. visoms valstybėms narėms.

Darbo tikslas – išanalizuoti tarptautinio bendradarbiavimo efektyvumą tiriant kibernetinius nusikaltimus ir identifikuoti esamas problemas dėl elektroninių duomenų, esančių kitoje valstybėje, rinkimo.

Darbo uždaviniai:

1. Atskleisti tarptautinio bendradarbiavimo baudžiamojoje justicijoje raidą, sistemą, rūšis ir formas Europos Sąjungos bei Lietuvos mastu.
2. Išnagrinėti kibernetinių nusikaltimų sampratą bei identifikuoti kibernetinių nusikaltimų teisėsaugos institucijoms keliamus iššūkius ir jų užkardymo pasitelkiant tarptautinį bendradarbiavimą problemas.
3. Išryškinti tarptautinio bendradarbiavimo svarbą renkant elektroninius duomenis kibernetinių nusikaltimų bylose ir esamą problematiką.
4. Išanalizuoti naująjį 2023 m. Europos Sąjungos teisės aktų paketą dėl elektroninių įrodymų rinkimo ir jo įgyvendinimo iššūkius, įvertinant paketo efektyvumą tarptautiniam bendradarbiavimui tiriant kibernetinius nusikaltimus.

Tyrimo objektas – tarptautinio bendradarbiavimo tiriant kibernetinius nusikaltimus, elektroninių duomenų, esančių kitoje valstybėje, rinkimo pasitelkiant tarptautinį

bendradarbiavimą reglamentavimas ir naujojo 2023 m. Europos Sąjungos teisės aktų, skirtų elektroninių duomenų gavimui, paketo (Reglamentas (ES) 2023/1543 ir Direktyva (ES) 2023/1544) ir įgyvendinimo problematika. Prieš tai išanalizuojant bei aptariant tarptautinio bendradarbiavimo Europos Sąjungoje raidą, sistema, rūšis bei formas, kibernetinių nusikaltimų sampratą ir tokių nusikaltimų keliamus iššūkius teisėsaugos institucijoms.

Tyrimo metodai. Šiame magistro darbe buvo naudoti istorinis, sisteminis, lyginamasis, loginis ir lingvistinis tyrimo metodai:

1. Istorinis metodas naudojamas analizuojant tarptautinio bendradarbiavimo raidą Europos Sąjungoje.
2. Sisteminis metodas naudojamas visapusiškai atskleidžiant tarptautinio bendradarbiavimo, susijusio su kibernetiniais nusikaltimais bei elektroninių duomenų gavimo teisinį reglamentavimą, jų ryšį su teisės principais ir kitais teisės aktais.
3. Lyginamasis metodas šiame magistro darbe naudotas siekiant palyginti 2023 m. Europos Sąjungos teisės aktų paketą dėl elektroninių įrodymų rinkimo su jo pirminiais teisėkūros dokumentais bei dabartiniu reglamentavimu.
4. Loginis metodas naudotas analizuojant teisės normas, sąvokas bei teismų praktiką.
5. Lingvistinis metodas darbe naudojamas siekiant aptarti teisines sąvokas ir jų apibrėžimus.

Originalumas. Šiame darbe nemažas dėmesys skiriamas elektroninių duomenų kaip įrodymų rinkimui pasitelkiant tarptautinį bendradarbiavimą. Kadangi naujasis elektroninių įrodymų teisės aktų rinkinys yra neseniai priimtas, nedaug mokslininkų yra apžvelgę šį teisės aktų paketą, kartu su tarptautinio bendradarbiavimo tiriant kibernetinius nusikaltimus sistema. Nepaisant to, kad įtvirtintas reglamentavimas yra dar labai naujas ir bus taikomas tik ateityje, dar iki priėmimo jis tapo aršiu diskusijų objektu. Suinteresuotosios šalys iki galo kovojo, kad elektroninių įrodymų reglamento priėmimas būtų sustabdytas. Nežinia kodėl, tačiau daug diskusijų sulaukęs šis teisės aktų paketas Lietuvos mokslininkų teisės tyrimo objektu netapo. Apskritai, Lietuvos mokslinėje literatūroje yra nagrinėta tik kibernetinių nusikaltimų samprata bei atskirų kibernetinių nusikaltimų rūšių reglamentavimas, tačiau ne tarptautinis bendradarbiavimas ir su juo susiję klausimai tiriant kibernetinius nusikaltimus.

Svarbiausi šaltiniai. Rengiant magistro darbą buvo naudojami teisės norminiai aktai, specialioji literatūra bei teismų praktika. Šiame darbe svarbiausi teisės norminiai aktai yra 2001 m. Konvencija dėl elektroninių nusikaltimų, Reglamentas (ES) 2023/1543 dėl Europos įrodymų pateikimo orderių ir Europos įrodymų saugojimo orderių elektroniniams įrodymams baudžiamajame procese ir laisvės atėmimo bausmių vykdymui pasibaigus

baudžiamajam procesui, Direktyva (ES) 2023/1544, kuria nustatomos suderintos paskirtųjų įmonių ir teisinių atstovų skyrimo elektroniniams įrodymams bei jų parengiamieji dokumentai ir kiti su tema reikšmingai susiję Europos Sąjungos bei Lietuvos teisės aktai. Taip pat, šiame darbe buvo panaudota specialioji literatūra, kuri padėjo išsamiai išanalizuoti tam tikrų požymių, sampratos ir tarptautinio bendradarbiavimo tiriant kibernetinius nusikaltimus problematikos specifiką. Tarptautinio bendradarbiavimo Europos Sąjungoje raidą padėjo atskleisti knyga „Handbook of European Procedure“, kibernetinių nusikaltimų sampratą bei keliamus iššūkius knyga - „Cybercrime, Digital Forensics and Jurisdiction“. Reikšmingi specialios literatūros autoriai – J. Clough, M. Chawki, R. E. Kostoris, L. Belevičius, V. Franssen, S. Tozska.

1. TARPTAUTINIO BENDRADARBIAVIMO BAUDŽIAMOJOJE JUSTICIJOJE TEORINIAI ASPEKTAI

Bendradarbiavimo ištakos siekia ankstyviausias žmonių visuomenes ir tai visais laikais buvo svarbus įrankis socialinių ryšių ir savitarpio pagalbos vystymuisi, didelių konfliktų išsprendimui. Bendradarbiavimas apima kolektyvinį asmenų ar grupių siekį pasiekti bendrų tikslų, kurių negalima pasiekti vien tik individualiomis pastangomis (Mattessich, Monsey, 1992, p. 4). Bendradarbiavimo esmė - sinergijos principas, pagal kurį bendros grupės pastangos duoda geresnių rezultatų ir didesnį poveikį, nei atskirų asmenų poveikių suma (Kinderis, Jucevičius, 2013, p. 30). Psichologijoje bendradarbiavimas, paprastai, įvardijamas kaip komunikacija, kuri reiškia keitimąsi informacija, naudojant kokią nors ženklų sistemą. Čia informacija yra suprantama plačiąją prasme – viskas kas susiję su informacija, jos gavimas, traktavimas, nuskaitymas. (Lekavičienė *et al.*, 2015, p. 16 - 23). Psichologai yra išvystę komunikacijos proceso teorijas (modelius), kurios paaiškina kaip yra keičiamasi informacija tarp komunikacijos procese dalyvaujančių asmenų. Nors komunikacijos proceso modelių egzistuoja įvairių, tačiau pagrindiniai elementai yra siunčiama žinia, jos siuntėjas ir gavėjas (priėmėjas). Sudėtingesni modeliai apima ir atgalinį ryšį, siuntimo būdus, kontekstą, trikdžius ir kt. (Devito, 2003, cituota Lekavičienė *et al.*, 2015, p. 18). Informacija keliauja tarp kanalų, kurie būna įvairiausi, priklausomai nuo komunikacijos tikslo ir prasmės. Teisine prasme, bendradarbiavimo atveju, komunikacija vyksta tarp dviejų įgaliotų institucijų, kurių tikslas yra siekti vieningo teisinio gėrio, kadangi vienas iš valstybės funkcijų – teisingumo įvykdymas (Gutauskas, 2013, p. 140). Tarptautinis bendradarbiavimas yra valstybių, tarptautinių organizacijų, nevyriausybinių organizacijų, įmonių ir kitų subjektų tarpusavio sąveika, siekiant bendrų tikslų ar sprendžiant globalias problemas. Toks bendradarbiavimas gali apimti įvairias sritis, tokias kaip baudžiamoji justicija, ekonomika, aplinkos apsauga, sveikatos sistema, moksliniai tyrimai, švietimas ir daugelį kitų.

1.1. Tarptautinio bendradarbiavimo baudžiamojoje justicijoje Europos Sąjungos lygmeniu raida

Atsidarius valstybių sienoms, atsirado žmonių poreikis laisvai keliauti, plėsti akiratį. Sienos atsivėrė ne tik pasaulėžiūros praplėtimui, tačiau ir nusikalstamumui. Nusikaltimai įgavo tarptautinį pobūdį, kuomet nusikalstamos veikos peržengė konkrečios valstybės teritorijos ribas. Užkardyti tokias nusikalstamas veikas tapo sudėtinga užduotis valstybėms, kadangi jų jurisdikcija persipina su kitomis valstybėmis, o vienas iš tarptautinių teisės principų yra nesikišimo principas. Dėl šios priežasties, valstybių institucijos buvo įpareigotos pasirašyti tarptautines sutartis, nusistatyti taisykles, kad būtų lengviau užkardyti bei išaiškinti tokio

pobūdžio nusikalstamas veikas ir atitinkamai kaltus asmenis dėl padarytos nusikalstamos veikos patraukti atsakomybėn.

Iki XVIII – XIX a. teisinės pagalbos suvokimas buvo kitoks, nei yra dabar. Tai buvo ne tiek teisinio baudžiamojo proceso dalis, o politinis – diplomatinis santykis. Valstybės geranoriškai bendradarbiaudavo viena su kita diplomatiniais kanalais, t. y. per valstybių atstovus, diplomatinės atstovybes (Kostoris *et al*, 2018, p. 11). Europos Bendrijų steigimo sutartyse[1] iš pradžių nebuvo nuostatų dėl institucinių ir teisminio bendradarbiavimo baudžiamosiose bylose, nes svarbiausi valstybių narių tikslai buvo sukurti vieningą Europą, pašalinti pasaulietinius nacionalinius prieštaravimus ir išsaugoti ilgalaikę taiką siekiant ekonominio bendradarbiavimo. Kuriant bendrąją rinką, siekiant valstybių steigėjų tikslų, taip pat siekiant laisvo darbuotojų ir asmenų judėjimo, kilo daugybė pavojų, darančių įtaką Bendrijos interesams. Tarpvalstybinis nusikalstamumas - daugiausia prekyba narkotikais ir terorizmas - buvo tik viena iš tokių problemų. Nuo 1970 m. Bendrijos biudžetas turėjo nuosavų pajamų, dėl kurių buvo sunku kontroliuoti pinigų judėjimą, o tai sudarė pagrindą piktnaudžiavimui. Kita vertus, verslo įmonės ir privatūs asmenys pasinaudojo bendrąja rinka, pasinaudodami privalomais mokėjimais į Bendrijos biudžetą (Harmati et al. 2008, p. 4). Kovojant su tarptautiniu nusikalstamumu, tapo svarbi ir Bendrijos finansinių interesų apsauga, nes daugėjo nusikaltimų, ypač sukčiavimo, turinčių įtakos Bendrijos biudžetui. Siekiant kovoti su nusikalstamumu ir veiksmingai apsaugoti Bendrijų finansinius interesus, atsirado būtinybė bendradarbiauti baudžiamosiose ir teisminėse bylose tarp valstybių narių. 1992 m. vasario mėn. buvo pasirašyta Mastrichte sutartis, kuria įsteigta Europos Sąjunga. Europos Sąjungos (toliau ir – ES) sutartimi visa veikimo struktūra buvo suskirstyta į tris ramsčius: pirmasis ramstis yra griežtai Bendrijos reikalas, skirtas Europos Bendrijai (į kurią susijungė Europos anglių ir plieno bendrija bei Europos ekonominė bendrija); antrasis ramstis susijęs su tarpvyriausybiniu bendradarbiavimu bendros užsienio ir saugumo politikos srityje; teisingumo ir vidaus reikalų bendradarbiavimas Europos integracijos lygmeniu institucionalizuotas kaip trečiasis ES ramstis (Europos Sąjungos sutartis, 1992). Nors baudžiamosios teisės institucija yra esminis nacionalinio suvereniteto veiksnys, trečiasis ramstis, panašiai kaip ir antrasis ramstis, liko atskirai nuo Bendrijos institucinės ir teisinės struktūros kaip tarpvyriausybinė pagalba[2] griežtai susijusi su Europos Taryboje

[1] 1951 m. balandžio 18 d. pasirašyta Europos anglių ir plieno bendrijos steigimo sutartis ir dvi 1957 m. Romoje pasirašytos Europos ekonominės bendrijos (EEB) ir Europos atominės energijos bendrijos (Euratomas) steigimo sutartys

[2] 1997 m. Amsterdamo sutartimi trečiasis ramstis buvo iš esmės pakeistas. Kai kurios politikos sritys, pavyzdžiui, prieglobsčio, imigracijos, sienų kontrolės, buvo įtrauktos į pirmąjį (Europos Bendrijos) ramstį. Trečiojo ramsčio pavadinimas iš „Bendradarbiavimas teisingumo ir vidaus reikalų srityse“ tapo „Policijos ir teisminis bendradarbiavimas baudžiamosiose bylose“.

atstovaujamų vyriausybių, kurios svarstė daugiausia vienbalsiai, valia, be jokios Europos Komisijos ir Teisingumo Teismo kontrolės ir nedalyvaujant Europos Parlamentui (Craig, de Búrca, 2003, p. 25-26). Tarpvyriausybinio bendradarbiavimo srityje įsteigtos tokios organizacijos kaip Europos policijos biuras (Europolas)[3], kurio tikslas didinti valstybių narių kompetentingų institucijų veiksmingumą ir bendradarbiavimą, dalijantis ir kaupiant kriminalinės žvalgybos informaciją, siekiant užkirsti kelią sunkiam tarptautiniam organizuotam nusikalstamumui, Europos teisminis tinklas (ETT)[4], kurio tikslas palengvinti teisminį bendradarbiavimą baudžiamosiose bylose, teikiant teisines ir praktines konsultacijas, ir padėti užmegzti tiesioginius nacionalinių kompetentingų institucijų kontaktus, ir galiausiai jau po kurio laiko - Europos Sąjungos bendradarbiavimo baudžiamosios teisenos srityje agentūra (Eurojustas)[5], kuris įsteigtas gerinti kompetentingų institucijų bendradarbiavimą, visų pirma sudarant palankesnes sąlygas tarptautinės savitarpio teisinės pagalbos teikimui ir Europos arešto orderio įgyvendinimui (ši institucija veikia kaip tarpininkas valstybėms, neretai sprendžia jurisdikcijos kolizijas). Tačiau vien to neužteko, kadangi bendradarbiavimas buvo svarbus ne vien tik dėl sunkių organizuotų nusikaltimų, terorizmo atvejais. Už valstybių sienos ribų buvo daromi ne tik sunkūs nusikaltimai, kurių užkardymas buvo ES interesas, tačiau ir kitos nusikalstamos veikos. Valstybių narių siekis buvo užkardyti ir kitas veikas, kurios turi tarptautinį elementą. Dėl šios priežasties, 2000 m. gegužės 29 d. buvo priimta Konvencija dėl Europos Sąjungos valstybių narių savitarpio pagalbos baudžiamosiose bylose, kurią pagal Europos Sąjungos sutarties 34 straipsnį patvirtino Europos Taryba, kuri pakeitė ir papildė iki to laiko galiojusią tarpusavio pagalbos baudžiamosiose bylose institutą (Konvencija dėl Europos Sąjungos..., 2000). Šia konvencija buvo siekiama paskatinti ir palengvinti teismų, policijos bei muitinių savitarpio pagalbą baudžiamosiose bylose, suteikia galimybę valstybėms narėms tiesiogiai susisiekti vienai su kita ir pagerinti teisminio bendradarbiavimo greitį bei veiksmingumą. Nepaisant visų reikšmingų naujovių, ES baudžiamojo teisingumo erdvėje buvo susidurta su pasipriešinimu ir sunkumais. Tai aiškiai matyti iš Europos teisminio ir policijos bendradarbiavimo subjektams suteiktų ribotų įgaliojimų: nepaisant kai kurių veiksmų, kuriais siekiama atnaujinti ES tarptautinio bendradarbiavimo subjektų struktūrą (pavyzdžiui Eurojusto ar Europolo organizacijų stiprinimas[6]) nė vienai iš šių įstaigų nebuvo

[3] 1995 m. liepos 26 d. Konvencija, grindžiama Europos Sąjungos sutarties K.3 straipsniu, dėl Europos policijos biuro įsteigimo (Europolo konvencija).

[4] 1998 m. birželio 29 d. Tarybos priimti remiantis Europos Sąjungos sutarties K.3 straipsniu dėl Europos teisminio tinklo sukūrimo (98/428/TVR)

[5] 2002 m. vasario 28 d. Tarybos sprendimas įkuriantis Eurojustą siekiant sustiprinti kovą su sunkiais nusikaltimais (2002/187/TVR)

[6] 2008 m. gruodžio 16 d. Tarybos sprendimas 2009/426/TVR dėl Eurojusto stiprinimo, iš dalies keičiantį Sprendimą 2002/187/TVR, įsteigiantį Eurojustą siekiant sustiprinti kovą su sunkiais nusikaltimais, arba 2009

suteikti privalomi įgaliojimai nacionalinių valdžios institucijų atžvilgiu. Kiti sunkumai, su kuriais susidurta derybose dėl tarpusavio pripažinimo priemonių priėmus Pagrindų sprendimą dėl Europos arešto orderio[7], ir jo įgyvendinimo nacionaliniu lygmeniu vėlavimas ir nesilaikymas taip pat buvo šio pasipriešinimo požymis. Galiausiai, daugiausiai problemų kėlė nacionalinių baudžiamųjų įstatymų suderinamumo klausimas, kadangi teisės aktų suderinimas nacionaliniais lygiais buvo paviršutiniškas dėl valstybėms narėms suteiktos didelės diskrecijos.

2009 m. gruodžio 1 d. įsigaliojus Lisabonos sutarčiai, buvo padaryta esminių pokyčių tarptautinio bendradarbiavimo srityje. Lisabonos sutartimi panaikintas trečiasis ramstis, kuris reglamentavo policijos ir teisminį bendradarbiavimą baudžiamosiose bylose, ir vietoje jo pradėtas taikyti Bendrijos metodas (trečiasis ramstis buvo perkeltas į Sutarties dėl Europos sąjungos veikimo (SESV)[8] III dalies V antraštinę dalį, kurioje teisminis bendradarbiavimas ir policijos bendradarbiavimas buvo atskirtas į skirtingus skyrius). Pagrindiniai pokyčiai apėmė institucinę struktūrą ir sprendimų priėmimo procedūras teisminiame ir policijos bendradarbiavime, leidžiant sprendimus priimti kvalifikuota balsų dauguma Taryboje ir reikalaujant Europos Parlamento pritarimo. Tai reiškia, kad valstybės narės prarado galimybę blokuoti sprendimus vienbalsiu veto, skatinant jas aktyviau ieškoti kompromisų. Lisabonos sutartis taip pat sustiprino ES teisminę kontrolę baudžiamojo teisingumo srityje, išplėsdama Europos Teisingumo Teismo jurisdikciją ir užtikrindama, kad ES teisės aktai būtų taikomi baudžiamojo proceso srityje. Tarp jų aktualūs tapo reglamentai ir direktyvos. Tai bene svarbiausias pokytis ES mastu, kadangi reglamentai yra tiesiogiai taikomi valstybėse narėse, o direktyvoms, esant ES Teisingumo Teismo apibrėžtoms sąlygoms, gali būti taikomas vertikalusis tiesioginis veikimas, kuris reiškia, kad privatus asmuo gali remtis direktyvos nuostatomis, jei valstybė narė jas netinkamai įgyvendino arba visiškai neįgyvendino. Be to, sutartyje nustatyti aiškesni teisiniai pagrindai nacionalinių įstatymų suderinimui baudžiamojoje teisėje ir proceso srityse, taip pat sustiprintos Eurojusto ir Europolo agentūrų galios ir numatyta Europos prokuratūros įsteigimo galimybė (įsteigta 2017 m. spalio 12 d.).

