ISSN 1392-6195 (print)
ISSN 2029-2058 (online)
JURISPRUDENCIJA
JURISPRUDENCE
2021, 28(1), p. 200–216.

NUSIKALSTAMOS VEIKOS ELEKTRONINĖJE ERDVĖJE IR TERITORINĖ BAUDŽIAMOJI JURISDIKCIJA

Renata Marcinauskaitė
Mykolo Romerio universiteto Teisės mokyklos
Baudžiamosios teisės ir proceso institutas
Elektroninis paštas: rennata@mruni.eu

Pateikta 2021 m. birželio 6 d., parengta spaudai 2021 m. birželio 14 d.

DOI: 10.13165/JUR-21-28-1-10

Santrauka. *Straipsnyje nagrinėjama teritorinio baudžiamosios jurisdikcijos principo taikymo ir su juo susijusios nusikalstamos veikos padarymo vietos elektroninėje erdvėje nustatymo problemos. Atkreipiamas dėmesys į tai, kad Lietuvos Respublikos baudžiamojo kodekso (toliau – ir BK) 4 straipsnio 2 dalyje įtvirtinta nuostata, kad nusikalstamos veikos padarymo vieta yra vieta, kurioje asmuo veikė (arba turėjo ir galėjo veikti), arba vieta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai, yra taikoma nustatant veikos padarymo vietą ne tik fizinėje, bet ir elektroninėje erdvėje. Atsižvelgiant į elektroninės erdvės ir veiksmų joje ypatumus, straipsnyje aptariami kriterijai, kurie galėtų susieti nusikalstamą veiką elektroninėje erdvėje su fizinės erdvės teritorija. Šiai analizei pasitelkti ir Europos Sąjungos bei tarptautiniai teisės aktai, kurių nuostatas Lietuva yra įgyvendinusi BK.*

Straipsnyje išskirti fizinio asmens ir informacinės sistemos buvimo vietos kriterijai, pateikiami aiškinimo variantai, kodėl teisės aktuose pasirinkti būtent tokie elektroninėje erdvėje padarytos nusikalstamos veikos susiejimo su fizine erdve būdai. Nemažai dėmesio skiriama ir esminio ryšio su valstybės teritorija kriterijui. Straipsnyje prieita prie išvados, kad BK nuostatos, įtvirtinančios teritorinės baudžiamosios jurisdikcijos principą, turėtų būti suderintos su pakitusiu nusikalstamos veikos padarymo vietos supratimu, kai veika padaryta elektroninėje erdvėje.

ISSN 1392-6195 (print), ISSN 2029-2058 (online)
http://www.mruni.eu/lt/mokslo_darbai/jurisprudencija/
http://www.mruni.eu/en/mokslo_darbai/jurisprudencija/

Reikšminiai žodžiai: *nusikalstama veika elektroninėje erdvėje, baudžiamoji jurisdikcija, teritorinis principas, informacinė sistema, esminio ryšio kriterijus.*

Įvadas

Valstybės baudžiamoji jurisdikcija yra įgyvendinama principų, kurie apibrėžia tos valstybės baudžiamųjų įstatymų galiojimą erdvėje, pagrindu. Baudžiamoji jurisdikcija gali remtis teritoriniu principu, taip pat baudžiamųjų įstatymų galiojimo teisinė erdvė gali būti išplėsta pasitelkus eksteritorinės baudžiamosios jurisdikcijos principus[1]. Šiuo atveju BK aspektu aktualūs vėliavos (BK 4 straipsnio 1 dalis), aktyvus personalinis (BK 5 straipsnis), valstybės interesų apsaugos (BK 6 straipsnis) ir universalusis (BK 7 straipsnis) principai. Taigi, viena vertus, elementų – teritorijos, nusikalstamą veiką padariusio asmens statuso ir nusikalstamos veikos pobūdžio – kombinacija leidžia parinkti tinkamą baudžiamosios jurisdikcijos įgyvendinimo principą; kita vertus, jų analizė taip pat gali vesti prie išvados, kad dėl konkrečios nusikalstamos veikos valstybė baudžiamosios jurisdikcijos neturi. Aktualu ir tai, kad Lietuvos baudžiamasis įstatymas neįtvirtina individualių interesų apsaugos (pasyvaus personalinio) principo, todėl nusikalstamos veikos elektroninėje erdvėje (toliau – ir e. veikos) padarymo atveju galimybės nustatyti Lietuvos baudžiamąją jurisdikciją pagal nukentėjusiojo teisinį statusą, pavyzdžiui, atsižvelgiant į tai, kad jis yra Lietuvos pilietis ar kitas nuolatos Lietuvoje gyvenantis asmuo, kol kas nėra[2].