Visi šie pakeitimai sudarė glaudesnio bendradarbiavimo galimybes, tačiau nepaisant šių teigiamų pokyčių, kai kurios valstybės narės pasinaudojo galimybėmis neprisijungti prie tam tikrų sutarties aspektų, sukurdamos taip vadinamąją „kintamąją geometriją“ (angl.

m. balandžio 6 d. Tarybos sprendimas 2009/371/TVR dėl Europos policijos biuro (Europolo) įsteigimo įgyvendinimo

[7] 2002 m. birželio 13 d. Tarybos pagrindų sprendimas dėl Europos arešto orderio ir perdavimo tarp valstybių narių tvarkos (2002/584/TVR)

[8] Anksčiau buvusi Europos bendrijos sutartis arba kitaip pirmasis ramstis

variable geometry) ES baudžiamojo teisingumo srityje (Weyembergh, 2018, p. 193). Tai sąvoka, atsiradusi dėl skirtingo ES valstybių narių dalyvavimo ir įsipareigojimo baudžiamosios teisenos bendradarbiavimo srityje. Šiame kontekste tai reiškia, kad ne visos ES šalys vienodai taiko visus Lisabonos sutarties aspektus, kai kuriais atvejais leidžiant tam tikrą lankstumą dalyvavime ar įgyvendinime. Tokia situacija susidarė dėl to, kad vienoms valstybėms buvo suteikta galimybė tam tikromis sąlygomis blokuoti konkrečios teisinės priemonės priėmimą arba suteikta galimybė visai atsisakyti dalyvauti. Ypač išsiskyrė Danija, Jungtinė Karalystė (žinoma dabar tai tapo nebeaktualu atsižvelgiant į Didžiosios Britanijos išstojimą iš Europos Sąjungos po 2016 m. birželio 23 d. referendumo) ir Airija. Danija, pasinaudodama Amsterdamo sutartyje įtvirtintu specialiu statusu dėl prieglobsčio, imigracijos, vizų ir civilinės teisenos, nusprendė išplėsti savo atsisakymo teisę ir įtraukti bendradarbiavimo baudžiamosiose bylose sritį. Ji dalyvauja tik toje apimtyje įgyvendinant bendradarbiavimą baudžiamosiose bylose, kiek tai apima Šengeno sutartis. Airija ir Jungtinė Karalystė, kuri jau yra išstojusi iš Europos Sąjungos, nebuvo visiškai integruotos į Šengeno erdvę, kadangi nepritarė vidaus sienų kontrolės panaikinimui, naudojosi *à la carte* tvarka, leidžiančia joms selektyviai dalyvauti baudžiamosios justicijos priemonėse kiekvienu konkrečiu atveju. Dėl to, tai iki šiol kelia daugelį problemų ir kitų valstybių narių nepasitenkinimą, kadangi kiekvienu konkrečiu teisinės pagalbos atveju, šios šalys (Airija ir Danija) turi labai didelę diskreciją ir gali atsisakyti tenkinti kitos valstybės prašymą.

Tačiau nepaisant to, Lisabonos sutartimi buvo sudarytos palankesnės sąlygos glaudesniam norinčių valstybių narių bendradarbiavimui, ypač tais atvejais, kai priimant tam tikras priemones nepavykdavo pasiekti vieningo sutarimo. Šis mechanizmas leidžia valstybių narių grupei sparčiau siekti pažangos konkrečiose srityse, net jei kai kurios valstybės narės atsisako arba pasinaudoja veto teise. Nors šios nuostatos suteikia lankstumo, tačiau tuo pačiu, sudaro sudėtingą ir nenuoseklią ES baudžiamosios teisenos sistemą. Skirtingas dalyvavimo ir įsipareigojimo lygis gali turėti įtakos ES baudžiamojo teisingumo erdvės ir veikimo nuoseklumui ir veiksmingumui, nes yra sukuriama aplinka, kurioje valstybės narės gali pasirinkti įsitraukimo lygį.

Po Lisabonos sutarties įsigaliojimo, didesnis dėmesys buvo skirtas teisės aktų derinimui baudžiamosiose bylose, ypatingai materialiojoje teisėse, kurioje buvo priimtos svarbios direktyvos, siekiant kriminalizuoti ir suvienodinti pavojingiausias nusikalstamas veikas, o baudžiamosios teisės proceso srityje buvo pasiekta pažanga stiprinant tarpusavio pripažinimo principą, taip galiausiai išvystyta ir įgyvendindama Europos baudžiamojo teisingumo erdvės koncepcija.

Apibendrinant galima teigti, kad baudžiamosios justicijos tarptautinio bendradarbiavimo ES istorinė raida buvo ganėtinai dinamiška. Nors pačioje pradžioje ES nebuvo jokių nuostatų ar tikslų, kurie apimtų tarpvalstybinį bendradarbiavimą baudžiamojoje justicijoje, tačiau vėliau jis buvo įtrauktas į ES sutartis, išlaikant bendradarbiavimą tik tarpvyriausybinį, o galiausiai priimant Lisabonos sutartį, tarptautinis bendradarbiavimas baudžiamojoje justicijoje visiškai integruotas į ES teisinę sistemą. Vis dėlto, pakitusi sistema nėra iki galo nuosekli ir yra susiduriama su iššūkiais, kurie siejami su valstybių diskrecija.

1.2. Tarptautinio bendradarbiavimo baudžiamojoje justicijoje rūšys, formos ir vieta Lietuvos teisės sistemoje

Dabartinis tarptautinis teisinis bendradarbiavimas, kitaip dar vadinamoji teisinė (savitarpio) pagalba, baudžiamosiose bylose vyksta tik teisiniu pagrindu. Tarptautinio teisinio bendradarbiavimo su užsienio valstybių teisėsaugos institucijomis ir teismais, taip pat ir tarptautinėmis institucijomis tvarką nustato Lietuvos Respublikos baudžiamasis kodeksas (toliau – BK), Baudžiamojo proceso kodeksas (toliau – BPK), Bausmių vykdymo kodeksas bei Lietuvos Respublikos tarptautinės sutartys, kurios gali būti skirstomos pagal prisijungusiųjų skaičių: į dvišales, trišales ir daugiašales, arba pagal turinio apimtį: universaliąsias, apimančias didelę teisinės pagalbos formų įvairovę, ir specialiąsias, apimančias tik vieną teisinės pagalbos formą arba teisinę pagalbą tik konkrečių nusikalstamų veikų atžvilgiu (Čepas, Švedas, 2008). Tačiau, tarptautinės sutarties nebuvimas neužkerta kelio teisinei pagalbai, nei teikti prašymą kitai šaliai, nei vykdyti kitos šalies prašymą. Bet tokiais atvejais nei viena iš valstybių nėra įpareigota vykdyti, o prašymų vykdyti apimtis, tvarka bei atsisakymo pagrindai sureguliuoti kiekvienos valstybės nacionaliniuose įstatymuose.

Kai kurie mokslininkai (pavyzdžiui, de Amicis, Kostoris, Lovrich, Gaffney ir kt.) išskiria tarptautinį bendradarbiavimą į „vertikalųjį“ ir „horizontalųjį“. Vertikaliajame bendradarbiavime vyrauja priklausomybės santykiai, kai bendradarbiavimo sąnaudos ir nauda yra labai asimetriški skirtingų valdžios lygių dalyviams (Carr, Gerber, Lupher, 2008). Kitaip tariant, vertikalusis bendradarbiavimas suprantamas kaip skirtingų valdžios lygių arba tos pačios organizacijos skirtingų lygių bendradarbiavimas. Vertikalusis bendradarbiavimas baudžiamojoje justicijoje vyksta tarp centralizuotų administracinių ir policijos įstaigų. Joms yra priskiriamos valstybių narių teisminės ir policijos institucijos, tarptautinės ar Europos sąjungos centrinės įstaigos, tokios kaip Interpolas, Eurojustas, Europolas, Europos prokuratūra ir kt. Be centralizuoto lygmens koordinavimo, vargu ar galima būtų veiksmingai kovoti su tarpvalstybiniais nusikaltimais. Jų veikla, vykstanti iš

aukštesnio, Europos, lygio į žemesnį, nacionalinį, parodo, jog šis bendradarbiavimo modelis yra „vertikalus“ - skiriamas nuo „horizontaliojo“ bendradarbiavimo, kuris įvyksta, kai šalys bendrauja tiesiogiai viena su kita. Vertikalusis bendradarbiavimas padeda sukurti bendrą teisminę erdvę remiantis Europos teritoriškumo principais ir teismo sprendimų laisvu judėjimu. Svarbu paminėti, kad šis „vertikalumas“ nereiškia institucijų pavaldumo viena kitos atžvilgiu ir neturi tiesioginių įgaliojimų prieš valstybių narių institucijas, jų tikslas yra paremti ir padėti ikiteisminiams tyrimams tarptautiniu lygmeniu (de Amicis, Kostoris, 2018, p. 201–247).

Horizontalusis bendradarbiavimas vyksta tarp to paties lygmens valdžios institucijų arba organizacijų, kurių funkcijos panašios, bet kurios veikia skirtingose jurisdikcijose ar srityse. Pavyzdžiui, kaimyniniai policijos departamentai gali bendradarbiauti kovodami su nusikalstamumu, kuris daro įtaką jų atitinkamoms teritorijoms. Horizontalaus bendradarbiavimo tikslas – pasidalinti geriausia praktika tarp institucijų, koordinuoti tyrimus ir baudžiamąjį persekiojimą, taip pat stiprinti institucijų pajėgumus, kad būtų galima kuo greičiau ir operatyviau užkirsti kelią nusikalstamai veikai arba surasti nusikalstamos veikos kaltininkus ir patraukti atsakomybėn. Tiek vertikalusis, tiek horizontalusis bendradarbiavimas yra svarbūs siekiant užtikrinti baudžiamosios justicijos veiksmingumą tarptautiniu lygmeniu (Bergström, Cornell, 2011, p. 30).

Nors kai kurie mokslininkai savo darbuose akcentuoja tokį išskyrimą, tačiau darbo autorės nuomone, toks išskyrimas nėra būtinas (visgi daugumoje teisės doktrinos autorių darbuose nėra užsimenama apie tokį skirstymą) ir kartais toks išskyrimas atrodo beprasmiškai, kadangi tarptautinio bendradarbiavimo esmė yra ne pačios institucijos ar jų tarpusavio santykis, o teisinė pagalba siekiant bendro teisinio gėrio, kuris yra sudrumsčiamas nusikalstamoms veikoms peržengiant nacionalinės jurisdikcijos ribas.

Vis dėlto, analizuojant skirtingų autorių konstruojamoje tarptautinio bendradarbiavimo sampratą, Lietuvos Respublikos baudžiamąjį kodeksą, darytina išvada, kad tarpvalstybinis teisinis bendradarbiavimas gali būti įgyvendinamas įvairiomis formomis (Belevičius, 2013, p. 174):

- asmens, įtariamo ar kaltinamo padarius nusikaltimą, perdavimas ar išdavimas kitai valstybei ar tarptautinei teisminei institucijai, vykdančiai tokio asmens baudžiamąjį persekiojimą (tokia savitarpio pagalbos forma apima ekstradiciją, Europos arešto orderį, asmens perdavimą Tarptautiniam baudžiamajam teismui);
- baudžiamojo persekiojimo perdavimas – perėmimas;

- proceso veiksmų atlikimas (liudytojo, įtariamojo, kaltinamojo apklausos (įprastiniu ir nuotoliniu būdu), ekspertizė, apžiūra, dokumentų ir daiktinių įrodymų perdavimas, informacijos rinkimas ir pateikimas ir kt.);
- procesinės prievartos priemonių taikymas kitos valstybės teritorijoje (sekimas, krata, poėmis, elektroninių ryšių tinklais perduodamos informacijos perėmimas, kontroliuojamas gabenimas, slaptieji tyrimai ir kt.);
- bausmės vykdymo perdavimas - perėmimas.

Toks išskirstymas leidžia daryti prielaidas, kokioje baudžiamojo persekiojimo stadijoje vyksta bendradarbiavimas ir kokia teisinė institucija yra už tai atsakinga. Konkrečiai kiekviena šių formų plačiau darbe nebus nagrinėjama, kadangi Lietuvos teisinėje doktrinoje yra ganėtinai plačiai aptarta[9] ir yra susiformavusi gana aiški jų taikymo praktika.

Lietuvos Respublikoje tarptautinis bendradarbiavimas baudžiamojoje justicijoje dažniausiai suprantamas kaip nusikalstamų veikų prevencijos, tyrimo bei teismų priimtų sprendimų vykdymas, kai tarptautinių sutarčių bei Europos Sąjungos teisės nustatytais pagrindais kartu veikia ne mažiau kaip dvi valstybės arba valstybė ir tarptautinė organizacija ar Europos Sąjungos institucija (Kaupinis, 2016, p. 10). Dažniausiai tarptautinis bendradarbiavimas pasitelkiamas tada, kai nusikalstama veika turi „užsienio elementą“ (įtariamasis arba auka yra užsienietis, nusikalstama veika padaryta kitos valstybės jurisdikcijoje arba bylai reikalingi duomenys, kurie gali turėti reikšmės tiriant nusikalstamą veiką ir vėliau gali būti pripažinti įrodymais, yra kitoje valstybėje) ir reikia atlikti tam tikrus procesinius veiksmus, gauti duomenų ar dalintis informacija su užsienio ar tarptautinėmis institucijomis. Lietuvoje BPK IV skyrius numato taisykles dėl Lietuvos Respublikos teismų ir prokuratūros susižinojimo su užsienio valstybių įstaigomis ir tarptautinėmis organizacijomis. 66 str. numatyta bendra tvarka, kad prašymai siunčiami ir įgyvendinami per Lietuvos Respublikos teisingumo ministeriją ar Lietuvos Respublikos generalinę prokuratūrą, o esant neatidėliotinoms aplinkybėms per Eurojustą (Lietuvos Respublikos baudžiamojo proceso kodeksas, 2002). Įstatymų ir tarptautinių sutarčių numatytais atvejais, įmanomas ir tiesioginis bendradarbiavimas tarp užsienio žinybos institucijų (tokios situacijos susiklosto dažniausiai keičiantis informacija).

[9] Plačiau nagrinėję mokslininkai: Švedas G., Čepas A., Ažubalytė R., Namavičius J. ir kt.

2. NUSIKALTIMAI KIBERNETINĖJE ERDVĖJE IR JŲ UŽKARDYMAS PASITELKIANT TARPTAUTINĮ BENDRADARBIAVIMĄ

Šiuolaikiniame pasaulyje bendradarbiavimo svarbą didina pasauliniai iššūkiai, peržengiantys valstybių sienas ir individualius gebėjimus. Dažnai tarptautinį bendradarbiavimą apsprendžia ir pačios veikos pobūdis, kaip pavyzdžiui kibernetiniai nusikaltimai, kurie neturi sienų ir dėl to kelia daugybę sunkumų teisėsaugos institucijoms siekiant išsiaiškinti ir užkardyti kibernetines nusikalstamas veikas. Tiriant kibernetinius nusikaltimus, dėl egzistuojančio specifinio „beribiškumo“ pobūdžio, neretai susiduriama su nemenkais iššūkiais, kurie negali būti įveikiami be įvairiapusiško teisėsaugos institucijų bendradarbiavimo. Apskritai, kibernetiniai nusikaltimai yra viena iš sparčiausiai augančių nusikalstamumo sričių. Prie to prisideda ne tik greitai besivystanti technologinė kaita, bet ir nusikaltėliams patrauklūs kiti elektroninės erdvės suteikiami pranašumai, tokie kaip anonimiškumas, interneto sparta, įvairių pasaulio vietų pasiekiamumas (Chawki *et al.* 2015, p. 4). Debesų kompiuterijos (angl. *cloud computing*) pažanga padidino kibernetinių nusikaltėlių galimybes kirsti nacionalines sienas (Hooper *et al.*, 2013, p. 152). Tačiau bendradarbiavimą kibernetinių nusikaltimų atvejais apsunkina ir kultūriniai skirtumai, kurie priveda prie skirtingų kibernetinių nusikaltimų supratimo ir apibrėžimų.

2.1. Nusikaltimų kibernetinėje erdvėje samprata

Kibernetinių nusikaltimų samprata iki šiol kelia daugybę diskusijų ir nagrinėjant skirtingų autorių mokslinius darbus matyti, kad nėra aiškiai išskirtų atskaitos taškų, kuriais remiantis būtų galima apibrėžti konkrečią kibernetinių nusikaltimų sąvoką (Štitilis *et al*, 2016, p. 403). O įdomiausia yra tai, kad apibūdinant elektroninius nusikaltimus, vartojami skirtingi terminai: kompiuteriniai nusikaltimai (angl. *computer crime*), su kompiuteriais susiję nusikaltimai (angl. *computer-related crime*), aukštų technologijų nusikaltimai (angl. *high-tech crime*) (Sauliūnas *et al.* 2004, cituota Štitilis, 2011, p. 5), elektroniniai nusikaltimai, kibernetiniai nusikaltimai (angl. *cybercrime*) ir t.t., kurie tam tikrais atvejais suprantami arba *inter alia* traktuojami kaip sinonimai. Žinoma, gilinantis į kiekvieną sąvoką, išryškėja ir šių terminų skirtumai – vienos sąvokos yra platesnės ir apima kitas, pavyzdžiui, kibernetiniai nusikaltimai apima visus nusikaltimus padaromus erdvėje apjungiančioje telekomunikacinius, informacinius tinklus ir sistemas, elektroninę įrangą (Bučiūnas, 2015, p. 11), o kitos nurodo tik labai specifinius nusikaltimus. Iš pirminės pažiūros, tai neturėtų kelti problemų, kadangi naudojant bet kokį terminą, apibūdinantį kibernetinius nusikaltimus, dauguma supranta apie kokį reiškinį yra kalbama. Tačiau konkrečiai apibūdinti šį reiškinį tampa sudėtinga ir vieno visuotinai pripažinto apibrėžimo nėra.

Lietuvos baudžiamajame kodekse sutiksime tik elektroninių nusikaltimų sąvoką. Taip yra dėl to, kad Lietuvai 2004 m. ratifikavus 2001 m. lapkričio 23 d. Europos Tarybos konvenciją dėl elektroninių nusikaltimų (toliau – Budapešto Konvencija)[10] *de jure* buvo įteisintas elektroninio nusikaltimo terminas. Lyginant Konvencijos tekstą lietuvių ir originalo kalbomis – lietuviškame Konvencijos pavadinime yra minima sąvoka elektroniniai nusikaltimai, o originaliajame tekste Konvencija įtvirtina kibernetinius nusikaltimus (ang. *cybercrime*), tačiau peržvelgus visą tekstą kibernetiniai nusikaltimai yra siejami su nusikaltimais, įvykdytais internete ir kompiuterių tinkluose ir visa Konvencija kalba apie kompiuterinius nusikaltimus. Vis dėlto, Konvencija „elektroninių“ ar „kompiuterinių“ nusikaltimų sąvokos apibrėžimo nepateikia. Verta paminėti, kad įgyvendinant Budapešto Konvencijos nuostatas dėl kompiuterinių nusikaltimų, Lietuva įtvirtindama elektroninius nusikaltimus mini „elektroninių duomenų“ sąvoką, kai tuo metu Budapešto Konvencijoje yra įtvirtinta „kompiuterinių duomenų“ sąvoka. Iš to, galima daryti išvadą, kad Lietuva išplečia Konvenciją ir įgyvendindama jos nuostatas įtvirtina baudžiamajame įstatyme ne tik kompiuterinius nusikaltimus, tačiau ir elektroninius, kurie apima ir kompiuterinius nusikaltimus. Lietuvos nacionalinėje teisėje naudojamas terminas „elektroniniai duomenys“ pagal Lietuvos Aukščiausiojo Teismo (toliau – LAT) formuojamą praktiką atitinka „kompiuterinių duomenų“ sąvoką, tačiau doktrina siūlo elektroninių duomenų sąvoką aiškinti plačiau. Iš to darytina išvada, kad toks Lietuvoje naudojamos elektroninių nusikaltimų sąvokos įtvirtinimas yra sąmoningas veiksmas, kuriuo yra išplečiamas teisinis reguliavimas, kad jis apimtų ne tik kompiuterinius, kurie pasak Parker yra „tyčinės veikos, vienaip ar kitaip susijusios su kompiuteriais, dėl kurių nukentėjusysis patyrė ar galėjo patirti žalą, o nusikaltimo subjektas turėjo ar galėjo gauti iš to naudos“ (Parker, 1989, p. 3), bet ir visus elektroninius nusikaltimus.

Tęsiant toliau apie kibernetinių nusikaltimų sampratą ir jos nevienodą supratimą, tarp mokslininkų ir tyrinėtojų yra manančių, kad nereikia per daug gilintis į šį fenomeną. Antai, kriminologo P. Grabosky nuomone, kibernetiniai nusikaltimai - tai tradicinė nusikalstama veika, vykdoma elektroninėmis priemonėmis. Todėl neturėtume per daug analizuoti ir lįsti į šių nusikaltimų sampratas, kai visa tai veda prie tų pačių tradicinių teisės normų pažeidimų. Autorius virtualius nusikaltimus prilygina „senam vynui naujuose buteliuose“, pabrėždamas, kad pagrindinis skirtumas nuo tradicinio nusikalstamumo yra naudojami įrankiai – kompiuteriai (Grabosky, 2001, p. 243). Galima sutikti, kad visi kibernetiniai

[10] Council of Europe, Committee of Experts on Crime in Cyber-Space, European Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No 185, *pasiekiama per internetą:* https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf

nusikaltimai turi keletą tradicinių nusikaltimų sudėties elementų. Todėl kyla klausimas, kodėl reikia elektroninius nusikaltimus išskirti kaip atskirą fenomeną. Tačiau ar tikrai dalies nusikaltimų sudėties požymių buvimas leidžia asmenis patraukti baudžiamojon atsakomybėn, remiantis tradicinių nusikaltimų normomis? Iš baudžiamosios teisės principų žinoma, kad baudžiamoji teisė yra *ultima ratio* priemonė ir tam, kad būtų galima asmeniui inkriminuoti baudžiamajame įstatyme įtvirtintą veiką, ji turi atitikti visus atitinkamo baudžiamojo įstatymo normos sudėties požymius.

Daugelis mokslininkų nesutinka su P. Grabosky požiūriu ir technologijų atsiradimas verčia diskutuoti apie unikalius elektroninių nusikaltimų aspektus. N. Kshetri patikslina elektroninių nusikaltimų apibrėžtį, nurodydama, kad jie apima nusikaltimus, kurių pagrindinė nusikaltimo padarymo priemonė yra kompiuteriai arba kompiuterių tinklai (Kshetri, 2009, p. 1). Tai sukuria pagrindą naujoms nusikalstamoms veikos formoms bei modeliams. Tiek P. Grabosky, tiek N.Kshetri apibrėžimai šiuolaikiniame pasaulyje kelia abejonių, jie yra netikslūs, tačiau juos apjungus galima išvesti kiek tikslesnę kibernetinių nusikaltimų sąvoką. Apibendrinta elektroninių nusikaltimų apibrėžtis gali būti tokia „neteisėti veiksmai, kai kompiuteris yra įrankis ar taikinys arba ir įrankis, ir taikinys kartu“ (Chawki *et. al*, 2015 p. 3). Vėlgi, atsižvelgiant į kintantį ir sparčiai technologine prasme tobulėjantį pasaulį, pateiktas apibrėžimas taip pat nebūtų tikslus. Turint omenyje ryšių technologijų eksponentinį augimą, kompiuteris nebėra vienintelis įrankis ar būdas norit pasiekti kibernetinę erdvę ar elektroninius duomenis. Kibernetinių nusikaltimų sąvokoje kompiuteris turi būti pašalintas kaip vienas iš pagrindinių sąvokoje esančių elementų, o visas pagrindas turi atsiremti į kibernetinę erdvę.

M. Yar kompiuterinius nusikaltimus laiko visiškai nauju reiškiniu, kadangi kibernetinė erdvė sudaro galimybę beveik akimirksniu tarp dviejų dalyvių sukurti sąveiką. Kibernetinė erdvė sugriauna atstumo ir laiko barjerus, sukuria galimybę bendrauti su neribotu kiekiu žmonių, sudaro prielaidas anonimiškumui bei tapatybės keičiamumui. Neretai, kompiuteriniais nusikaltimais yra vadinamos, bet kokios nusikalstamos veikos, kurios turi nors menkiausią ryšį su kompiuteriais ar informacinėmis technologijomis (Yar, 2013, p. 9-12). Tačiau ar tikrai vien tik elektroninių prietaisų ar bet kokio prietaiso, kuris gali prisijungti prie interneto ryšio, panaudojimas nusikaltimui automatiškai priskiriamas prie kibernetinių nusikaltimų? Pasak J. Marcinauskaitės, kibernetinės erdvės saugumas yra baudžiamojo įstatymo saugomas papildomas objektas. Kibernetiniai nusikaltimai yra ne tik tradicinės nusikalstamos veikos, vykdomos pasitelkiant šiuolaikines technologijas, bet ir kėsinimasis į pačios kibernetinės erdvės saugumą (Marcinauskaitė, 2011). Todėl, atsižvelgiant į šią nuostatą ir atsakant į prieš tai pateiktą dilemą, elektroninis prietaisas turi

būti pagrindinė atakos prieš kibernetinės erdvės saugumą priemonė, kad būtų galima tokį nusikaltimą priskirti kibernetiniams nusikaltimams (Panomariovaitė, Zokaitė, 2021, p. 237).

Žinoma, pirmiausiai reikėtų suprasti, kas apskritai yra ta kibernetinė erdvė. Lietuvos Respublikos kibernetinio saugumo įstatymas 2 str. 6 d. apibrėžia, kad *kibernetinė erdvė – aplinka, kurią sudaro kompiuteriai ir kita ryšių ir informacinių technologijų įranga ir juose sukuriama ir (arba) jais perduodama elektroninė informacija*. Kitaip tariant, kibernetinė erdvė apima ne tik internetą, bet ir visą skaitmeninį, virtualų pasaulį, kuriame laikomi ar sukuriami skaitmeniniai duomenys, informacijos duomenų keitimosi srautai ar ryšiai tarp skirtingų elektroninių prietaisų.

Tos pačios nuomonės laikosi ir kriminologijos profesorius D.S. Wall. Kriminologas pasiūlė išplėsti kibernetinių nusikaltimų sąvoką, ir ją apibūdina, kaip „Kibernetiniai nusikaltimai yra nusikalstama arba žalinga veikla, kuri yra informacinė, pasaulinė ir tinklinė, ir ją reikia skirti nuo nusikaltimų, kai kompiuteris yra tik paprasčiausia priemonė ir nieko daugiau. Jie yra tinklinių technologijų, kurios pakeitė nusikalstamo darbo pasidalijimą ir suteikė visiškai naujų galimybių ir naujų nusikaltimų formų, paprastai susijusių su informacijos ir jos vertės įgijimu ar manipuliavimu pasauliniuose tinkluose siekiant pasipelnyti, produktas. Juos galima suskirstyti į nusikaltimus, susijusius su sistemos vientisumu; nusikaltimus, kai kompiuterių tinklas naudojamas nusikaltimams vykdyti; ir nusikaltimus, susijusius su kompiuterių turiniu (Wall, 2007, p. 4). Šis apibrėžimas gana tiksliai apibūdina šių nusikaltimų sampratą ir yra vertingas tuo, kad jis apima įvairių formų kibernetinius nusikaltimus. Nepaisant to, galima būtų ginčytis dėl kai kurių šio apibrėžimo aspektų. Atkreiptinas dėmesys, kad nors dažniausiai manipuliavimas pasitelkiamas kibernetinėje erdvėje ar apskritai tokio pobūdžio nusikaltimai daromi siekiant materialinės naudos, tačiau tikslas virtualių nusikaltimų gali būti nukreiptas ir į kitas savanaudiškas paskatas. Kibernetinių nusikaltimų motyvai, be finansinės naudos, gali būti smalsumas, pasitenkinimas, galios ar pripažinimo troškimas, kerštas, „sportinis interesas“, politika ar religija ar kt. (Sabillon *et al.*, 2016, p. 3).

Apibendrinant, galima teigti, kad kibernetiniai nusikaltimai - tai nusikalstama veika, nukreipta prieš kompiuterį, kompiuterių tinklą, tinklinį įrenginį ar kibernetinę erdvę arba nusikalstama veika padaryta naudojant kompiuterį, kompiuterių tinklą ar tinklinį įrenginį arba pačioje kibernetinėje erdvėje.

2.2. Kibernetinių nusikaltimų keliami iššūkiai.

Kibernetiniai nusikaltimai kelia nemažai iššūkių, įskaitant sunkumus atliekant tyrimus dėl jų tarpvalstybinio pobūdžio, netinkamos teisinės sistemos ir nusikaltėlių, kurie gali veikti skirtingose jurisdikcijose nei jų aukos, buvimo vietos ar jų pačių asmenybės nustatymo.

Autorius J. Clough išskiria net 6 probleminius aspektus, kurie padidina kibernetinį nusikalstamumą ir apsunkina šių nusikaltimų išaiškinamumą (Clough, 2010, p. 5-8). Pirmoji problema – nusikaltimų mastas. Remiantis statistikos duomenimis 5,35 milijardai pasaulyje žmonių, kurie sudaro 66,2 proc. visos Pasaulio populiacijos, turi prieigą ir naudojasi internetu (Statista, 2024). Tai sudaro labai platų potencialių nusikaltėlių bei aukų ratą ir leidžia padaryti nusikaltimą tokiu dideliu mastu, kurio nebūtų įmanoma padaryti įprastu būdu, nesinaudojant skaitmeninėmis technologijomis. Pasaulinė kibernetinių nusikaltimų padaryta žala siekia šimtus milijardų eurų per metus ir ši tendencija nuolat auga (Nacionalinė kibernetinio saugumo strategija, 2022, p. 10). Didelį nusikaltimų mastą sudaro ir nemaža skirtingų kibernetinių rūšių nusikaltimų įvairovė. Ne tik finansiniai, bet visi duomenys apskritai labai domina nusikaltėlius, duomenų pažeidimų skaičius vis didėja. Dabartiniais laikais, kai viskas yra skaitmenizuota, visi duomenys saugomi duomenų debesyse, įskaitant sveikatos korteles, slaptažodžius, valstybės paslaptis, projektus ir kt. (J. Clough nurodo, tai kaip dar vieną problematinį aspektą, kad duomenis galima lengvai suskaitmenizuoti ir perkelti į skaitmeninę erdvę). Pažeidėjams tapo lengviau pasiekti didelius informacijos duomenų srautus neišėjus iš namų ir įvykdyti didelio masto pažeidimus, kurie apima skirtingų pažeidimų rūšis, lyginat su įprastais nusikaltimo būdais.

Iš šios problemos kyla kita – lengvas prieinamumas. Tik atsiradus pirmiesiems kompiuteriams, jų prieinamumas asmeninių poreikių tenkinimui paprastiems asmenims buvo sunkiai realizuojamas. Kompiuteriai buvo dideli, spintos dydžio, užimdavo daug vietos patalpoje, sudėtingi ir brangūs įrenginiai, kuriuos naudodavo vyriausybės, mokslinių tyrimų ir finansų institucijos. Galimybę daryti kompiuterinio pobūdžio nusikaltimus turėjo tik tie asmenys, kurie turėjo prieigą ir specialiąsias žinias. Šiandien skaitmeninėmis technologijomis taip patobulėjus, jomis gali naudotis visi. O ką jau kalbėti, kad dauguma šeimų, turi tokią prieigą namuose. Eurostato duomenimis, 2016 metais netgi 85 proc. visos Europos namų ūkių turi namuose prieigą prie interneto (Eurostat, 2018). Tai irgi lemia didesnį įtariamųjų ir nukentėjusiųjų ratą. Taip pat, prieinamumas lėmė ne tik tai, kad vis daugiau asmenų, gali pasiekti skaitmenines technologijas, tačiau ir tai, kad šiuolaikiniame pasaulyje internetu galime įsigyti prekių, kurios palengvina nusikaltimo darymo metodus ar padeda nuslėpti padarytas nusikalstamas veikas, kaip antai programinės įrangos įrankių, leidžiančių vartotojui rasti kompiuterinių sistemų spragas arba įveikti

slaptažodžių apsaugas. Iš to išplaukia, kad norint atlikti nusikalstamus veiksmus nebereikia specialių įgūdžių, o užtenka apsukrumo ir noro.

Trečioji problema – anonimiškumas. Anonimiškumas kibernetinėje erdvėje gali padrąsinti nusikaltėlius ir leisti jiems veikti tariamai nebaudžiamai. Pažeidėjai gali sąmoningai nuslėpti savo tapatybę internete, naudodami tarpinius serverius, VPN sistemą, keisdami IP adresus ar susikurti ar suklastoti netikrus elektroninius paštus ar kitus identifikacijai naudojamus būdus. Konfidencialumas gali būti apsaugotas naudojant lengvai prieinamas šifravimo technologijas, o skaitmeninius pėdsakus galima pašalinti naudojant įprastą programinę įrangą. Šiuolaikinių ryšių tinklinis pobūdis savaime reiškia, kad duomenys, prieš pasiekdami paskirties vietą, paprastai yra perduodami per kelis kanalus, kurie netgi būna skirtingose jurisdikcijose (Chawki *et al*, 2015, p. 9). Nusikaltėliai dažnai specialiai mėto pėdsakus tam, kad būtų sunku atsekti nusikaltimo padarymo ir paskirties vietas, o netgi neretai ir tuos pačius duomenis laiko skirtingose vietose ar tose jurisdikcijose, kuriose teisinė reguliavimo ir priežiūros sistema yra ganėtinai silpna ar chaotiška. Tai dar labiau apsunkina nusikaltimų atskleidimą ar pažeidėjo tapatybės nustatymą.

Ketvirta, pasaulinis pasiekiamumas. Asmenys neišėję iš namų, informacinių technologijų pagalba gali pasiekti bet kurią pasaulio vietą. Dažnai tokio pobūdžio nusikaltimų kaltininkai veikia kitoje jurisdikcijoje, nei yra jų aukos. Pažeidimai gali būti padaromi netgi keliose jurisdikcijose tuo pačiu metu. Tas labai apsunkina ne tik susekamumą, tačiau ir kelia nemenkų problemų teisėsaugai dėl jurisdikcijos taikymo ir su juo susijusios nusikalstamos vietos padarymo nustatymo kibernetinėje erdvėje. Tradiciškai valstybės baudžiamosios teisės nuostatos taikomos tik tos šalies jurisdikcijoje, o ji yra įgyvendinama principais, kurie apibrėžia tos valstybės baudžiamųjų įstatymų galiojimą erdvėje. Jurisdikciją dažniausiai apsprendžia teritorinis principas, kuris gali būti išplėstas remiantis eksteritorinės erdvės principais (Nevera, 2006, p. 12). Šie principai yra taikomi nustatant nusikalstamos veikos padarymo vietą ne tik fizinėje erdvėje, tačiau ir kibernetinėje. Nors tarptautiniai ir ES teisės aktai numato kriterijus, kuriais vadovaujantis galima nustatyti jurisdikciją, tačiau esminė problema, yra ta, kad kibernetinio pobūdžio veikos apima kelias jurisdikcijas ir tarptautinis bendradarbiavimas yra neišvengiamas norint patraukti atsakomybėn asmenį, padariusį tokią veiką. Pastebėta, jog teisėsaugos institucijos yra mažiau linkusios vykdyti baudžiamąjį persekiojimą už kibernetinio pobūdžio nusikaltimus tais atvejais, kai padaryta palyginti nedidelė žala ir tai reikalauja arba duomenų išsireikalavimo iš kitos šalies jurisdikcijos arba netgi pažeidėjo ekstradicijos (Wei-Jung, 2020, p. 4).

Paskutinę problemą J. Clough būtent ir išskiria sudėtingą aptikimo ir patraukimo baudžiamojon atsakomybėn procesą. Nepastovus elektroninių duomenų pobūdis reikalauja sudėtingų kriminalistikos metodų, kad būtų užtikrintas skaitmeninių duomenų atkūrimas, išsaugojimas ir tinkamumas naudoti juos baudžiamajame procese. Iššūkį kelia ir tai, kad egzistuoja didelis vartotojų skaičius, o dėl šiuolaikinių komunikacijų tinklinio pobūdžio labai sudėtinga vykdyti stebėjimą. Be to, daugumą duomenų esančių skaitmeninėje erdvėje gali pasiekti ir valdo privačios institucijos ir skaitmeninių paslaugų teikėjai, o tas reiškia, kad teisėsaugos institucijos turi bendrauti su daug skirtingų subjektų, įskaitant ir privačius duomenų tvarkytojus, kas dar labiau apsunkina teisėsaugos institucijų darbą, kadangi privatūs sektoriai nėra linkę noriai bendradarbiauti, nebent jie yra nusikalstamos veikos aukos. Ryšiai paprastai perduodami per kelias jurisdikcijas, todėl būtina vietos teisėsaugos institucijų pagalba (Fantino, 2009, cituota Chawki *et al*, 2015, p. 20). Tarptautinėse sutartyse įtvirtintos savitarpio pagalbos procedūros, kurios yra begalo apsunkinančios, reikalauja diplomatinių kanalų įsitraukimo, o tas gali užtrukti labai ilgai, kartais net ištisus metus (Daskal, 2017, cituota Tosza, 2021, p. 9). Žinoma, ES viskas vyksta žymiai greičiau, nes tam tikrais atvejais institucijos gali tiesiogiai kreiptis į skaitmeninių duomenų tvarkytojus[11]. Net ir su duomenų tvarkytojų ar vietos teisėsaugos institucijų pagalba, duomenų saugojimas gali būti ribotas arba iš viso neegzistuoti, pavyzdžiui dėl duomenų apsaugos teisės aktų, negalima kaupti tokių duomenų arba dėl specifinės duomenų infrastruktūros nėra aišku, kur yra laikomi duomenys (Franssen, 2017, p. 534). Pavyzdžiui, naudojantis debesijos technologijomis, kaip „Google“, duomenys yra „suskaidomi“ į daugybę mažų dalelių, kurios yra saugomos visiškai skirtingose vietose (Tosza, 2021, p. 8). Dėl to, ne tik duomenų atkūrimas gali būti beveik neįmanomas, tačiau ir nėra aišku, kurioje vietoje yra tie duomenys, o iš to kyla ir klausimas, kurios valstybės(-ių) teisę taikyti ir kuri atsakinga. Turint omenyje tai, kad tinklo duomenų srautas yra trumpalaikis, duomenis reikia fiksuoti, kol jie yra perduodami. Juos užfiksavus lieka tik kopijos, o jų palyginimas su pirminiais duomenimis yra praktiškai nebeįmanomas (Casey, 2011, p. 31).

Be to, atviruose tinkluose yra begalė duomenų, o ieškoti juose naudingos informacijos, kuri padėtų baudžiamajam tyrimui reikalauja daug laiko ir kitų išteklių ir tai dar labiau gali apsunkinti tyrimą.

Dar vieną problemą galimą išskirti, tai šių nusikalstamų veikų latentiškumo pobūdį. Pasak N. Kshetri, elektroniniai nusikaltimai yra vieni latentiškiausių iš visų nusikalstamumo rūšių (Kshetri, 2010, p. 64). Tai lemia keli faktoriai (Štitilis, 2011, p. 6):

[11] Pavyzdžiui, Lietuvos Respublikos kibernetinio saugumo įstatyme yra numatyta, kuriais atvejais teisėsaugos institucijos gali tiesiogiai paprašyti skaitmeninių duomenų iš tam tikrų duomenų tvarkytojų.

1. Informacinių technologijų naudotojai dažnai neturi pakankamai žinių pastebėti tokiems nusikaltimams.
2. Aukos vengia informuoti apie aptiktus kompiuterinius nusikaltimus. Verslo srityje šis nenoras susijęs su dviem dalykais:

- vienos aukos nenori atskleisti informacijos apie savo darbą, bijodamos viešumo arba prarasti gerą vardą;
- kitos aukos bijo prarasti investuotoją, visuomenės pasitikėjimą.

Prie antrojo faktoriaus keli autoriai dar išskiria ir tai, kad aukos gali patirti daugiau žalos pranešdamos apie tokius nusikaltimus, nei dėl pačios nusikalstamos veikos. Tą apima gėdos jausmas, pagrindiniai darbuotojai įpareigojami rinkti reikšmingus duomenis, kurie vėliau pripažįstami įrodymais byloje, liudyti. Taip pat, teisinės išlaidos, padidėjusios draudimo įmokos ir netgi saugumo pažeidimų atskleidimas (Parker, 1998, p. 10; Chawki *et al*., 2015, p. 9)

Veiksmingam reguliavimui reikia įvairių priemonių, kuriomis būtų sprendžiami įvairūs su kibernetiniais nusikaltimais susiję klausimai ir problemos, tokios kaip nusikaltimų mastas, lengvas prieinamumas, anonimiškumas, leidžiantis nusikaltėliams veikti tariamai nepastebimai, pasaulinis pasiekiamumas, latentiškumas, kurios lemia sudėtingą aptikimo ir ištyrimo procesą. Tai rodo, kad kovoti su tokio pobūdžio nusikaltimais yra sudėtinga, ir pabrėžia pažangių teisinių ir teisėsaugos strategijų poreikį, kad būtų veiksmingai sprendžiami šie šiuolaikiniai iššūkiai.

2.3. Pirmasis tarptautinis teisės aktas apimantis tarptautinį bendradarbiavimą tiriant kibernetinius nusikaltimus ir iš jo kylanti bendradarbiavimo problematika

Užkardyti kibernetinio pobūdžio nusikalstamas veikas gali būti įmanoma tik gerinant tarptautinį bendradarbiavimą, kuris skatina nuoseklų kibernetinių nusikaltimų apibrėžimą ir baudžiamąjį persekiojimą bendradarbiaujančiose šalyse (Brenner, 2002, cituota Payne, 2020, p. 13).

Pirmasis ir bene svarbiausias dokumentas, reglamentuojantis tarptautinį bendradarbiavimo pareigą elektroniniuose nusikaltimuose yra 2001 m. Europos Tarybos Budapešto Konvencija (ETS Nr. 185) ir 2022 m. gegužės 12 d. pasirodęs jos antrasis papildomas protokolas (CETS Nr. 224). Budapešto konvencija, oficialiai vadinama Konvencija dėl elektroninių nusikaltimų, yra tarptautinė sutartis, skirta kovai su kibernetiniu nusikalstamumu. Ji buvo priimta Europos Tarybos 2001 m. lapkričio 23 d. Budapešte ir įsigaliojo 2004 m. liepos 1 d. Budapešto Konvenciją ratifikavo 68 valstybės, įskaitant visas Europos Tarybos nares ir keletą kitų Europos ir Šiaurės Amerikos valstybių

(23 ne ES valstybės)[12]. Šia konvencija buvo siekiama suderinti nacionalinius įstatymus kibernetinio nusikalstamumo srityje, pagerinti teisėsaugos institucijų tarpusavio bendradarbiavimą tiriant ir vykdant baudžiamąjį persekiojimą. Pagrindiniai Budapešto Konvencijos rengėjų rūpesčiai buvo dvejopi: pirmiausia, jie norėjo užtikrinti, kad nusikaltimų apibrėžimai būtų pakankamai lankstūs, kad būtų galima prisitaikyti prie naujų nusikaltimų ir jų padarymo metodų, ypatingai, kai jie taip sparčiai evoliucionuoja ir antra, projekto rengėjai norėjo, kad Konvencija liktų jautri valstybių vidiniams teisiniams režimams. Tai kėlė nemenkus iššūkius ypač žmogaus teisių srityje, nes kiekviena valstybė turi skirtingas moralines ir kultūrines vertybes (Hopkins, 2003, p. 105). Pavyzdžiui, Europos Sąjungoje duomenų apsaugos reglamentavimas yra griežtesnis nei Jungtinėse Amerikos Valstijose. Siekiant įgyvendinti Budapešto Konvencijos tikslus, buvo numatyta teisė šalims apriboti ar panaikinti tam tikrų nusikaltimų kriminalizavimą ir apriboti tyrimo procedūras taikant šioje konvencijoje numatytas išlygas[13]. Tarptautinio bendradarbiavimo nuostatos yra įtvirtintos Konvencijos III skyriuje ir apima nuostatas susijusias su ekstradicija, abipusio pripažinimo principu, taip pat numato specialias taisykles dėl duomenų skaitmeninėje erdvėje pasiekiamumo (ypač, kai nereikia kitos šalies sutikimo duomenims pasiekti) ir bendradarbiavimo renkant elektroninius įrodymus. Konvencija įpareigoja šalis nusistatyti įrodymų rinkimo procedūras, įskaitant pagreitintas paieškas ir duomenų rinkimą bei saugojimą, kadangi elektroniniai duomenys yra labai greitai pažeidžiami ar sunaikinami. Konkrečiai, Budapešto Konvencija reikalauja, kad valstybė, iš kurios kilęs kibernetinis nusikaltimas, pakenktosios šalies prašymu, saugotų ir atskleistų duomenis prašančiajai valstybei. Tačiau Budapešto Konvencijoje nėra nurodyta, ką teisėsaugos institucija turi įrodyti prieš gaudama potencialiai privačią informaciją. Dėl šios priežasties, praktinis šios Konvencijos įgyvendinimas savitarpio pagalbos srityje tarp valstybių, turinčių skirtingą žmogaus teisių apsaugą, yra sudėtingas.