Nagrinėjant baudžiamosios jurisdikcijos problematiką e. veikos padarymo atveju, reikėtų atkreipti dėmesį į tai, kad Europos Sąjungos (kaip ir tarptautiniai) teisės aktai pirmumą teikia teritorinei jurisdikcijai, palyginti su kitais baudžiamosios jurisdikcijos principais[3]. Atsižvelgiant į tai, straipsnyje yra pasirinkta plačiau aptarti būtent teritorinio baudžiamosios jurisdikcijos principo taikymo galimybes ir ypatumus tais atvejais, kai nusikalstama veika yra padaryta elektroninėje erdvėje. Dėl ribotos straipsnio apimties jame nėra nagrinėjami principo non bis in idem (negalima dukart bausti už tą patį teisės pažeidimą), jurisdikcijų konkurencijos ar kolizijos, ekstradicijos ar asmens perdavimo pagal Europos arešto orderį aspektai.

Lietuvos mokslininkų baudžiamosios jurisdikcijos nustatymo problemos, kai padaryta nusikalstama veika elektroninėje erdvėje, nėra plačiai nagrinėtos. Valstybės baudžiamosios jurisdikcijos principais domėjosi A. Nevera, J. Namavičius; plačiau baudžiamosios jurisdikcijos nustatymo klausimais e. veikų padarymo atvejais

---

1 Andrius Nevera, *Valstybės baudžiamosios jurisdikcijos principai* (Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006), 12.

2 Plačiau apie individualių interesų apsaugos principo taikymo galimybes, jo ribas žr. Nevera, *supra note*, 1: 121–125; Justas Namavičius, „Baudžiamojo įstatymo galiojimas erdvėje“, iš *Globalizacijos iššūkiai baudžiamajai justicijai: recenzuotų mokslinių straipsnių baudžiamosios teisės, bausmių vykdymo ir baudžiamojo proceso klausimais rinkinys*, Jonas Prapiestis ir kt. (Vilnius: Registrų centras, 2014).

3 André Klip, *European Criminal Law. An Integrative Approach*, 3-iasis leidimas (Cambridge: Intersentia, 2016), 209.

pasisakė D. Valatkevičius. Taip pat galima būtų paminėti nemažai užsienio šalių mokslininkų, kėlusių baudžiamosios jurisdikcijos nustatymo elektroninėje erdvėje klausimų, kaip antai A. A. S. Al Hait, K. Soukieh, F. M. Kristin, I. Walden, D. C. Menthe, S. W. Brenner, B.-J. Koops ir kt.

Tyrimui atlikti daugiausia taikyti mokslinės literatūros ir dokumentų analizės, loginis, apibendrinimo ir dedukcinis metodai.