Dar vienas probleminis aspektas kyla dėl nevienodų nacionalinių įstatymų, reglamentuojančių duomenų rinkimo, saugojimo apimtį ir jų išdavimą kitai valstybei.

[12] Europos Tarybos oficialus internetinis tinklapis. Budapešto konvencijos šalys: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 [žiūrėta 2024-03-19]

[13] *Supra* n. (10), Budapešto konvencijos 6 str. 3 d. (leidžiantis valstybei apriboti nusikaltimus, susijusius su „netinkamų įtaisų naudojimu“), 9 str. 4 d. (leidžianti valstybėms netaikyti arba dalinai taikyti nuostatas susijusias su nusikaltimais dėl vaikų pornografijos), 10 str. 3 d. (leidžianti valstybėms pasilikti teisę ribotomis aplinkybėmis nenustatyti baudžiamosios atsakomybės, už autorių teisių pažeidimus, jei yra kitų veiksmingų gynimo priemonių), 11 str. 3 d. (leidžianti valstybei apriboti arba panaikinti baudžiamąją atsakomybę už sąmoningą pasikėsinimą), 14 str. 3 d. (procesinių nuostatų taikymo apribojimas), 22 str. 2 d. (leidžianti valstybėms netaikyti arba dalinai taikyti numatytas jurisdikcijos taisykles), 29 str. 4 d. (atsisakymas vykdyti savitarpio pagalbą, susijusią su duomenų paieška arba panašia prieiga, areštu ar panašiu poėmiu arba su jų atskleidimu, dėl dvigubo baudžiamumo sąlygos) ir 42 str. (nustatantis valstybių išlygų pateikimo tvarką).

Konfliktas kyla tada, kai informaciją išduodančiosios šalies įstatymai prašančiajai šaliai leidžia surinkti ir perduoti daugiau informacijos, nei tai leidžia prašomosios valstybės jos pačios nacionaliniai teisės aktai. Tada kyla klausimas, ar išduodančioji valstybė galėtų išduoti daugiau duomenų negu prašančioji pati galėtų išduoti, jei būtų atvirkštinė situacija (Hopkins, 2003, p. 116). Be to, Konvencija leidžia valstybėms individualiai nusistatyti kibernetinių nusikaltimų sunkumo laipsnį, kurio reikia, kad jos galėtų iššifruoti ar surinkti reikiamus duomenis, kas gali pakenkti kitai valstybei, pradėjusiai baudžiamąjį persekiojimą dėl konkrečios kibernetinės veikos. Reikia paminėti, kad, apskritai, įžvelgiant privačių duomenų jautrų aspektą, Budapešto Konvencija leidžia valstybėms narėms nusistatyti konkrečią taikymo apimtį, kas liečia duomenų rinkimo ir saugojimo aspektus. Taip pat, yra numatyta, kad pasirašiusios šalys turi nusistatyti apsaugos priemones, jog būtų išlaikytas balansą tarp žmogaus teisių ir kibernetinių nusikaltimų tyrimo. Deja, bet Konvencija šių apsaugos priemonių nekonkretizuoja ar nereikalauja, kad šios apsaugos priemonės būtų suderintos su kitais tarptautiniais teisės aktais (Akdeniz, 2002, p. 231). Vadinasi, kad nors Konvencija ir atkreipia dėmesį į duomenų apsaugos svarbą, tačiau jos neužtikrina.

Kai kurie mokslininkai išskiria ir didelę finansinę ir resursinę naštą, kurią įnešė Budapešto Konvencija, kadangi ji neapima išlaidų, susijusių su duomenų rinkimu, perėmimu, saugojimu, apmokėjimo. Kritikai mano, kad tai užkrauna didelę naštą paslaugų tiekėjams saugoti duomenis ir atlikti papildomas apskaitos funkcijas bei reikalauja ne tik finansinių, tačiau ir žmogiškųjų išteklių (Godwin, 2001; Steinhard, 2001; Hopkins, 2003, p. 116). Konvencija turėtų numatyti nuostatą dėl tyrimo išlaidų paskirstymo.

2022 m. gegužės 12 d. Antrasis Budapešto Konvencijos papildomas protokolas (toliau – II Protokolas) būtent ir skirtas sustiprinti tarptautinį bendradarbiavimą, atsižvelgiant į naujausias technologines pažangas ir augantį kibernetinių nusikaltimų skaičių ir siekiant užpildyti esamas Budapešto Konvencijoje spragas dėl savitarpio pagalbos. Nors II Papildomą protokolą pasirašė 41 valstybė, tačiau jis vis dar nėra įsigaliojęs, kadangi jį turi ratifikuoti bent 5 Europos Tarybos narės[14]. Protokolas sukuria naujas procedūras, leidžiančias teisėsaugos institucijoms greičiau ir efektyviau bendradarbiauti tarptautiniu lygmeniu, apeinant centrines bendradarbiavimo institucijas, tačiau kartu užtikrinant ir numatant konkretesnes garantijas dėl žmogaus teisių (ypatingai bandant apsaugoti asmenų privatumą ir asmens duomenis), nei tai buvo numatyta Budapešto Konvencijoje, aukšto lygmens apsaugą asmenims ir atitiktį ES duomenų

[14] Europos Tarybos internetinis tinklapis. Nuoroda: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 [žiūrėta 2024-03-19]

apsaugos standartams. Protokolas numato galimybę rinkti liudytojų ar ekspertų parodymus vaizdo konferencijos būdu. Taip pat numatyta galimybė tiesiogiai bendradarbiauti su paslaugų tiekėjais ir skaitmeninių duomenų tvarkytojais, bei numatytos bendradarbiavimo taisyklės esant ekstremalioms situacijoms, kai reikia reaguoti itin skubiai.

Budapešto Konvencija padėjo pirmuosius žingsnius nacionalinių šalių įstatymų suderinimui dėl elektroninių nusikaltimų ir tapo pagrindiniu tarptautiniu dokumentu, nustatančiu standartus ir bendradarbiavimo principus kibernetinio nusikalstamumo srityje visame pasaulyje. Žinoma, kaip ir kitos tarptautinės sutartys, paliko labai daug vietos valstybių diskrecijai, kas trukdo nuosekliam ir greitam kibernetinių nusikaltimų išaiškinimui ir užkardymui.

3. TARPTAUTINIS BENDRADARBIAVIMAS DĖL ELEKTRONINIŲ ĮRODYMŲ[15] GAVIMO KIBERNETINIŲ NUSIKALTIMŲ BYLOSE

3.1. Savitarpio teisinė pagalba ir jos trūkumai

Savitarpio teisinė pagalba baudžiamosiose bylose yra numatytoji teisinė sistema skirta pagerinti šalių teisėsaugos institucijų efektyvumą tiriant nusikaltimus, persekiojant už juos ir užkertant jiems kelią. Tai yra dviejų ar daugiau valstybių susitarimas (pagal sutartį), teikti viena kitai pagalbą baudžiamaisiais teisiniais klausimais. Pagalbos rūšys, paprastai, apima dokumentų įteikimą, kratos ir arešto prašymų vykdymą, asmenų parodymų arba pareiškimų ėmimą, dokumentų, protokolų ir kitų įkalčių pateikimą, asmenų ar daiktų buvimo vietos ar tapatybės nustatymą ir kitus procesinius veiksmus. Pačiose sutartyse nors yra nurodyti veiksmai, dėl kurių susitariama teikti teisinę pagalbą, tačiau patį veiksmo procesą reglamentuoja kiekvienos šalies nacionaliniai įstatymai. Todėl galima teigti, kad visas savitarpio pagalbos procesas yra vidaus teisės ir sutarties tarp atitinkamų valstybių derinys.

Darbo temos kontekste, kibernetinių nusikaltimų tyrimui yra labai svarbūs duomenys, esantys kibernetinėje erdvėje ir dėl to reikėtų kalbėti apie savitarpio teisinę pagalbą, kurią teisėsauga naudoja siekdama gauti duomenis esančius už savo nacionalinės teisės ribų. Kitaip tariant, tais atvejais, kai duomenys laikomi užsienyje arba paslaugų teikėjas vienaip ar kitaip neveikia atitinkamoje šalyje, dėl ko jam būtų taikomos prievolės, kylančios iš tos šalies teisės. Europos Sąjungoje teisėsaugos institucijos gali iš esmės pasinaudoti Europos tyrimo orderiu, kuris bus aptartas vėliau. Tačiau, jei duomenų turi būti prašoma iš ES nepriklausančios valstybės, tokiu atveju, turi būti remiamasi savitarpio pagalbos sutartimi. Jungtinės Amerikos Valstijos yra viena iš pagrindinių ES valstybių narių savitarpio teisinės pagalbos prašymų dėl prieigos prie elektroninių duomenų gavėjų, jei ne pagrindinė, nes didžiausi paslaugų teikėjai, tokie kaip „Google“ (kuriai priklauso ir „Youtube“), „Microsoft“, „Meta“ („Facebook“, „Instagram“) yra įsikūrę JAV. Jungtinės Amerikos Valstijos ir Europos Sąjunga pasirašė savitarpio teisinės pagalbos susitarimą 2003 m. birželio 6 d., kuris įsigaliojo 2010 m. vasario 1 d. Tačiau šis susitarimas susijęs tik su kai kuriais bendradarbiavimo aspektais ir jame nėra teisinio pagrindo prašyti skaitmeninių duomenų. Pastarieji turi būti reglamentuoti kiekvienos ES valstybės narės dvišaliame susitarime su JAV. Lietuva su JAV savitarpio pagalbos sutartį yra pasirašiusi 1998 m., tačiau į sutartį nėra įtrauktos konkrečios nuostatos dėl duomenų gavimo, todėl

[15] Šiame skyriuje kalbėdami apie elektroninių duomenų surinkimą nesigilinsime į Lietuvos Respublikos BPK kūrėjų nurodomus terminų skirtumus tarp „duomenų“ ir „įrodymų“, atsižvelgiant į baudžiamojo proceso stadiją. ES institucijos teisės aktuose nurodo ir vartoja e. įrodymų sąvoką neišskiriant duomenų pripažinimo įrodymais specifiškumo, kaip tai yra nurodyta BPK, ir „duomenys“ bei „įrodymai“ šiuo atveju yra vartojami kaip sinonimai.

turėtų būti taikomos bendrosios nuostatos. Procedūra panaši kaip ir kitose savitarpio teisinės pagalbos sutartyse. Pagal sutartį reikalaujama, kad institucija, siekianti gauti duomenis, nusiųstų prašymą savo šalies centrinei institucijai, Lietuvos atveju – Teisingumo ministerijai ar Generalinei prokuratūrai, o po to ši perduoda prašymą JAV - Generaliniam prokurorui ar jo paskirtam asmeniui (Lietuvos Respublikos Vyriausybės ir Jungtinių..., 1998, 2 str.). Šiuo atveju, policija turėtų kreiptis į Generalinę prokuratūrą, kad ši išduotų prašymą JAV, be kita ko, prieš išduodama prašymą turi patikrinti tokio prašymo teisėtumą. 5 str. numatyta, kad prašymai yra vykdomi laikantis prašymą gavusios valstybės įstatymų, dėl to JAV savo ruožtu turi patikrinti ar toks prašymas ir išdavimas yra galimas pagal JAV įstatymus. Vadinasi, tiek viena, tiek kita valstybė turi vertinti savo nacionalinius teisės aktus ir prašymo išdavimas ar jo vykdymas turi atitikti valstybės įstatymus. Be to, prašymai neapsiriboja tik valstybių centrinėmis institucijomis, savo ruožtu, prašymą tenkinanti valstybė turi surinkti reikiamus duomenis iš savo teisėsaugos institucijų ar paslaugų teikėjų. Dėl šios priežasties, savitarpio teisinės pagalbos procesas gali užtrukti ilgai.

Duomenų gavimą apsunkina bei dar labiau prailgina prašymo įvykdymo procesą JAV įrodinėjimo standartas dėl tikėtinos priežasties (kad prašomi duomenys yra nusikaltimo įrodymai) (Daskal, 2017, p. 3). Šis reikalavimas, kylantis iš JAV Konstitucijos 4-osios pataisos, yra plačiai nagrinėjamas teismų praktikoje, tačiau praktikoje vis dar lieka neaiškus. Kadangi Europos teisėjai su juo nėra susipažinę, neretai jie susiduria su sunkumais taikydami šį standartą, o tai gerokai užvilkina procedūrą (Tosza, 2019, p. 272). Šią problemą jau pripažino Europos Komisija, skyrusi nemažai lėšų Europos teisėjų mokymui šiuo klausimu (Europos Komisija, 2017, p. 3). Be trukmės ir tikėtinos priežasties reikalavimo (kuris taip pat turi įtakos trukmei), savitarpio pagalbos sistema turi ir kitų trūkumų, kaip nurodyta Komisijos neoficialiame dokumente, kuriame apibendrinamas Komisijos atliktas ES valstybių narių šiuo klausimu vertinimas (Europos Komisija, 2016, p. 5). Visų pirma, valstybės narės įvardijo, kad savitarpio pagalba yra pernelyg sudėtinga ir reikalaujanti daug išteklių, atsižvelgiant į pirmiau aptartą procedūrą, kurioje dalyvauja įvairios abiejų šalių institucijos. Antra, prašymų priimtinumas priklauso nuo priimančiosios šalies teisinės sistemos, dėl ko prašymai dažnai yra nepatenkinami (tai apima ne tik tikėtinos priežasties reikalavimą, tačiau ir duomenų neperdavimą dėl duomenų ištrynimo, abipusio baudžiamumo nebūvimo ar dėl neišsamių ar netinkamų prašymų). Taip pat susiduriama su problema dėl perdavimo priemonių netinkamumo, nes dauguma valstybių narių naudojasi laiškais, faksu arba elektroniniu paštu, o saugiais kanalais naudojasi labai nedaug šalių.

Nors savitarpio pagalba yra vienas iš būdų siekiant užkardyti nusikalstamas veikas, tačiau toks procesas dažniausiai trunka ilgai ir dėl skirtingų valstybių teisinių sistemų, tikslas gali būti nepasiektas.

3.2. Europos tyrimo orderis

2014 m. balandžio 3 d. Europos Parlamento ir Tarybos priimta direktyva 2014/41/ES dėl Europos tyrimo orderio baudžiamosiose bylose (toliau ir - ETO) buvo svarbus žingsnis į priekį teisminio bendradarbiavimo baudžiamosiose bylose ES srityje. Jis tapo pagrindine teisine priemone tarpvalstybiniams įrodymams rinkti ir pakeitė tradicines savitarpio pagalbos sutartis, kurios iki šiol daugiausia buvo naudojamos šiam tikslui. Be kita ko, jis padeda lengviau gauti duomenis iš juridinių asmenų, esančių kitoje valstybėje narėje nei ta, kurioje atliekamas tyrimas. Vis dėlto, verta paminėti, kad ETO nebuvo sukurtas atsižvelgiant būtent į skaitmeninių duomenų rinkimą, kuris yra svarbus kibernetinių nusikaltimų tyrimui. Visos ETO nurodytos priemonės yra nukreiptos į „realaus pasaulio“ duomenų (kalbant apie kibernetinių nusikaltimų tyrimus, tokia priemonė gali būti panaudota tik telefono numerio ar IP adreso nustatymui), finansų įstaigose esančius duomenų rinkimą arba į „gyvą“ ryšių perėmimą (Tosza, 2019, p. 277). Renkant duomenis išduodant Europos tyrimo orderį, buvo pastebėta, kad kibernetinių nusikaltimų tyrimams tai nėra veiksmingas mechanizmas dėl elektroninių duomenų nepastovumo ir ETO nustatytos taikymo procedūros. ETO grindžiamas abipusio pripažinimo principu ir praktiškai veikia taip pat, kaip ir kitos ES abipusio pripažinimo priemonės, pavyzdžiui, Europos arešto orderis. Taikant tokią procedūrą, dalyvauja abiejų valstybių teisminės institucijos, ir tik priėmus ar patvirtinus kitos valstybės teismo sprendimą siekiant gauti įrodymus, vykdančiosios valstybės kompetentinga institucija gali nurodyti interneto paslaugų teikėjui pateikti duomenis. Ne tik taikymo procedūra sumažina tokio mechanizmo naudojimą, bet ir ETO direktyvoje numatyti terminai taip pat gali būti laikomi per lėtais skaitmeninio pasaulio poreikiams. Europos tyrimo orderiui vykdyti skirtas 90 dienų terminas, po to, kai jau buvo nustatytas ilgas 30 dienų terminas sprendimui dėl Europos tyrimo orderio pripažinimo arba vykdymo priimti, yra labai ilgas (Europos tyrimo orderio direktyvos 12 str. 3 d. ir 4 d.). Skubi procedūra, deja, bet nėra numatyta. Kaip nurodyta Direktyvos 12 str. 2d. tyrimo orderį išduodančioji institucija gali prašyti trumpesnio termino, o vykdančioji institucija „*turi kuo labiau atsižvelgti į šį reikalavimą*“, tačiau tokia nuostata nesukuria teisinės prievolės skubiau įvykdyti prašymą.

Taigi, nors Europos tyrimo orderis padėjo pirmuosius žingsnius siekiant palengvinti įrodymų rinkimą baudžiamosiose bylose, tačiau toks duomenų rinkimas yra ganėtinai ilgas

procesas ir nėra efektyvus kibernetinių nusikalstamų veikų tyrimui, atsižvelgiant į elektroninių duomenų nepastovumą.

3.3. Privačių skaitmeninių paslaugų teikėjų bendradarbiavimas su teisėsaugos institucijomis

Nusikaltimams persikėlus į kibernetinę erdvę, policija ir teisminės institucijos kasdien susiduria su elektroninių duomenų, kurie vėliau gali būti pripažįstami įrodymais, rinkimo problema. Iššūkį kelia tai, kad informaciją, kuria nusikaltėliai dalijasi arba saugo naudodamiesi interneto paslaugomis ir (ar) informacinėmis ir ryšių technologijomis (toliau - IRT), paprastai apdoroja bei valdo privačios bendrovės (technologijų įmonės arba skaitmeninių paslaugų teikėjai), todėl be šių privačių subjektų bendradarbiavimo ji nėra prieinama valdžios institucijoms. Nesant jų pagalbai, teisėsaugos institucijos paprasčiausiai negali nustatyti, tirti ir (arba) patraukti baudžiamojon atsakomybėn atsakingus asmenis už kibernetinėje erdvėje įvykdytas nusikalstamas veikas. Privačių subjektų pasitelkimas vykdant baudžiamąjį persekiojimą nėra visiškai naujas dalykas. Pavyzdžiui, finansų įstaigos įpareigotos vykdyti pinigų plovimo prevenciją Lietuvoje jau nuo 1998 m. (Matevičius, 2020, p. 46). Tačiau net ir kitais atvejais teisėsaugos ir IRT paslaugas teikiančių bendrovių bendradarbiavimas nėra naujiena - policija ir teisminės institucijos jau dešimtmečius bendradarbiauja su telekomunikacijų operatoriais ir paslaugų teikėjais (Franssen, 2018). Dažniausiai tokiais atvejais privatūs subjektai gali atlikti dvejopas funkcijas. Pirma, tai pačio skaitmeninio turinio priežiūra ir kova su neteisėtu turiniu internete. Šiuo atveju paslaugų teikėjai atlieka itin svarbų vaidmenį stebint ir pašalinant neteisėtą turinį. Iš vienos pusės tai yra subjektų pareiga, kuri reglamentuojama nacionaliniais teisės aktais, tačiau ir patys paslaugų teikėjai aktyviai ir savanoriškai tą daro.

Bet kuriuo atveju, kyla moralinė dilema tarp žmogaus teisių, konkrečiai žodžio ir saviraiškos laisvės, užtikrinimo asmenims, kurie naudojasi kibernetine erdve ir paslaugų teikėjų teikiamomis internetinėmis ar skaitmeninėmis paslaugomis, ir nusikalstamų veikų atskleidimo ar jų prevencijos. Ir, antra, skaitmeninių duomenų, kurie vėliau gali būti pripažįstami įrodymais, rinkimas ikiteisminiam tyrimui, kai paslaugų teikėjų bendradarbiavimas tapo būtinybe teisėsaugos institucijoms, siekiančioms gauti tokio pobūdžio duomenis. Dažnai tarpvalstybinis prieigos prie duomenų aspektas sukūrė sąlygas, kuriomis paslaugų teikėjai turi įvertinti teisėsaugos institucijų prašymų teisėtumą ir proporcingumą, o jų vaidmuo tampa panašus į viešųjų subjektų (Tosza, 2021, p. 2). Apskritai, teisėsaugos institucijos vis dažniau ėmėsi savanoriško skaitmeninių paslaugų teikėjų bendradarbiavimo. Žinoma, tokios formos bendradarbiavimas priklauso nuo to, ar nėra tokio bendradarbiavimo draudimo teisės aktuose, taikomuose paslaugų teikėjams ir

nuo paslaugų teikėjų noro bendradarbiauti. Kadangi bendradarbiavimas tarp teisėsaugos institucijų ir paslaugų teikėjų nėra privalomas, priklausomai nuo kiekvienos valstybės nacionalinės teisės, nėra jokios garantijos, kad skaitmeninių paslaugų teikėjai iš tikrųjų pateiks prašomus duomenis. O bendradarbiavimas su užsienio teisėsaugos institucijomis gali būti netgi uždraustas, pavyzdžiui, Jungtinėse Amerikos Valstijose (toliau – JAV) yra uždrausta perduoti duomenis kitų valstybių teisėsaugai, jei tai yra turinio duomenys[16] (Daskal, 2018, p. 220). Tačiau su turiniu nesusiję duomenys gali būti savanoriškai perduoti JAV skaitmeninių paslaugų teikėjų kitų valstybių teisėsaugos institucijoms. Kadangi nėra konkrečios teisinės sistemos būtent savarankiško pobūdžio pagalbai, paslaugų teikėjai patys turi nusistatyti taisykles, kaip vertinti iš užsienio gaunamus prašymus bei turi įvertinti tokių prašymų tikrumą ir teisėtumą (Tosza, 2021, p. 9). Ir tokiais atvejais kyla grėsmė pažeisti žmogaus teises ir užkraunama didelė atsakomybė ant skaitmeninių paslaugų teikėjų. Iš kitos pusės, gavus tokius duomenis iš skaitmeninių paslaugų teikėjų, gali kilti problemų dėl tokiu būdu surinktų įrodymų leistinumo. Vis dėlto, savanoriškumo aspektas gali ir įpareigoti perduoti duomenis, net kai kyla kolizija su trečiųjų valstybių teisės aktais. Pavyzdžiui, Belgija „savanoriškumą“ byloje su „Yahoo“[17] išaiškino kaip skaitmeninių paslaugų teikėjo savanorišką pasirinkimą teikti paslaugas Belgijoje, kai galima nustatyti ryšį (atsižvelgiant į domeno pavadinimą, paslaugų kalbas ir tikslinę reklamą) su šalimi. Dėl šios priežasties, ją saisto vietos prievolės. Šioje byloje Belgija skyrė baudą „Yahoo“ kompanijai, esančiai Kalifornijoje, kuri atsisakė pateikti šalies institucijoms IP adresus asmens, įtariamo padarius elektroninį sukčiavimą, norėdama apsaugoti savo vartotojų duomenis ir nepažeisdama JAV teisės dėl asmens duomenų perdavimo. JAV bendrovė atsisakymą pateikti duomenis grindė ir tuo, kad Belgija savo baudžiamuosius įstatymus taiko ekstrateritorialiai, tačiau turėtų remtis tik teritoriškumo principu ir atsakomybę taikyti tik tiems paslaugų teikėjams, kurie yra registruoti Belgijoje, o kadangi „Yahoo“ nėra įsisteigus Belgijoje ir nėra jokio „fizinio“ buvimo (t. y. neturi būstinės ar infrastruktūros), jai negali būti taikomos Belgijos teisės aktuose numatytos pareigos. Antverpeno apeliacinis teismas nurodė, kad kaltinimai dėl ekstrateritorialumo galėtų būti priimtini tik tuo atveju, jei būtų prašoma perduoti duomenis ar objektus, esančius JAV, su kuriais nėra jokio Belgijos teritorinio ryšio, ir jei šių objektų ar duomenų turėtojas nėra pasiekiamas Belgijoje

[16] Ši nuostata įtraukta į Jungtinių Amerikos Valstijų 18 kodekso (18 U.S.C.) 2702 straipsnį. Nuo 2018 m. yra taikomos išimtys, kai JAV priėmė teisės aktą „Cloud Act“. Tokių duomenų perdavimas leidžiamas tik JAV ir atitinkamos šalies susitarimu pagal „Cloud Act“, atsižvelgiant į valstybių vertybinių principų ir asmenų privatumo standartų vertinimą.

[17] Eurojust pateikia visa bylos nagrinėjimo santrauką 2016 m. „Cybercrime Judicial Monitor“ leidinyje. Prieiga per internetą: https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2016-06_CJM-1_EN.pdf p. 14 - 31

(fiziškai ar virtualiai). Belgijos Aukščiausiasis teismas patvirtino apeliacinio teismo argumentus ir nurodė, kad „Yahoo“ „savanoriškai“ paklūsta Belgijos teisei, nes aktyviai dalyvauja Belgijos ekonominiame gyvenime. Vėliau toks požiūris kodifikuotas ir Belgijos baudžiamajame kodekse. Kita vertus, toks savavališkas teritorinio principo išplėtimas gali turėti poveikį kitų valstybių suverenitetui (Franssen, 2017, p. 225). Be to, nacionaliniai teisės aktai ir praktika taip pat sukuria prieštaringas teisines prievoles paslaugų teikėjams ir kelia rimtų sunkumų siekiant veiksmingai apsaugoti įtariamųjų ir neįtariamųjų pagrindines teises (žr. ten pat).

Lietuvos Respublikos kibernetinio saugumo įstatymas 11 str. 1 d. 4 p. numato kibernetinio saugumo subjektams pareigą „*teikti policijai informaciją, reikalingą teisės pažeidimams, turintiems nusikalstamų veikų požymių, kibernetinėje erdvėje užkardyti ir tirti, ir vykdo kitus policijos nurodymus*“. Įstatyme minimas kibernetinio saugumo subjektas reiškia, kad tai subjektas*, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų elektroninių ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas*, paslaugas teikiantis Lietuvos Respublikoje ir (arba) kitose Europos Sąjungos valstybėse narėse (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014). Vadinasi, pareiga apima privačius skaitmeninių duomenų tvarkytojus esančius ne tik Lietuvoje, bet ir Europos Sąjungoje, vykdančius veiklą Lietuvoje. Įdomu yra tai, kad nors įstatyme pareiga numatyta beveik visiems subjektams, kurie teikia ir vykdo paslaugas elektroninėje erdvėje Lietuvoje ir (ar) ES (pareiga neapima mažų ir labai mažų įmonių), tačiau Lietuvos policijos generalinio komisaro įsakyme dėl informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veiklos požymių, užkardyti ir tirti, pateikimo, numatyta pareiga surinkti reikalingus duomenis, tiriant kibernetinius incidentus, susijusius nusikalstamomis veikomis, apima tik viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių, elektroninės informacijos prieglobos paslaugas teikiančius subjektus, kitaip dar įsakyme vartojama sąvoka „*informacijos teikėjas*“ (Lietuvos policijos generalinio komisaro įsakymas..., 2015). Analizuojant kibernetinio įstatymo ir generalinio komisaro įsakymo pakeitimus, ši klaida galėjo įsipainioti dėl neapdairaus įstatymų leidėjo veiksmų, kadangi pareiga ir kitiems skaitmeninių paslaugų teikėjams atsirado tik įsigaliojus 2018 m. liepos 4 d. kibernetinio saugumo įstatymo pataisoms (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2018), o paskutinė policijos generalinio komisaro įsakymo redakcija galioja nuo 2018 m. vasario 20 d. (Lietuvos policijos generalinio komisaro įsakymas..., 2018). Nepaisant to, įsakymas turi galioti ir kitoms institucijoms, nurodytoms kibernetinio saugumo įstatyme.

Kaip nurodyta įstatyme ir įsakyme, pareiga bendradarbiauti su policija apima tik informacijos perdavimą policijai, kai policiją tokį prašymą pateikia skaitmeninių paslaugų teikėjui. Ji neapima pareigos patiems pastebėjus apie tariamus neteisėtus veiksmus, kurie galėtų būti kibernetinės nusikalstamos veikos, pranešti reikalingoms institucijoms. Tačiau privatūs subjektai tai gali atlikti savanoriškai, o ypač mažos ir labai mažos įmonės bendradarbiauja tik savanorišku pagrindu, kitaip tariant nėra įpareigotos teikti informaciją ir pranešti apie galimus kibernetinius pažeidimus. Valstybinio audito duomenimis, tik 19 iš 143 auditorių apklaustų kibernetinio saugumo subjektų praneša policijai apie kibernetinius incidentus, kurie galimai yra nusikalstamos veikos elektroninėje erdvėje (Valstybinio audito ataskaita, 2020, p. 8). Tiek mažai pranešančių yra dėl to, kad kibernetinio saugumo subjektai nežino kaip atpažinti ir reaguoti į nusikalstamas veikas ir kaip įvertinti nusikalstamos veikos nuostolį ar žalą.

Nepaisant to, kad teisės aktai numato teisėsaugos institucijų teisę kreiptis į privačius skaitmeninių paslaugų teikėjus, ir tam tikrais atvejais net įpareigoja išduoti reikalingus duomenis, ne tik nacionaliniu mastu, bet ir Europos Sąjungoje, tačiau toks bendradarbiavimas tampa vis sudėtingesnis. Atsiranda naujų IRT ir daugelį jų teikia paslaugų teikėjai, kurie nėra kibernetinio saugumo subjektai, taip pat dėl daugelio pasaulinių interneto paslaugų teikėjų (tokių kaip „Meta“, „Google“, „Microsoft“ ir kt.), kurie yra už tyrimą atliekančių teisėsaugos institucijų teritorijos ribų, masto. Tokiais atvejais reikia naudoti tarpvalstybinio bendradarbiavimo priemones, teikiamas ES, tokias kaip Europos tyrimo orderį arba savitarpio teisinę pagalbą už ES ribų. Tačiau net ir šių instrumentų taikymas sukuria priešingas teisines prievoles ir nevienodą jų taikymo apimtį, kas neretai kelia nemenkų iššūkių privatiems skaitmeninių paslaugų teikėjams, kurie stengiasi atsižvelgti į teisėsaugos institucijų prašymus, kai jiems reikia atsirinkti ir žinoti, kuriuos įsakymus privalo vykdyti, o kuriuos ne. Dėl šios priežasties pasaulinėje rinkoje bandoma suvienodinti elektroninių įrodymų surinkimo ir perdavimo sistemą ir atrasti balansą tarp nusikaltimų elektroninėje erdvėje užkardymo ir asmens duomenų apsaugos.

3.4. Naujasis ES E – įrodymų teisės aktų paketas – naujas sprendimo būdas?

Pastebint kibernetinių nusikaltimų skaičiaus didėjimą ir vis dar esant nemažiems iššūkiams, kuriuos sukelia kibernetiniai nusikaltimai, kol kas trūksta konkretaus teisinio reglamentavimo modelio. Atsižvelgdama į didėjantį valstybių narių supratimą apie teisėsaugos institucijoms kylančius iššūkius, susijusius su naujomis IRT, ir jų priklausomybę nuo privačių subjektų bendradarbiavimo nustatant, tiriant nusikalstamas veikas ir vykdant baudžiamąjį persekiojimą už jas, ES Taryba 2016 m. birželio mėn.

paprašė Europos Komisijos parengti „bendrąją sistemą“ Europos Sąjungoje šiuo klausimu. 2016 m. gruodžio mėn. pateikusi pirmąją pažangos ataskaitą[18], 2017 m. gegužės mėn. Komisija paskelbė neoficialų dokumentą, kuriame pateikė keletą praktinių priemonių, skirtų tarpvalstybinei prieigai prie elektroninių įrodymų (toliau ir – e. įrodymai) tobulinti, tačiau tuo pačiu padarė išvadą, kad reikia imtis teisėkūros veiksmų, susijusių su tiesioginiu bendradarbiavimu su skaitmeninių paslaugų teikėjais - šiai išvadai vėliau pritarė „didžioji dauguma“ valstybių narių (3546-asis ES Tarybos posėdis, 2017, p. 10). Įdomu tai, kad ES Komisija nuo 2017 m. rugpjūčio 4 d. iki 2017 m. spalio 27 d. atliko tarpvalstybinę skirtingų teisėsaugos institucijų bei privačių skaitmeninių paslaugų teikėjų apklausą dėl tarpvalstybinės prieigos prie e. įrodymų, o šios apklausos rezultatai ganėtinai kontraversiški (Report of open public consultation on E-evidence, 2017) – iš vienos pusės, valstybės narės pritarė, kad reikia naujos bendros sistemos e. įrodymų gavimui, tačiau tai kėlė ir susirūpinimų dėl tam tikrų aspektų (jie bus aptarti vėliau)[19]. Galiausiai, po penkerius metus trukusių derybų, tam, kad bendradarbiavimas ne tik tarp šalių, tačiau ir tarp skaitmeninių paslaugų teikėjų būtų sklandesnis ir būtų galima greičiau ir efektyviau išaiškinti nusikaltimus, padarytus kibernetinėje erdvėje, Europos Taryba ir Europos parlamentas, 2023 m. liepos pabaigoje priėmė teisės aktus, kuriais bus įdiegta nauja elektroninių įrodymų rinkimo baudžiamosiose bylose ES sistema. Naujas e. įrodymų taisykles (angliškai dažnai vadinamas *e-evidence regulation* arba *e-evidence package*) sudaro du teisės aktai:

1) Reglamentas (ES) 2023/1543 (toliau – Reglamentas) dėl Europos įrodymų pateikimo orderių ir Europos įrodymų saugojimo orderių elektroniniams įrodymams baudžiamajame procese ir laisvės atėmimo bausmių vykdymui pasibaigus baudžiamajam procesui;

2) Direktyva (ES) 2023/1544 (toliau – Direktyva), kuria nustatomos suderintos paskirtųjų įmonių ir teisinių atstovų skyrimo elektroniniams įrodymams baudžiamajame procese rinkti taisyklės.

Pagrindinis šių naujųjų ES teisės aktų tikslas - sukurti alternatyvų, greitesnį ir veiksmingesnį mechanizmą esamoms tarptautinio bendradarbiavimo ir savitarpio teisinės pagalbos priemonėms, kad būtų konkrečiai sprendžiamos problemos, kylančios dėl e. įrodymų nepastovumo ir saugomų duomenų „vietos praradimo“ aspekto ir įteisinti naują baudžiamosios teisės reguliavimą – tiesioginį teisėsaugos institucijų ir privataus sektoriaus

[18] Prieigą per internetą: https://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf

[19] Kiekviena šalis pateikė atgalinio ryšio ataskaitą apie Komisijos siūlymą dėl tarpvalstybinės prieigos prie e. įrodymų. Prieiga per internetą: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/1453-Improving-cross-border-access-to-electronic-evidence-in-criminal-matters_en

(skaitmeninių paslaugų teikėjų) bendradarbiavimą. Visą diskusijų laikotarpį buvo stengiamasi rasti pusiausvyrą tarp veiksmingo ir efektyvaus baudžiamųjų bylų tyrimo (teisėsaugos institucijoms), teisinio tikrumo bei pagrindo (skaitmeniniams paslaugų teikėjams) ir pagrindinių teisių apsaugos (įtariamiesiems ir kitiems kibernetinės erdvės naudotojams) (Franssen, 2018).

Reglamente nustatomos taisyklės, pagal kurias valstybės narės institucija baudžiamajame procese gali išduoti Europos įrodymų pateikimo orderį (toliau – EĮPO) arba Europos įrodymų saugojimo orderį (toliau – EĮSO) ir taip (tiesiogiai) nurodyti paslaugų teikėjui, teikiančiam paslaugas Sąjungoje ir įsisteigusiam kitoje valstybėje narėje arba, jei jis neįsisteigęs, atstovaujamam teisinio atstovo kitoje valstybėje narėje, pateikti arba išsaugoti elektroninius įrodymus, neatsižvelgiant į duomenų buvimo vietą (Reglamento 1 str. 1 d.). EĮPO leidžia išduodančiosios valstybės narės teisminėms institucijoms reikalauti, kad skaitmeninis paslaugų teikėjas (netaikoma paslaugų teikėjams teikiantiems finansines paslaugas pagal Europos Parlamento ir Tarybos direktyvos 2006/123/EB 2 str. 2 d. b punktą[20]) esantis kitoje valstybėje narėje pateiktų tam tikrus reikšmingus duomenis, reikalingus baudžiamajam procesui, o EĮSO leidžia saugoti duomenis iki 60 dienų (išduodančioji institucija šį laikotarpį gali pratęsti dar 30 dienų), kad atitinkami duomenys nebūtų sunaikinti arba prarasti ir iki tol, kol bus išduotas tolesnis EĮPO. Taip pat, nustatomas privalomas 10 dienų terminas, per kurį turi būti atsakyta į įsakymą pateikti duomenis, neatidėliotinais atvejais šis terminas sutrumpinamas iki 8 valandų. Reikia paminėti, kad EĮSO ir EĮPO gali būti išduoti tik baudžiamojo proceso tikslais ir tik vykstant baudžiamajam procesui arba sprendimams dėl įkalinimo, kurių trukmė ne trumpesnė nei keturi mėnesiai (Reglamento 2 str. 2 d.). Šie įsakymai gali būti susiję su visais internetinių paslaugų saugomais duomenimis, pvz., abonentų, srauto ir turinio duomenimis. Reglamentas taikomas tik jau saugomiems duomenims, t. y. jis netaikomas duomenims, kuriuos galima tiesiogiai stebėti, ir duomenims, kurie bus sukurti ateityje. Dėl srauto duomenų (išskyrus duomenų, kurių prašoma tik siekiant nustatyti naudotojo tapatybę) ir turinio duomenims numatytas apribojimas (orderį šiems duomenims gali išduoti tik teismas, ar ikiteisminio tyrimo teisėjas). Šie duomenys gali būti naudojami tik nusikaltimams, už kuriuos išduodančiojoje valstybėje baudžiama laisvės atėmimo bausme ne mažiau kaip trejiems metams arba tam tikroms nusikalstamoms veikoms, susijusioms su elektroniniais nusikaltimais, vaikų pornografija, negrynųjų mokėjimo priemonių

[20] Netaikoma finansinėms paslaugoms, tokioms kaip, bankų, kreditavimo, draudimo ir perdraudimo, profesinių ir asmeninių pensijų, vertybinių popierių, investicijų, fondų, mokėjimo ir investavimo konsultacijų paslaugoms, įskaitant 2006/48/EB I priede išvardytas paslaugas.

padirbinėjimu ar terorizmu (Reglamento 40 - 41 punktai). Įprastinių valstybių narių savitarpio teisinės pagalbos prašymų nebereikės. Reglamentas bus taikomas nuo 2026 m. rugpjūčio 18 d. (Reglamento 34 str. 2 d.).

Direktyvoje nustatytos taisyklės dėl tam tikrų paslaugų teikėjų, kurie siūlo paslaugas Sąjungoje (t. y. paslaugas teikia daugiau nei vienoje valstybėje narėje), paskirtųjų įstaigų paskyrimo ir teisinių atstovų paskyrimo, siekiant gauti, vykdyti ir vykdyti valstybių narių kompetentingų institucijų priimtus sprendimus ir įsakymus, skirtus elektroniniams įrodymams baudžiamosiose bylose rinkti (Direktyvos 1 str. 1 d.). Teisinis atstovas veiks kaip nacionalinių institucijų teisinis kontaktinis asmuo visoje ES. Kadangi įrodymų orderiai bus teikiami tiesiogiai skaitmeninių paslaugų teikėjams, valstybių narių teisėsaugos institucijos procese nedalyvaus. Išskyrus tuos atvejus, kai paslaugų teikėjas nesilaiko nustatytų reikalavimų arba yra kitos išimtys, nurodytos Reglamente. Direktyva turi būti perkelta į nacionalinę teisę iki 2026 m. vasario 18 d. (Direktyvos 7 str. 1 d.).

3.4.1. Skaitmeninių paslaugų teikėjų ir išduodančiųjų valstybių atsakomybė

Esminis pokytis nuo kitų savitarpio pagalbos sutarčių yra tas, kad naujasis e. įrodymų taisyklių paketas leis vienos valstybės narės teisėsaugos institucijoms tiesiogiai prašyti kitos valstybės narės skaitmeninių paslaugų teikėjų pateikti prašomus duomenis iš esmės nedalyvaujant pastarosios valstybės institucijoms. Ne tik pirminiuose taisyklių rengimo dokumentuose (Pasiūlymas Europos Parlamento ir Tarybos...2018/0108, 2018), tačiau ir dabartiniame Reglamente yra numatyta, kad tais atvejais, kai paslaugų teikėjai „*mano, kad EĮPOS* (Europos įrodymų pateikimo orderio sertifikatas) *arba EĮSOS* (Europos įrodymų orderio saugojimo sertifikatas) *vykdymas galėtų pažeisti imunitetus ar privilegijas arba taisykles dėl baudžiamosios atsakomybės, susijusios su spaudos laisve ir saviraiškos laisve kitose medijose, nustatymo ir apribojimo taisykles pagal vykdymą užtikrinančios valstybės teisę, adresatas* [paslaugų teikėjas ar teisinis atstovas] *turėtų informuoti išduodančiąją instituciją ir vykdymą užtikrinančią instituciją*“ (Reglamento 57 punktas) - tai sukėlė didelę nepasitenkinimų audrą, kadangi tokiu atveju užkraunama labai didelė atsakomybė skaitmeninių paslaugų teikėjams, t. y. privačiam subjektui. Jam būtų pavesta atlikti pareigas, kurios paprastai priskiriamos valstybės narės teisminėms institucijoms, įskaitant orderio išdavimo teisėtumo, galiojimo ir jo atitikties Chartijai vertinimą (Corhay, 2023). Kas iš tiesų labai apsunkintų skaitmeninių paslaugų teikėjus, kadangi jie turėtų turėti įmonėje darbuotojų, kurie išmanytų teisės aktus ir žmogaus teisių nuostatas, bei žinotų ne tik savo nacionalinių, tačiau ir Europos Žmogaus Teisių Teismo praktiką (Direktyvos 3 str. 4 d.). Didžiausią rūpestį tai kelia mažosioms įmonėms, kadangi tai reikalauja finansinių ir

žmogiškųjų išteklių. Vis dėlto reikia pabrėžti, kad patys skaitmeninių paslaugų teikėjai nėra atsakingi už orderio teisėtumo vertinimą ir jei kyla bent menkiausia abejonė ar gali išduoti duomenis ar ne, jie turi galimybę kreiptis į vykdymą užtikrinančią instituciją (t. y. vykdymą užtikrinančios valstybės įgaliota teisėsaugos instituciją). Jie gali tik prašyti paaiškinimo, įskaitant konsultavimąsi su vykdymą užtikrinančios valstybės kompetentingomis institucijomis tiesiogiai arba per Eurojustą ar Europos teisminį tinklą, orderį išduodančią instituciją, kai mano, kad tam tikros informacijos išdavimas gali kelti grėsmę asmens duomenims ar kitoms Europos Žmogaus Teisių Konvencijoje garantuojamoms teisėms, kitaip tariant pagrindinėms Chartijos teisėms (Reglamento 5 str. 10 d.). Iš esmės, skaitmeninių paslaugų teikėjas turi tik ribotą vertinimo funkciją ir pagrindinių teisių sąlyga apsiriboja tik „akivaizdžiais“ pažeidimais, nes skaitmeninių paslaugų teikėjas negaus viso orderio, o tik sertifikatą, kuriame yra nurodyta mažiau informacijos nei pačiame orderyje. Dėl sertifikate nurodytos informacijos skaitmeninių paslaugų teikėjams bus ganėtinai sudėtinga atlikti bet kokį pagrindinių teisių vertinimą. Kaip pabrėžiama Reglamento 71 punkte „*atsakomybė užtikrinti atitinkamo orderio teisėtumą, visų pirma jo būtinumą ir proporcingumą, turėtų tekti išduodančiajai institucijai“*.

Analizuojant pradines dokumentų rengimo stadijas, ES Taryba išbraukė žmogaus teisių išlygą iš pagrindų, kuriais remdamiesi skaitmeninių paslaugų teikėjai gali atsisakyti vykdyti įrodymų orderius, ir iš pagrindų, kuriais remdamiesi skaitmeninių paslaugų teikėjai gali prieštarauti įrodymų orderio vykdymui, sąrašo (General Approach... 10206/19, 2019). Todėl atsakomybė už pagrindinių teisių apsaugą tenka tik išduodančiajai valstybei. Tai dar griežtesnis požiūris nei ES Komisijos požiūris, o bendrasis požiūris (angl. *general approach*) sulaukė griežtesnės kritikos nei ES Komisijos pasiūlymas, kuriuo buvo perkeliama pagrindinių teisių apsauga skaitmeniniams paslaugų teikėjams. ES Taryba norėjo apriboti skaitmeninio paslaugų teikėjo, kaip pagrindinių teisių saugotojo, vaidmenį. Europos Parlamentas skeptiškai vertino pasiūlymą dėl e. įrodymų, iškeldamas daug svarbių teisinių problemų. Iš tiesų, Europos Parlamento galutinėje ataskaitoje (Report on the proposal..., 2020) buvo pateikiami 267 Komisijos pasiūlymo pakeitimai, kuriais siekiama pakeisti ne tik kiekvieną atskirą ES Komisijos ir ES Tarybos projektų straipsnį, bet ir kai kuriuos svarbius šių projektų mechanizmus ir ramsčius. Europos Parlamentas, pasitelkęs Europos Parlamento piliečių laisvių, teisingumo ir vidaus reikalų (LIBE) komitetą ir jo pranešėją, iš tiesų griežtai pasisakė prieš pagrindinių teisių vertinimo perdavimą privačiam subjektui ir pareiškė, kad labai abejotina skaitmeninių paslaugų teikėjams pavesti spręsti dėl piliečių pagrindinių teisių (3rd. Working Document (A), 2019, p. 5-6). Komitetas primygtinai pabrėžė, kad svarbu išlaikyti valstybių narių institucijų, gaunančių orderį,

dalyvavimą. Galiausiai ES institucijos laikėsi Europos Parlamento požiūrio ir priimtame Reglamente išlaikė antrosios valstybės dalyvavimą procese ir pasirinko ribotą skaitmeninių paslaugų teikėjų vaidmenį. Vis dėlto, nors vykdančiosios valstybės dalyvavimas buvo įtrauktas (privalomas vykdančiosios valstybės teisėsaugos institucijos informavimas pateikus įrodymų pateikimo orderį dėl srauto ir turinio duomenų), tačiau tuo pačiu ir apribotas, nes orderį išduodančioji valstybė neprivalo informuoti vykdančiosios valstybės užtikrinimo institucijos apie orderį, kaip ir skaitmeninių paslaugų teikėjas neprivalo konsultuotis su vykdančiosios valstybės institucija dėl įrodymų orderio įvykdymo (bus aptarta vėliau).

Nors dabartiniame Reglamente iš tiesų, atsakomybė perkeliama orderį išduodančiosioms institucijoms, tačiau dėl to gali kilti kitų problemų – išduodančioji valstybė yra suinteresuota gauti elektroninius duomenis ir dėl to padarys viską, kad tuos duomenis gautų. Reglamentas nurodo, kad įrodymų pateikimo orderis turėtų būti išduodamas tik jei tai „*būtina, proporcinga tinkama ir taikytina konkrečioje byloje. Išduodančioji institucija turėtų atsižvelgti į įtariamojo ar kaltinamojo teises procese, susijusiame su nusikalstama veika, ir turėtų išduoti Europos įrodymų pateikimo orderį tik tuo atveju, jei tokį orderį būtų buvę galima tokiomis pačiomis sąlygomis išduoti panašioje nacionalinėje byloje. Vertinant, ar turėtų būti išduotas Europos įrodymų pateikimo orderis, reikėtų atsižvelgti į tai, ar toks orderis apsiriboja tuo, kas būtina pasiekti teisėtam tikslui, t. y. gauti duomenis, kurie yra reikšmingi ir būtini įrodymai konkrečioje byloje*“ (Reglamento 38 punktas). Būtų naivu tikėtis, kad išduodančiosios valstybės institucijos visada nuodugniai patikrins ar tikrai orderio išdavimas nepažeidžia jokių asmens duomenų ar žmogaus teisių, ypač, kai tai skubus atvejis ir duomenis reikia gauti kuo greičiau, kad būtų galima užkardyti nusikaltimą. Žinoma, Reglamente yra nurodyta, kad įrodymų tiek pateikimo, tiek saugojimo orderius dėl visų duomenų gali išduoti, o jei išduoda kita institucija, tada turi patvirtinti kompetentingas teisėjas, teismas arba ikiteisminio tyrimo teisėjas (Reglamento 3 str.). Prokurorai gali išduoti Europos įrodymų pateikimo orderius, dėl duomenų apie abonentą ar dėl duomenų, kurių prašoma tik siekiant nustatyti naudotojo tapatybę, kas yra ganėtinai problematinis aspektas, kadangi tai taip pat yra asmens duomenys Bendrojo duomenų apsaugos reglamento (toliau – BDAR) ir Direktyvos (ES) 2016/680[21] kontekste, o retrospektyvinė teisinė apsauga yra ganėtinai sudėtinga tokiais

[21] Renkant asmens duomenis baudžiamosiose bylose yra taikoma 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 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, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. Ši direktyva, kaip ir BDAR, priimta siekiant užtikrinti fizinių asmenų

atvejais, kai duomenys gaunami iš kitų valstybių narių (Europos ekonomikos ir socialinių reikalų komiteto nuomonė, 2018, 3.10 punktas). Prokurorai gali išduoti ir Europos įrodymų saugojimo orderius. Tokių orderių atveju prokuroras taip pat yra kompetentinga institucija, galinti patvirtinti kitų tyrimo institucijų orderius (be teisėjo, teismo ar ikiteisminio tyrimo teisėjo) (Reglamento 3 str.). Tai vėlgi, gali kelti šiokių tokių abejonių, ar tikrai prokuroras nuodugniai išanalizuos ir užtikrins pagrindinių teisių laikymąsi, kai jis vadovauja ikiteisminiam tyrimui ir konkrečios bylos baigtis gali priklausyti būtent nuo reikiamų skaitmeninių duomenų. Be kita ko, net ir pačių valstybių teismų sprendimuose ar ikiteisminiuose tyrimuose kyla konfliktų dėl šių aspektų. Žinoma, visa tai atsiremia į valstybių abipusio pasitikėjimo principą ir užtikrinimas privalo būti, tačiau nėra aišku kaip tai bus įgyvendinama ateityje. Atkreiptinas dėmesys, kad išduodančioji institucija privalo išduodant įrodymų pateikimo orderį pagrįsti priežastis, dėl kurių toks orderio išdavimas atitinka būtinumo ir proporcingumo sąlygas (Reglamento 5 str. 5 d. i punktas). Taip pat, išduodančioji institucija turi patikrinti teisines situacijas, kuriomis Europos įrodymų pateikimo orderio išdavimas yra ribojamas arba kurioms taikoma išimtis. Tai taikoma:

1) Europos įrodymų pateikimo orderiams dėl visų kategorijų duomenų, jei lygiagrečiai vyksta baudžiamasis procesas kitoje valstybėje narėje (*non bis in idem* situacijos), ir

2) Europos duomenų pateikimo orderiams dėl srauto ir turinio duomenų, jei:

- duomenys saugomi pagal išduodančiosios valstybės teisę taikoma profesinės paslapties apsauga (Reglamento 5 str. 9 d.);
- duomenis apsaugo imunitetai ar privilegijos pagal vykdančiosios valstybės teisę, įskaitant duomenis, kuriems taikomos baudžiamosios atsakomybės nustatymo ir apribojimo taisyklės, susijusios su spaudos laisve ir saviraiškos laisve kitose žiniasklaidos priemonėse pagal vykdančiosios valstybės teisę (Reglamento 5 str. 10 d.).

Europos įrodymo pateikimo orderio dėl srauto ir turinio duomenų atveju išduodančioji institucija turi pranešti vykdančiajai institucijai (t. y. valstybės, kurioje yra įsisteigęs paslaugų teikėjas arba gyvena jo teisinis atstovas, kompetentingai institucijai), jei duomenų subjektas arba nusikaltimas yra už išduodančiosios valstybės jurisdikcijos ribų (Reglamento 8 str.). Bet kuriuo atveju, kaip rašoma Reglamente, EĮPO arba EĮSO neturi būti išduodamas, kai išduodančioji institucija turi pagrindo manyti, kad tai prieštarautų *non*

pagrindines teises ir laisves, visų pirma jų teisę į asmens duomenų apsaugą tuo pačiu ir leidžiant teisėsaugos institucijoms keistis tokiais duomenimis.

bis in idem principui ar pažeistų kitas žmogaus teises. O vykdančioji institucija savo ruožtu turi įvertinti šiuos aspektus kaip *non bis in idem*, abipusį baudžiamumą, ES sutarties 6 str. ir Chartijoje nustatytas pagrindines teises, bei pagal savo teise imunitetų ar privilegijų apsaugą ar jei prašomiems duomenims taikomos taisyklės dėl baudžiamosios atsakomybės, susijusios su spaudos laisve ir saviraiškos laisve kitose medijose ir jei tai atitinka bent vieną iš šių punktų, gali atsisakyti vykdyti orderį ir turi pranešti apie tai skaitmeninių paslaugų teikėjui, kad duomenų neperduotų, ir išduodančiajai institucijai, kad sustabdytų įrodymų orderį. Iš kitos pusės, vykdymą užtikrinančiai valstybei ir jos institucijai yra priskiriamas tik labai ribotas peržiūros vaidmuo ir valstybė gali turėti įtakos tik tuo atveju, jei skaitmeninių paslaugų teikėjas suabejoja orderio teisėtumu ir atsisako vykdyti nurodymą. *A contrario*, kai skaitmeninių paslaugų teikėjas vykdo nurodymą pagal išduodančiosios valstybės orderį, vykdančioji valstybė gali net nežinoti apie orderio egzistavimą ir negali tam prieštarauti. Dėl šios priežasties vykdančiosios valstybės įgaliota institucija ne visada galės atlikti apsaugos funkcijas, atsisakydama vykdyti orderį, kaip tai yra įprasta kituose savitarpio pagalbos sutartyse. Taigi, visa atsakomybė dėl apsaugos užtikrinimo tenka kompetentingai išduodančiosios valstybės institucijai ir iš dalies privačiam subjektui, atsakingam už orderių vykdymą.

Kalbant apie orderio įvykdymą ir duomenų perdavimą, Reglamente nėra užsiminta apie duomenų, kai jau juos perima išduodančioji institucija, saugojimą. Duomenų saugojimas yra ne mažiau svarbus ir glaudžiai susijęs su e. įrodymų dalyku. Negalima paneigti tinkamo duomenų saugojimo reglamentavimo. Bet kuris baudžiamasis procesas, kaip žinia, trunka ilgai, siekiant užtikrinti teisingą bylos nagrinėjimą ir tinkamai garantuoti įtariamųjų ir kaltinamųjų teises. Apskritai, dažniausiai nusikaltimai išaiškinami tik praėjus nemažai laiko nuo nusikaltimų padarymo. Jei tokiais atvejais duomenys nesaugomi arba saugomi per trumpą laiką, kyla pavojus, kad visos jų gavimą reglamentuojančios taisyklės bus taikomos ribotai ir gali kilti pavojus, kad jos netgi liks tik simboliniu veiksmu ir tada visai nebetenka prasmės toks e. įrodymų taisyklių taikymas (Forlani, 2023, p. 180). Pats Reglamentas daro nuorodą į ES 2016/680 direktyvą, kurios 5 str. numatyta, kad valstybės narės turi nusistatyti asmens duomenų ištrynimo ir saugojimo terminus. Vadinasi, duomenų saugojimą turėtų reglamentuoti kiekvienos valstybės nacionalinė teisė. Tačiau bent minimalūs principai ir taisyklės dėl saugojimo laikotarpio turėjo būti nustatytos ar aprašytos ir naujajame reglamentavime, pavyzdžiui, kad duomenys bus pašalinti po baudžiamosios bylos užbaigimo ar kad duomenys negali būti panaudoti kitiems tikslams, nei buvo išduotas e. įrodymų orderis. Kadangi šiuo atveju, valstybės narės gali nusistatyti labai skirtingus terminus, kas gali iššaukti žmogaus teisių pažeidimus. ESTT ne kartą yra

nagrinėjęs bylas apie elektroninių ryšių duomenis ir yra pasakęs, kad viena vertus saugant tokius duomenis atsiranda galimybė „vyriausybei kontroliuoti savo gyventojus“, tačiau kita vertus, „privaloma vyriausybę įpareigoti kontroliuoti save pačią, kiek tai susiję su saugomų duomenų laikymu ar prieiga prie jos“ (Europos Sąjungos Teisingumo Teismo 2016 m. gruodžio 21 d. sprendimas). Ir negalima tuos pačius duomenis naudoti skirtingų rūšių procesams.

3.4.2. Teisinės garantijos įtariamajam ir kitiems skaitmeninių paslaugų naudotojams

Rengiant naująsias e. įrodymų taisykles, buvo nustatyta, kad nors skaitmeninių paslaugų teikėjai yra linkę bendradarbiauti su teisėsaugos institucijomis, tačiau jiems kelia susirūpinimą, kaip šis naujasis reglamentavimas paveiks jų santykį su klientais, kadangi tai yra pagrindinis veiklos aspektas (Report of open public consultation on E-evidence, 2017, p. 5). Be to, kad privatusis sektorius privalo laikytis Bendrojo duomenų apsaugos reglamento ir jame nustatytų įpareigojimų, skaitmeninių paslaugų teikėjai nurodė, kad jie jaučia atsakomybę už savo klientų duomenų apsaugą ir privatumo išsaugojimą. Jie tai laiko esminiu savo verslo modelio aspektu ir klientų pasitikėjimo jais šaltiniu (3rd. Working Document (A), 2019, p. 4). Vokietijos skaitmeninė asociacija „Bitkom“, nagrinėdama pasiūlymą dėl e. įrodymų taisyklių ir išreikšdama savo poziciją šiuo klausimu kaip skaitmeninių paslaugų teikėjų atstovė, pabrėžė skaidrumo klientams svarbą. Buvo išreikštas pageidavimas, kad naujose e. įrodymų taisyklėse būtų numatyta galimybė pranešti savo naudotojams, kai jų duomenų prašo teisėsaugos institucijos ir kai toks pranešimas nekelia pavojaus tyrimui (Weiß, 2018, p. 4). Iš tiesų, į pastabas buvo atsižvelgta ir naujasis Reglamentas numato informavimo prievolę, tačiau ši prievolė saisto ne duomenų tvarkytoją, t. y. skaitmeninių paslaugų teikėją, o orderį išduodančiąją instituciją. Išduodančioji institucija „*nepagrįstai nedelsdama informuoja asmenį, kurio duomenų prašoma, apie duomenų pateikimą remiantis Europos įrodymų pateikimo orderiu*“, išskyrus atvejus, kai išduodančioji institucija turi priežasčių, dėl kurių informacijos pateikimas atidedamas arba ribojamas. Tokiu atveju, bylos medžiagoje išduodančioji institucija turi nurodyti atidėjimo, apribojimo ar neinformavimo priežastis ir pateikti skaitmeninių paslaugų teikėjui trumpą pagrindimą (Reglamento 13 str.). Tai, kad išduodančioji institucija turi informuoti duomenų valdytoją, yra ganėtinai įprasta praktika baudžiamosiose bylose, po to, kai yra pritaikytos procesinės prievartos priemonės, tokios kaip elektroninių ryšių tinklais perduodamos informacijos kontrolė, jos fiksavimas ir kaupimas, tačiau tai nepaneigia skaitmeninių paslaugų teikėjų baimės dėl galimo klientų nepasitikėjimo atsiradimo.

Atsižvelgiant į tai, asmuo, dėl kurio duomenų yra išduodamas įrodymų pateikimo orderis, turi teisę į veiksmingas teisių gynimo priemones išduodančiosios valstybės teisme, pagal jos nacionalinę teisę ir ji turėtų apimti galimybę ginčyti priemonės teisėtumą, įskaitant jos būtinumą ir proporcingumą, nedarant poveikio pagrindinių teisių garantijoms vykdymą užtikrinančioje valstybėje ar kitoms papildomoms teisių gynimo priemonėms pagal nacionalinę teisę. Jeigu tas asmuo yra įtariamasis ar kaltinamasis, toks asmuo turėtų turėti teisę į veiksmingas teisių gynimo priemones per baudžiamąjį procesą, kuriame tie duomenys naudojami kaip įrodymai (Reglamento 18 str.). Tačiau šiuo atveju, kyla abejonių, ar vienintelė pareiga sukurti veiksmingą teisių gynimo priemonę išduodančioje valstybėje narėje, o ne nukentėjusio ar įtariamojo/kaltinamojo asmens valstybėje narėje, iš tikrųjų yra veiksminga priemonė Chartijos prasme, kadangi nebus sutelktas dėmesys į asmenį, kuris yra susijęs su įrodymų orderio išdavimu (nukentėjusysis ar įtariamasis/kaltinamasis) ir tokio asmens valstybė negalės vykdyti savo apsaugos funkcijų ir užtikrinti pagrindines asmenų, esančių jos teritorijoje, teises, kaip reikalaujama pagal Europos žmogaus teisių sistemą (Franssen, 2018). Pažymėtina, jog asmens pilietybė šiuo atveju neturi reikšmės. Iš tikrųjų vykdančiosios valstybės nustatymą lems paslaugų teikėjo, kuris turės nurodyti valstybę narę kaip savo įsisteigimo valstybę arba valstybę, kurioje yra jo teisinis atstovas, pasirinkimas. Skaitmeniniame pasaulyje valstybė, kurioje vykdomas įrodymų orderis, retai būna ta pati valstybė, kurioje gyvena asmuo, su kuriuo susijęs orderio išdavimas. Tai reiškia, kad vykdančiosios valstybės narės teritorija ir teritorija, kurioje gyvena asmuo, gali nesutapti. Ir šiuo atveju, nėra sąžininga „užkrauti“ didesnę atsakomybės dalį išduodančiajai valstybei asmens atžvilgiu, kadangi pastarajam bus sudėtinga ginti savo teises pagal kitos šalies nacionalinę teisę. Be to, nėra aišku, kaip išduodančioji valstybė sugebėtų atsižvelgti ir nagrinėti pažeidimus, kai tai būtų dėl vykdančiosios valstybės teisės, pavyzdžiui, jei yra išduodamas įrodymų pateikimo orderis, nesusijęs su srauto ir turinio duomenimis (tokiais atvejais jis neturi pranešti vykdančiajai institucijai) ir skaitmeninių paslaugų teikėjas perduoda duomenis orderį išdavusiai institucijai, tačiau toks išdavimas pažeidžia kokią nors vykdančiosios nacionalinės teisės nuostatą. Reglamento 10 str. 5 d. nustato, kad išduodančioji institucija privalo atsižvelgti į kitos valstybės teisę, imunitetus ir privilegijas, bet kaip tas bus įgyvendinama praktiškai, kyla abejonių. Reikia nepamiršti, kad visoje ES yra įvairių valstybių ir jų teisinių sistemų. Atsižvelgiant į skirtingus valstybių proceso standartus, gali kilti problema įvertinant imunitetų ir privilegijų nuostatas, kurios gali būti išduodančiajai valstybei tiesiog nesuprantamos.

Gali įvykti atvejų, kai kitoje šalyje esantys duomenys galėtų padėti įtariamajam ginti savo teises ar įrodyti jo nekaltumą. Dėl šios priežasties Reglamente yra numatyta teisė, kad

įtariamasis arba kaltinamasis (arba jo advokatas) gali prašyti savo valstybės įgaliotų institucijų išduoti Europos įrodymų pateikimo arba saugojimo orderį „*naudodamiesi taikytinomis teisėmis į gynybą pagal nacionalinę baudžiamojo proceso teisę.*“ (Reglamento 1 str. 2 d.). Ši nuostata neįpareigoja šalių savo nacionaliniuose įstatymuose nusimatyti šios teisės, tačiau tada vis tiek turi būti užtikrinamos įtariamojo teisės ikiteisminio tyrimo metu.

Apibendrinant galima teigti, kad nors ir Reglamente yra numatyta, kad asmuo turi turėti teisę į veiksmingas teisių gynimo priemones išduodančiosios valstybės teisme, tačiau nėra aišku, nei kaip tos teisės turi būti įgyvendinamos nei ar tikrai išduodančioji valstybė sugebės jas užtikrinti, ypač, kai tai apims kitos šalies nacionalinės teisės apsaugos priemones.

3.4.3. Trečiųjų šalių skaitmeninių duomenų teikėjai ir reglamentavimo kolizija

Dar viena svarbi naujovė, be to, kad nebereikės teikti įprastinių savitarpio pagalbos prašymų dėl e. įrodymų gavimo, bus tiesioginis bendradarbiavimas ne tik su ES įsisteigusiomis įmonėmis, bet ir galimybė gauti duomenis iš trečiųjų valstybių skaitmeninių duomenų tvarkytojų. Pagal naująjį Reglamentą nesvarbu, kur iš tikrųjų saugomi duomenys, kurie turi būti perduoti pagal Europos įrodymų pateikimo orderį. Galima išduoti orderį a)valstybėje narėje, kurioje yra paskirtasis atstovas, b)kitoje ES valstybėje narėje, taip pat c)trečiojoje šalyje, nepriklausančioje Europos Sąjungai. Tai, kad pareiga atskleisti duomenis taikoma nepriklausomai nuo duomenų saugojimo vietos, išplaukia iš įvairių Reglamento nuostatų (pavyzdžiui, Reglamento 1 str. 1 d. ar 17 str. 2 d. b punkto). Galimybė išduoti orderį trečiosios šalies skaitmeninių paslaugų teikėjui yra tada, kai atitinkama įmonė savo paslaugas teikia ES. Naujosios taisyklės netaikomos tik grynai nacionaliniams paslaugų teikėjams, kurie turi klientų tik vienoje valstybėje narėje, ir ne ES paslaugų teikėjams, kurie paslaugų ES nesiūlo. Ar paslaugų teikėjas „siūlo paslaugas ES“ ar ne, priklauso nuo esminio ryšio su ES egzistavimo – vien tik prieigos prie paslaugų teikėjo svetainės ar el. pašto adreso gavimas toje svetainėje nėra pakankamas (Reglamento 29 punktas). Esminio ryšio kriterijus užsienio paslaugų teikėjams yra grindžiamas konkrečiais faktiniais kriterijais, tokias kaip *didelis vartotojų skaičius vienoje ar keliose valstybėse narėse* arba *kurių veikla nukreipta į vieną ar daugiau narių*. Taip pat, tai priklauso nuo tokių veiksnių, kaip *toje valstybėje narėje paprastai vartojama kalba ar naudojama valiuta* arba *galimybė užsisakyti prekių ar paslaugų, programėlės prieinamumas atitinkamoje nacionalinėje programėlių parduotuvėje*, *vietinė reklama arba reklama valstybėje narėje vartojama kalba*, *santykių su klientais atveju vartojama kalba yra valstybės narės kalba* - tokiu atveju, pakanka nustatyti tik vienos valstybės narės ryšį su trečiosios šalies paslaugų

teikėju (Reglamento 30 punktas). Taigi, šios taisyklės bus taikomos ne tik ES skaitmeninių paslaugų teikėjams, tačiau tai bus aktualu ir kitiems dideliems trečiųjų paslaugų teikėjams, o ypač JAV didelėms kompanijoms. Kaip jau minėta ankščiau, JAV paslaugų teikėjams paprastai draudžiama atskleisti JAV serveriuose saugomus turinio duomenis užsienio teisėsaugos institucijoms (18 U.S.C. § 2702) ir įrodymų orderio išdavimas šiuo atveju kertasi su JAV teise. Siekiant užtikrinti pagarbą suvereniems trečiųjų valstybių interesams, apsaugoti atitinkamą asmenį ir spręsti paslaugų teikėjų pareigų prieštaravimo problemą, Reglamentas numato konkretaus teisminės peržiūros mechanizmą, kuris taikomas tais atvejais, kai dėl Europos įrodymų pateikimo orderio vykdymo paslaugų teikėjai negalėtų vykdyti trečiosios valstybės teisėje nustatytų teisinių pareigų (Reglamento 74 punktas). Esant šioms situacijoms, užsienio paslaugų teikėjai galėtų pasinaudoti Reglamento 17 str. numatyta galimybe ir pateikti „motyvuotą prieštaravimą“ išduoti prašomus duomenis ir taip informuoti tiek išduodančiąją instituciją tiek vykdymą užtikrinančią instituciją dėl teisių kolizijos. Jeigu išduodančioji institucija pageidauja palikti orderį galioti, išduodančiosios valstybės kompetentingas teismas priima sprendimą ar palikti galioti orderį ar ne, įvertindamas kriterijus pateiktus Reglamento 17 str. 4 d. Tuo atveju, kai teismas nustato, kad taikytina trečiosios šalies teisė, pagal kurią draudžiama atskleisti atitinkamus duomenis, teismas automatiškai nepanaikina Europos įrodymų pateikimo orderio, bet turi įvertinti susijusius interesus, pateiktus 17 str. 6 d. ir priimti subalansuotą sprendimą. Iš vienos pusės, sveikintina, kad yra atsižvelgiama į trečiosios šalies nacionalinę teisę ir skaitmeninių duomenų teikėjų įsipareigojimus, tačiau iš kitos pusės, trečiųjų valstybių suverenitetas vis dėlto yra sumenkinamas ir ES teisė jų atžvilgiu yra išaukštinama, kai valstybių narių teismai gali nepaisyti teisinių prieštaravimų ir vis tiek įpareigoti duomenų tvarkytojus perduoti duomenis arba atitinkamai skirti sankcijas. Iš esmės, galėtų būti sunku valstybių narių teismams suprasti trečiosios šalies teisę ir pasverti duomenų pateikimą ir tam prieštaraujančias nuostatas trečiosios valstybės teisiniame reglamentavime, dėl to Reglamentas numato galimybę, išduodančiosios valstybės teismui konsultuotis su trečiąja valstybe dėl jos teisinio reglamentavimo, jeigu tai neprieštarauja atitinkamam baudžiamajam procesui (Reglamento 17 str. 7 d.). Svarstant galimybes dėl Europos įrodymų pateikimo orderio išdavimo reikėtų atsižvelgti į kitos valstybės arba valstybės, kuri neleidžia atskleisti informacijos, duomenų apsaugos interesus ir į baudžiamosios bylos ryšio su ES laipsnį. Tačiau kaip tai bus atsižvelgta praktikoje, sunku nustatyti.

Turėdami mintyje šią problemą, dar 2019 m. Europos Komisijai buvo pavesta derėtis dėl Europos Sąjungos ir JAV susitarimo dėl skaitmeninių įrodymų. ES požiūriu, siekiama užtikrinti, kad JAV duomenų apsaugos teisė nebedraustų JAV paslaugų teikėjams vykdyti

Europos įrodymų pateikimo orderius ir atskleisti informaciją, susijusią su JAV saugomais duomenimis. Kita vertus, JAV vyriausybės atstovai taip pat nori, kad JAV paslaugų teikėjams nebūtų taikoma ES duomenų apsaugos teisė, ypač Bendrojo duomenų apsaugos reglamento V skyriaus straipsniai, kurie susiję su asmens duomenų perdavimu į trečiąsias šalis, kas prieštarauja JAV Cloud Act įstatymui atskleisti Europos Sąjungos serveriuose saugomus duomenis (Daskal, 2018, p. 221). Atitinkamai, ir ES tvarkomų duomenų atskleidimas be Europos Sąjungos ir atitinkamos trečiosios šalies, į kurią duomenys turi būti perduoti, susitarimo (kitaip tariant nesant atitinkamos savitarpio pagalbos sutarties), paprastai, yra draudžiamas. Todėl, viena vertus, reikėtų reglamentuoti e. įrodymų Reglamento taikymą JAV paslaugų teikėjams ir, kita vertus, JAV tyrėjų prieigą prie Europos Sąjungoje saugomų duomenų (Meißner, 2023), ESTT ne kartą laikėsi prielaidos, kad ES tvarkomus asmens duomenis perdavus JAV, neteisėtai sumažėtų duomenų apsaugos lygis (remiantis bylomis „Schrems I“ (C-362/14) ir „Schrems II“ (C-311/18)). Dėl to kyla labai didelė dilema ar reikėtų su JAV susitarti dėl visos apimties duomenų perdavimo, nes kaina už tai, kad ES baudžiamasis persekiojimas siekiant gauti skaitmeninių įrodymų taptų veiksmingesnis ir greitesnis, yra per didelė, jei, dėl to JAV tyrėjams suteikiama beveik nereglamentuota prieiga prie ES saugomų duomenų.

3.4.4. Sankcijos ir išlaidų atlyginimas

Pradiniuose rengimo etapuose buvo aršiai diskutuojama ir apie sankcijas paslaugų teikėjams, kai šie atitinkamai nevykdo įsipareigojimų ir nepateikia priimtinų priežasčių. Reglamento projekte nebuvo nustatytų specialių minimalių taisyklių dėl sankcijų, taikytinų, jei paslaugų teikėjas atsisako vykdyti išduodančiosios valstybės narės nurodymą. Siūlomame Reglamente buvo daroma nuoroda į nacionalinę teisę ir tik reikalaujama, kad valstybės narės nustatytų „veiksmingas, proporcingas ir atgrasančias pinigines sankcijas“ (Pasiūlymas Europos Parlamento ir Tarybos..., 2018, 13 str.). Priimtame Reglamente išliko nuostata, kad vykdančiosios valstybės pačios nusistato baudų dydžius, kurios turi būti atgrasančios, proporcingos ir veiksmingos, tačiau atsižvelgus, į sulauktą kritiką pasiūlymo metu, jog buvo palikta labai didelė veiksmų laisvė valstybėms, buvo nubrėžta riba, kad piniginės baudos negali viršyti 2 % paslaugų teikėjo bendros pasaulinės metinės apyvartos (Reglamento 15 str.). Be to, Reglamentas nedraudžia valstybėms narėms taikyti baudžiamąsias sankcijas, kas rodo, kad nors ir nustatyta maksimali sankcijų riba, tačiau tai vis tiek palieka ganėtinai didelę diskrecija valstybėms. Mokslininkė Vanessa Franssen mano, kad tai sudarys sąlygas skaitmeninių paslaugų teikėjams ieškoti palankesnės teisinės padėties (angl. „*forum shopping*“). Paslaugų teikėjai gali būti linkę paskirti savo teisinį

atstovą toje valstybėje narėje, kurioje sankcijos už reikalavimų nesilaikymą yra palyginti nedidelės ir nebaudžiamojo pobūdžio, nes užsakymo nevykdymo atveju bus taikoma vykdančiosios valstybės narės teisė (Franssen, 2018, p. 6). Vertinant tai, kad skaitmeninių paslaugų teikėjams labai svarbu išlaikyti santykį su klientais, kyla klausimas ar nebus piktnaudžiaujama šia reglamentavimo spraga. Ir skaitmeninių paslaugų teikėjai nevykdys įrodymų orderių tam, kad neprarastų klientų, nes tam tikrais atvejais pigiau yra susimokėti baudą, negu prarasti klientus ir pastovias pajamas.

Dar vienas aspektas, kuris sulaukė labai didelės kritikos – tai kompensavimo sistemos nebuvimas. Reglamento 14 str. teigiama, kad paslaugų teikėjai gali prašyti, kad „*išduodančioji valstybė narė atlygintų jų išlaidas, jei tokia galimybė, susijusi su panašiose situacijose išduodamais šalies nacionaliniais orderiais, numatyta nacionalinėje išduodančiosios valstybės teisėje, ir tai padarytų pagal tos valstybės nacionalinę teisę*“. Taigi šis klausimas paliekamas spręsti nacionaliniu lygmeniu, o tai skaitmeninių paslaugų teikėjams kelia ne tik daug neaiškumo, bet ir susirūpinimo. Šis Reglamentas įpareigos ne tik didžiules kompanijas, tačiau ir mažas ir net labai mažas įmones bendradarbiauti su teisėsauga. Maža įmonė laikomos tos įmonės, kurios turi iki 50 darbuotojų, jos apyvarta arba bendras balansas yra iki 10 mln. eurų, labai maža įmonė turi iki 10 darbuotojų ir jos apyvarta arba bendras balansas neviršija 2 mln. eurų (2003 m. gegužės 6 d. Europos Komisijos rekomendacija 2003/361/EB). Kaip jau minėta, mažoms ir labai mažoms įmonėms, jei jos paslaugas teikia ne vienoje ES valstybėje narėje, EĮPO ir EĮSO vykdymas kels nemažų iššūkių, jei joms nebus atlyginama už išlaidas, padarytas vykdant orderius. Vis dėlto, duomenų gavimas yra išduodančiosios valstybės interesas, o ne įmonės, todėl ir kaštus už orderio įvykdymą turėtų prisiimti išduodančioji valstybė. Tai neturėtų būti palikta pačios valstybės diskrecijai.

Apskritai, šios naujos taisyklės dėl e. įrodymų yra nauja revoliucija teisiniame bendradarbiavime. Jos padarys didelį poveikį ES skaitmenines paslaugas teikiantiems paslaugų teikėjams, iš naujo apibrėš jų pareigas teisėsaugos institucijoms ir darys įtaką jų santykiams su klientais. Nors viešųjų funkcijų perkėlimo ant skaitmeninių paslaugų teikėjų galiausiai pavyko iš dalies išvengti, tačiau ribota pareiga vis dėlto išliko ir šie turės peržiūrėti, kad nebūtų akivaizdžiai pažeidžiamos pagrindinės teisės. Praktika parodys ar naujosios e. įrodymų taisyklės yra pažanga, ir tikrai leis greičiau išaiškinti kibernetinius nusikaltimus ar jos lems, dažnai autorių pabrėžiamą, „paradigmos pokytį“ bendradarbiavimo srityje. Labiausiai baiminamasi valstybių piktnaudžiavimo ir didelės žalos pagrindinėms teisėms.

IŠVADOS

1. Lietuvos Respublikoje tarptautinis bendradarbiavimas baudžiamojoje justicijoje suvokiamas kaip nusikalstamų veikų prevencijos, tyrimo bei teismų priimtų sprendimų vykdymas, kai tarptautinių sutarčių bei Europos Sąjungos teisės nustatytais pagrindais kartu veikia ne mažiau kaip dvi valstybės arba valstybė ir tarptautinė organizacija ar Europos Sąjungos institucija. Jis pasitelkiamas, kai nusikalstama veika turi „užsienio elementą“ ir reikia atlikti tam tikrus procesinius veiksmus, gauti duomenų ar dalintis informacija su užsienio ar tarptautinėmis institucijomis. Baudžiamosios justicijos tarptautinio bendradarbiavimo Europos Sąjungoje istorinė raida parodė, kad ilgai kitusi tarptautinio bendradarbiavimo sistema iki šiol nėra nuosekli, o tokio instituto efektyvumą mažina valstybių diskrecija, leidžianti atsisakyti vykdyti kitų valstybių prašymus.

2. Atliktas tyrimas leidžia daryti išvadą, kad kibernetinių nusikaltimų, kurie suprantami kaip nusikalstamos veikos, nukreiptos prieš kompiuterį, kompiuterių tinklą, tinklinį įrenginį, kibernetinę erdvę arba nusikalstamos veikos padarytos naudojant kompiuterį, kompiuterių tinklą, tinklinį įrenginį ar pačioje kibernetinėje erdvėje, problematika – nusikaltimų mastas, lengvas prieinamumas, anonimiškumas, globalus pasiekiamumas, ir latentiškumas. Šie veiksniai lemia sudėtingą aptikimo ir už tai atsakingo asmens patraukimo baudžiamojon atsakomybėn procesą, todėl tarptautinio bendradarbiavimo pasitelkimas tokio pobūdžio nusikaltimų užkardymui yra būtinas.

3. Budapešto Konvencija žengė reikšmingą žingsnį suderinant valstybių nacionalinius įstatymus dėl elektroninių nusikaltimų ir tapo pamatiniu tarptautiniu dokumentu, nustatančiu standartus bei bendradarbiavimo principus šioje srityje. Deja, taip pat, paliko ir daug neišspręstų klausimų, tokių kaip didelis valstybių diskrecijos lygis, nevienodi nacionaliniai įstatymai, lemiantys skirtingą žmogaus teisių apsaugą, nepakankamas duomenų apsaugos užtikrinimas, ir neaiškus įrodymų rinkimo bei perdavimo standartas trukdo nuosekliam ir efektyviam kibernetinių nusikaltimų tyrimui ir užkardymui.

4. Išanalizavus esamus tarptautinio bendradarbiavimo tiriant kibernetinius nusikaltimus mechanizmus (savitarpio teisinė pagalba, Europos tyrimo orderis, teisėsaugos institucijų tiesioginis bendradarbiavimas su privačiais skaitmeninių paslaugų teikėjais) dėl elektroninių duomenų, esančių kitoje valstybėje, gavimo, išryškėjo, kad nors tai yra svarbios priemonės kovojant su nusikalstamumu kibernetinėje erdvėje, jos turi trūkumų, trukdančių efektyviam bei greitam tyrimui. Nustatytos pagrindinės problemos: 1) pasitelkiant tiek savitarpio pagalbą, tiek Europos tyrimo orderį, duomenų gavimas apima ilgą ir sudėtingą procesą, kuris gali lemti duomenų praradimą dėl elektroninių duomenų nepastovumo specifikos, 2) nevienodos valstybių teisinės sistemos ir procedūros, 3)

elektroninius duomenis saugo ir apdoroja privatūs juridiniai asmenys, o tokių duomenų perdavimas teisėsaugos institucijoms dažnai yra neįpareigojantis, tačiau net ir esant tokių duomenų perdavimui kyla įrodymų teisėtumo problema.

5. Atsižvelgiant į naująsias Europos Sąjungos elektroninių įrodymų gavimo taisykles, kurios leis tiesioginį bendradarbiavimą su skaitmeninių paslaugų teikėjais, galima teigti, jog nauja sistema gali patobulinti tarptautinį bendradarbiavimą, tačiau turės didelį poveikį Europos Sąjungoje skaitmenines paslaugas teikiantiems paslaugų teikėjams. Jiems bus apibrėžtos naujos pareigos teisėsaugos institucijoms, o tai gali paveikti jų santykius su klientais. Nors viešųjų funkcijų perkėlimo ant skaitmeninių paslaugų teikėjų galiausiai pavyko iš dalies išvengti, tačiau ribota pareiga, vis dėlto, išliko ir šie turės peržiūrėti, kad nebūtų „akivaizdžiai“ pažeidžiamos pagrindinės teisės. Be to, susirūpinimą kelia ir kitos tam tikros naujojo teisės aktų paketo nuostatos, kurios gali paskatinti valstybes piktnaudžiauti galia, siekiant gauti elektroninius duomenis iš skaitmeninių paslaugų teikėjų. Tai gali sukelti didelę žalą pagrindinėms teisėms bei jų neužtikrinimui, kadangi visa atsakomybė dėl apsaugos užtikrinimo tenka tik kompetentingai duomenų prašančiai valstybės institucijai, kuri privalės įvertinti ir kitų valstybių teisės apsaugos priemones. Kritikuotinas ir tam tikrų aspektų nesureglamentavimas, pavyzdžiui, išlaidų atlyginimas skaitmeninių paslaugų teikėjams ar konkretesnių sankcijų nenustatymas, kas gali lemti skaitmeninių paslaugų teikėjų piktnaudžiavimą. Dėl šių priežasčių reikėtų eliminuoti egzistuojančias reglamentavime problemas bei užtikrinti didesnę apsaugą pagrindinėms teisėms.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai:

Tarptautiniai teisės norminiai aktai:

1. Konvencija dėl elektroninių nusikaltimų (2001). *Valstybės žinios*, 2004, 36-1188.
2. Konvencija dėl Europos Sąjungos valstybių narių savitarpio pagalbos baudžiamosiose bylose, kurią pagal Europos Sąjungos sutarties 34 straipsnį patvirtino Taryba (2000). *Valstybės žinios*, 2004, 154-5599.
3. Konvencijos dėl elektroninių nusikaltimų antrasis papildomas protokolas dėl glaudesnio bendradarbiavimo ir elektroninių įrodymų atskleidimo (2023). OL L 63, p. 28

Europos Sąjungos teisės norminiai aktai:

4. 1992 m. liepos 29 d. Europos Sąjungos sutartis. OL L 191, p. 1
5. 2003 m. gegužės 6 d. Europos Komisijos rekomendacija dėl labai mažų, mažų ir vidutinių įmonių apibrėžimo 2003/361/EB OL L 124, p. 36.
6. 2003 m. birželio 6 d. Tarybos sprendimas dėl susitarimų tarp Europos Sąjungos ir Jungtinių Amerikos Valstijų dėl ekstradicijos ir savitarpio teisinės pagalbos baudžiamosiose bylose pasirašymo. OL L 181, p. 25.
7. Lisabonos sutartis, iš dalies keičianti Europos Sąjungos sutartį ir Europos bendrijos steigimo sutartį pasirašyta Lisabonoje, 2007 m. gruodžio 13 d., 2007/C 306/01, p. 1.
8. Europos Parlamento ir Tarybos 2014 m. balandžio 3 d. direktyva 2014/41/ES dėl Europos tyrimo orderio baudžiamosiose bylose. OL L 130, p. 1
9. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, p. 1
10. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. direktyva (ES) 2016/680 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, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. OL L 119, p. 89.

11. Europos Parlamento ir Tarybos 2023 m. liepos 12 d. reglamentas (ES) 2023/1543 dėl Europos įrodymų pateikimo orderių ir Europos įrodymų saugojimo orderių elektroniniams įrodymams baudžiamajame procese ir laisvės atėmimo bausmių vykdymui pasibaigus baudžiamajam procesui. OL L 191, p. 118.
12. Europos Parlamento ir Tarybos 2023 m. liepos 12 d. direktyva (ES) 2023/1544, kuria nustatomos suderintos paskirtųjų įmonių ir teisinių atstovų skyrimo elektroniniams įrodymams baudžiamajame procese rinkti taisyklės. OL L 191, p. 181.

Nacionaliniai teisės norminiai aktai:

13. Lietuvos Respublikos Vyriausybės ir Jungtinių Amerikos Valstijų Vyriausybės sutartis dėl savitarpio teisinės pagalbos baudžiamosiose bylose (1998). *Valstybės žinios,* 59-1660.
14. Lietuvos Respublikos baudžiamasis kodeksas (2000). *Valstybės žinios*, 89-2741.
15. Lietuvos Respublikos Baudžiamojo proceso kodeksas (2002). *Valstybės žinios*, 37-1341
16. Lietuvos Respublikos kibernetinio saugumo įstatymas (2014). TAR, 20553
17. Lietuvos policijos generalinio komisaro 2015-02-02 įsakymu Nr. 5-V-101 patvirtintas Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veiklos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetiniu incidentų tyrimo tvarkos aprašas (2015). TAR, 1654
18. Dėl Lietuvos policijos generalinio komisaro 2015 m. vasario 2 d. įsakymo Nr. 5-V-101 „Dėl Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašo patvirtinimo“ pakeitimo (2018). TAR, 2423.
19. 18 U.S. Code § 3559 (2018)

Specialioji literatūra:

20. Akdeniz, Y. (2002). *Anonymity, Democracy, and Cyberspace*. Social Research, 69(1), 223–237 [interaktyvus]. Prieiga per internetą: http://www.jstor.org/stable/40971545 [žiūrėta 2024 m. vasario 18 d.].
21. Belevičius, L. (2013). Tarptautinis teisinis bendradarbiavimas ir Europos Sąjungos baudžiamasis procesas: aktualijos, perspektyvos, lūkesčiai. Iš: Jurka, R. et al.

(2013). *Baudžiamojo proceso tarptautiškumas: patirtis ir iššūkiai.* Vilnius: Mykolo Romerio universitetas, 170-210.

22. Bergström M. and Cornell A. J. (2011) *Policing the World: The Practice of International and Transnational Policing*. Working Paper, Uppsala: Uppsala University [interaktyvus] Prieiga per internetą: https://www.diva-portal.org/smash/get/diva2:491924/FULLTEXT01.pdf [žiūrėta 2024 m. kovo 2 d.]
23. Bučiūnas, G. (2015). *Terminų vartojimas tiriant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui*. Visuomenės saugumas ir viešoji tvarka (13) ISSN 2029–1701
24. Carr, J. B., Gerber, E. R. and Lupher, E. W. (2008) *Explaining horizontal and vertical cooperation on public services in Michigan: The role of local fiscal capacity, DigitalCommons@WayneState* [interaktyvus]. Prieiga per internetą: https://digitalcommons.wayne.edu/interlocal_coop/34/ [žiūrėta: 07 March 2024 m. kovo 7 d.].
25. Casey, E. (2011). *Digital Evidence and Computer Crime Third Edition*. [interaktyvus] Prieiga per internetą: https://rishikeshpansare.files.wordpress.com/2016/02/digital-evidence-and-computer-crime-third-edition.pdf. [žiūrėta 2024 m. vasario 25 d.]
26. Chawki, M. et al. (2015). *Cybercrime*, *Digital Forensics and Jurisdiction*. Springer, New York: Springer International Publishing, 3-24.
27. Clough, J. (2010) *Principles of Cybercrime,* Victoria: Monash University, 365-387, doi:10.1017/CBO9780511845123.
28. Corhay, M. (2023). *It is a Long Way to...E-Evidence: EU Reforms in the Collection of Electronic Evidence – Part 1*. Information Law and Policy Centre Blog [interaktyvus]. Prieiga per internetą: https://infolawcentre.blogs.sas.ac.uk/2023/01/24/it-is-a-long-way-to-e-evidence-eu-reforms-in-the-collection-of-electronic-evidence-part-1/ [žiūrėta 2024 m. kovo 3 d.].
29. Craig, P. and De Búrca, G. (2011). *EU law: text, cases, and materials*. Oxford: Oxford University Press. [ineraktyvus]. Prieiga per internetą: https://global.oup.com/academic/product/eu-law-9780198856641?prevNumResPerPage=100&facet_narrowbytype_facet=Books+for+Courses&lang=en&cc=nz [žiūrėta: 2024 m. vasario 15 d.].
30. Čepas, A. ir Švedas, G. (2008). *Asmenų, įtariamų padarius nusikalstamą veiką, išdavimas baudžiamajam persekiojimui (ekstradicija, perdavimas Tarptautiniam*

baudžiamajam teismui arba pagal Europos arešto orderį): Tarptautinė teisinė pagalba baudžiamosiose bylose. Vilnius: Teisinės Informacijos Centras.

31. Daskal, J. (2017). *Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights*. Statement to the Committee on the Judiciary Subcommittee on Crime and Terrorism United States Senate.
32. Daskal, J. (2018). *Unpacking the CLOUD Act*. 4 eucrim p. 220-225
33. De Amicis, G., Kostoris, R. E. (2018). Vertical Cooperation. In: Kostoris, R. (eds) (2018). *Handbook of European Criminal Procedure*. Springer Nature: Springer International Publishing AG., 201-245, doi:10.1007/978-3-319-72462-1_5
34. Forlani, G. (2023). *The E-evidence Package*. eucrim 2/2023, 174-181, doi:10.30709/eucrim-2023-013.
35. Franssen, V. (2017). *The Belgian Internet Investigatory Powers Act - A Model to Pursue at European Level?*. European Data Protection Law Review, 534-542. doi:10.21552/edpl/2017/4/18
36. Franssen, V. (2018). *The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?*. European Law Blog, [interaktyvus]. Prieiga per internetą: europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/ [žiūrėta 2024 m. kovo 23 d.].
37. Grabosky, P. N. (2001). *Virtual Criminality: old wine in new bottles?* Social and legal studies, Vol. 10(2), 243–249.
38. Gutauskas, A. (2013). Kai kurių nusikalstamų veikų, susijusių su organizuotu nusikalstamumu, tarptautiniai aspektai: žvilgsnis į ateitį. Iš: Jurka, R. et al. *Baudžiamojo proceso tarptautiškumas: patirtis ir iššūkiai*. Mokslo studija. Vilnius: Mykolo Romerio universitetas, 138-168.
39. Harmati et al. (2008). *International Cooperation in Criminal Matters in the European Union.* THEMIS, Bucharest: National Institute of Magistracy.
40. Hooper, C. et al. (2013). *Cloud computing and its implications for cybercrime investigations in Australia*. Computer Law & Security Review, Volume 29, Issue 2, 152-163, doi: 10.1016/j.clsr.2013.01.006.
41. Hopkins, S. L. (2003). *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*., 2 J High Tech L. 101-121
42. Yar, M. (2013) *Cybercrime and Society*. London: SAGE Publications Inc.

43. Kaupinis Ž. (2016). *Tarptautinis bendradarbiavimas tiriant su terorizmu susijusius nusikaltimus.* Magistro baigiamasis darbas. Vilnius: Mykolo Romerio universitetas.
44. Kinderis, R. Jucevičius, G. (2013). *Komplementarumas kaip verslo modelių bendradarbiavimo raiškos pagrindas*. Mokslas ir edukaciniai procesai, Nr. 2 (17). 28-36.
45. Kostoris, R. (eds) (2018). *Handbook of European Criminal Procedure*. Springer Nature: Springer International Publishing AG, doi: 10.1007/978-3-319-72462-1_5
46. Krašto apsaugos ministerija (2022). *Nacionalinė kibernetinio saugumo strategija*. Vilnius: Lietuvos Respublikos krašto apsaugos ministerija.
47. Kshetri N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perpective*. Springer-Verlag.
48. Kshetri, N. (2009). *Positive externality, increasing returns, and the rise in cybercrimes*. Communications of the ACM, Vol. 52, Issue 12.
49. Lekavičienė, R. et al. (2015). *Bendravimo psichologija šiuolaikiškai*. Vadovėlis aukštosioms mokykloms. Vilnius: Alma littera. ISBN 978-9955-38-708-0
50. Marcinauskaitė, R. (2011). *Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema*. Socialinių mokslų studijos, Nr. 3(3), p. 897–914.
51. Matevičius, P. (2020). *Pinigų plovimo prevencija*. Magistro baigiamasis darbas, socialiniai mokslai, teisė, Vilnius: Vilniaus universitetas.
52. Mattessich, P. W, Monsey, B. R. , (1992). *Collaboration: What Makes It Work*. St. Paul: Amherst H.Wilder Foundation, ISBN 0-940069-02-4
53. Meißner, P. (2023). *Digitale Beweise im EU-/US-Datenschutzkonflikt*. Verfassungsblog [interaktyvus]. Prieiga per internetą : https://verfassungsblog.de/digitale-beweise-im-eu-us-datenschutzkonflikt/ [žiūrėta 2024 m. kovo 11 d.].
54. Nevera, A. (2006). *Valstybės baudžiamosios jurisdikcijos principai*. Monografija. Vilnius: Mykolo Romerio universitetas.
55. Payne, B. K. (2020). Defining cybercrime. In Holt, T. and Bosler, A. M. (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham, Springer, 3-25.
56. Panomariovaitė, G., Zokaitė, J. (2021). *Kibernetinis persekiojimas (cyberstalking): viktimizacijos ypatumai ir teisinio reagavimo galimybės*. Teisės mokslų pavasaris. Vilnius: Vilniaus universiteto leidykla. 235-257.

57. Parker D. B. (1989). *Computer Crime*. Criminal Justice Resource Manual [interaktyvus]. Prieiga per internetą: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf [žiūrėta 2024 m. vasario 13 d.].
58. Sabillon, R. et al. (2016) *Cybercrime and cybercriminals: A comprehensive study*, Repositori Institucional (O2): Página de inicio. [interaktyvus]. Prieiga per internetą: https://openaccess.uoc.edu/handle/10609/78507 [žiūrėta 2024 m. kovo. 12 d.].
59. Sippel, B. (2020). *REPORT on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.* A9-0256/2020. European Parliament [interaktyvus]. Prieiga per internetą: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html [žiūrėta 2024 m. kovo 23 d.].
60. Štitilis D., et al. (2016). *Interneto ir technologijų teisė*. Vilnius: Mykolo Romerio universitetas.
61. Štitilis, D. (2011). Elektroniniai nusikaltimai. Metodinė priemonė, Vilnius: Mykolo Romerio universitetas. ISBN 978-9955-19-329-6
62. Tosza, S (2019). *Cross-Border gathering of electronic evidence: Mutual legal assistance, its shortcomings and remedies.* Brussels: Larcier/Bruylant, 269 – 285.
63. Tosza, S. (2021). *Internet Service Providers as Law Enforcers and Adjudicators. A Public Role of Private Actors*. Computer Law & Security Review, vol. 43, Elsevier Ltd. https://doi.org/10.1016/j.clsr.2021.105614.
64. Tsakalidis, G., Vergidis, K. and Madas, M. (2018). *Cybercrime Offences: Identification, Classification and Adaptive Response*. Thessaloniki: 5th International Conference on Control, Decision and Information Technologies (CoDIT), 470-475, doi: 10.1109/CoDIT.2018.8394816.
65. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Oxford: Polity.
66. Weyembergh, A. (2018). History of the Cooperation. In: Kostoris, R. E. (eds) (2018). *Handbook of European Criminal Procedure*. Springer Nature: Springer International Publishing AG., 173-197, doi: 10.1007/978-3-319-72462-1_5
67. Wei-Jung, C. (2020). *Cyberstalking and Law Enforcement*. Procedia Computer Science.
68. Weiß, R. (2018). *Position Paper - E-Evidence*. Bitkom: Federal Association for Information Technology, Telecommunications and New Media [interaktyvis].

Prieiga per internetą: https://www.bitkom.org/sites/main/files/file/import/20181010-Bitkom-Position-Paper-on-E-Evidence.pdf [žiūrėta 2024 m. kovo 26 d.].

Teismų praktika:

69. Belgijos Kasacinio Teismo 2015 m. gruodžio 1 d. nutartis baudžiamojoje byloje YAHOO! Inc. Nr. P.13.2082.N/1.
70. *Schrems.*[ESTT], Nr. C-362/14, [2015-10-06]. ECLI:EU:C:2015:650.
71. *Tele2 Sverige AB prieš Post- och telestyrelsen ir Secretary of State for the Home Department prieš Tom Watson ir kt.* [ESTT], Nr. C-203/15, [2016-12-21]. ECLI:EU:C:2016:970.
72. *Schrems II.* [ESTT], Nr. C-311/18, [2020-07-16]. ECLI:EU:C:2020:559.

Travaux préparatoires:

73. European Economic and Social Committee (2018). *Opinion on Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters [COM(2018) 225 final – 2018/0108(COD)] and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [COM(2018) 226 final – 2018/0107(COD)]*, Council of the European Union, SOC/596, 11533/18 [interaktyvus]. Prieiga per internetą: https://data.consilium.europa.eu/doc/document/ST-11533-2018-INIT/en/pdf [žiūrėta 2024 m. kovo 15 d.].
74. 2018 m. balandžio 17 d. Pasiūlymas Europos Parlamento ir Tarybos Reglamentas dėl Europos elektroninių įrodymų baudžiamosiose bylose pateikimo ir saugojimo orderių, COM(2018) 225 final - 2018/0108(COD). Document 52018PC0225
75. Committee on Civil Liberties, Justice and Home Affairs (2019). *3rd Working Document (A) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2019)(2018/0108 (COD)) - Execution of EPOC(-PR)s and the role of service providers* [interaktyvus]. Prieiga per internetą: https://www.europarl.europa.eu/doceo/document/LIBE-DT-634849_EN.pdf?redirect [žiūrėta 2024 m. kovo 13 d.].

76. EU Council (2019). *The General approach on the proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters*. No. 10206/19
77. Amended proposal for a REGULATION (EU) 2023/... OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of ... on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, (2023). Council Doc. No. 5449/23. [interaktyvus]. Prieiga per internetą: https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf [žiūrėta 2024 m. kovo 2 d.]

Kiti šaltiniai:

78. EU Commission (2016). *Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace* [interaktyvus]. http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf [žiūrėta 2024 m. kovo 17 d.].
79. EU Commission (2017). *Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward* [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf [žiūrėta 2024 m. kovo 17 d.].
80. EU Commission (2017). *Report of open public consultation on E-Evidence* [interaktyvus]. Prieiga per internetą: https://commission.europa.eu/document/download/93910214-1908-4008-9934-51520edfd724_en?filename=report_of_open_public_consultation_on_e_evidence_april2018.pdf [2024 m. kovo 15 d.].
81. Eurostat (2018) *Archive:internet access and use statistics - households and individuals - Statistics Explained* [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=379591 [žiūrėta 2024 m. vasario 3 d.].
82. Valstybinio audito ataskaita (2020). *Ar veiksmingai kovojama su elektroniniais nusikaltimais*. VAE-7.
83. Statista, 2024. *Number of internet and social media users worldwide as of January 2024* [interaktyvus]. Prieiga per internetą:

https://www.statista.com/statistics/617136/digital-population-worldwide/ [žiūrėta 2024 vasario 3d.].

84. Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (2024). *Duomenys apie užregistruotas nusikalstamas veikas, padarytas elektroninėje erdvėje* [interaktyvus]. Prieiga per internetą: https://www.ird.lt/lt/reports/view_item_datasource?id=10857&datasource=91746 [žiūrėta 2024 m. sausio 16 d.]

SANTRAUKA

Tarptautinis bendradarbiavimas tiriant kibernetinius nusikaltimus

Gabija Panomariovaitė

Magistro darbe nagrinėjamas tarptautinio bendradarbiavimo institutas tiriant kibernetinius nusikaltimus, prieš tai apžvelgiant pačio tarptautinio bendradarbiavimo raidą Europos Sąjungoje, formas, reglamentavimą Lietuvos Respublikoje, kibernetinių nusikaltimų sampratą bei tokio pobūdžio nusikaltimų keliamus iššūkius. Atliktame tyrime analizuojami elektroninių duomenų kaip įrodymų, esančių kitose valstybėse, gavimo metodai, tokie kaip savitarpio teisinė pagalba, Europos tyrimų orderis ir teisėsaugos institucijų bendradarbiavimas su privačiais skaitmeninių paslaugų teikėjais, ir jų keliama problematika, ypatingą dėmesį skiriant naujajam 2023 m. Europos Sąjungos teisės aktų paketui, skirtam elektroninių duomenų kaip įrodymų iš kitos valstybės narės gavimui.

Esami tarptautinio bendradarbiavimo mechanizmai padeda ištirti kibernetinius nusikaltimus, tačiau nėra tokie efektyvūs ir greiti dėl ilgo ir sudėtingo proceso, nevienodų valstybių nacionalinės teisės sistemų ir skirtingo duomenų apsaugos užtikrinimo lygio. Nors naujosios Europos Sąjungos elektroninių įrodymų taisyklės leis greitesnį ir efektyvesnį tarptautinį bendradarbiavimą, ypač tiesioginį su privačiais skaitmeninių paslaugų teikėjais renkant elektroninius įrodymus kibernetinių nusikaltimų bylose, vis dėlto, tam tikros šių taisyklių nuostatos kelia susirūpinimą, kaip praktiškai jos bus įgyvendinamos. Nepaisant to, kad naujasis teisės aktų paketas teoriškai užtikrina, kad būtų suteikiamos atitinkamos apsaugos priemonės asmens duomenims ir pagrindinėms teisėms, bet toks teisių užtikrinimas daugiausiai sutelkiamas į duomenų prašančiosios valstybės rankas. Kas, be kita ko, gali lemti duomenų apsaugos ir pagrindinių teisių pažeidimus. Atsižvelgiant į darbe iškeltus probleminius aspektus, autorės nuomone, yra būtina eliminuoti tokių pažeidimų atsiradimą bei įvesti griežtesnes apsaugos priemones.

SUMMARY

International Cooperation in Cybercrime Investigation

Gabija Panomariovaitė

The Master's thesis examines the institute of international cooperation in the investigation of cybercrime, followed by a review of the development of international cooperation in the European Union, its forms, its regulation in the Republic of Lithuania, the concept of cybercrime, and the challenges posed by this type of crime. The study analyses the methods of obtaining electronic data as evidence in other countries, including mutual legal assistance, the European Investigation Order and cooperation between law enforcement authorities and private digital service providers, and the issues they raise, with a particular focus on the new 2023 European Union legislative package for obtaining electronic data as evidence from another Member State.

Existing international cooperation mechanisms help to investigate cybercrime, but are not as effective and fast due to the lengthy and complex process, the different national legal frameworks and the varying levels of data protection. While the new European Union rules on electronic evidence will allow for faster and more efficient international cooperation, particularly through direct cooperation with private digital service providers in the collection of electronic evidence in cybercrime cases, certain provisions of these rules raise concerns about how they will be implemented in practice. Despite the new legislative package theoretically ensuring adequate safeguards for personal data and fundamental rights, enforcement of such rights is largely concentrated in the hands of the requesting state. This can lead to violations of data protection and fundamental rights, among other issues. In view of the problematic aspects raised in the work, the author considers it necessary to eliminate such violations and introduce stronger safeguards.