1. Baudžiamosios jurisdikcijos nustatymo problemos elektroninėje erdvėje, teritorinio principo dilema

Analizuojant Lietuvos baudžiamojo įstatymo nuostatas, reglamentuojančias šio įstatymo galiojimą erdvėje, matyti, kad jame neįtvirtina specialių baudžiamosios jurisdikcijos nustatymo taisyklių e. veikai. Taigi išvados, ar Lietuva dėl jų gali įgyvendinti savo baudžiamąją jurisdikciją, turėtų būti prieinama tinkamai interpretuojant bendrąsias jurisdikcijos nustatymo taisykles. Mokslinėje literatūroje nurodoma ir tai, kad „nepaisant nematerialios interneto prigimties teritorialumas vis dar laikomas pagrindiniu veiksniu“[4] nustatant valstybės baudžiamąją jurisdikciją e. veikos padarymo atveju. Kaip matyti, tokios pozicijos laikomasi „nepaisant ateritorinio interneto pobūdžio ir kompiuterinių duomenų nematerialumo“[5]. Atitinkamai BK 4 straipsnio 2 dalis, įtvirtinanti, kad „nusikalstamos veikos padarymo vieta yra vieta, kurioje asmuo veikė arba turėjo ir galėjo veikti, arba vieta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai“, yra skirta ne tik fizinei, bet ir elektroninei erdvei. Kita vertus, ši nusikalstamos veikos padarymo vietą apibrėžianti nuostata gali būti tinkamai pritaikoma tik prieš tai išsprendus elektroninės erdvės vietos problemą ir nustačius, ar ši vieta laikytina Lietuvos valstybės teritorija.

Pripažįstant teritorinio principo absoliutumą[6], valstybės teritorinė jurisdikcija bendriausia prasme reiškia, kad valstybės baudžiamieji įstatymai taikomi asmenims, padariusiems nusikalstamą veiką jos teritorijoje: „<...> asmenys, padarę nusikalstamas veikas Lietuvos valstybės teritorijoje <...> atsako pagal šį kodeksą“ (BK 4 straipsnio 1 dalis). Todėl nagrinėjant teritorinio principo esmę, be kita ko, yra svarbūs Lietuvos valstybės teritorijos ir nusikalstamos veikos padarymo vietos aspektai. Kai nusikalstama veika padaroma elektroninėje erdvėje, nusikalstamos veikos padarymo vieta, atsižvelgiant į elektroninės erdvės, veiksmų joje ypatumus, gali būti kiek gluminanti. Pirmiausia, tradicinė teritorinė baudžiamoji jurisdikcija paprastai yra apibrėžiama „keturių erdvių teorija“[7], todėl valstybės sausumos, vandens teritorija, valstybės oro

4 Kim Soukieh, „Cybercrime – The Shifting Doctrine of Jurisdiction“, *Canberra Law Review* 10, 1 (2011): 226.

5 Darius Valatkevičius, „Jurisdikcijos problematika tiriant kompiuterinius nusikaltimus“, *Teisė* 62 (2007): 136.

6 Nevera, *supra note*, 1: 27.

7 Li Jun ir Jia Jidong, „Confusion and Relief of Criminal Jurisdiction of Cybercrimes“, *Advances in Computer Science Research* 65 (2018): 51.

erdvė ir žemės gelmės, turinčios fiksuotas ribas fizinėje erdvėje, tampa svarbiais sprendžiant, ar nusikalstama veika padaryta konkrečios valstybės teritorijoje. Šie teritorijos elementai turi aiškų pastovų ryšį su fizine erdve, taigi akivaizdų ryšį su fizine erdve išsaugo ir tradicinė nusikalstama veika (pavyzdžiui, nužudymas (BK 129 straipsnis), kontrabanda (BK 199 straipsnis), jūros teršimas iš laivų (BK 270[3] straipsnis), neteisėtas valstybės sienos perėjimas (BK 291 straipsnis). Kadangi elektroninė erdvė pagal savo prigimtį neatitinka nei vienos iš minėtųjų, ji mokslinėje literatūroje bandoma įvardyti „penktąja erdve“[8], kurioje nebetenka prasmės fizinės erdvės ribos, joje nebėra apibrėžtų teritorijų – ištisas informacinių sistemų sukurtas pasaulis yra tarsi paprastas „paspaudimas“[9]. Tokio supratimo priežastys, be kita ko, susijusios su tuo, kad „geografinės ribos, kurios egzistuoja realiame pasaulyje, neegzistuoja elektroniniame pasaulyje“[10]. Kadangi nematerialios elektroninės erdvės neįmanoma suskirstyti į atitinkamas teritorijas kaip fizinės erdvės, sprendžiant dėl teritorinės baudžiamosios jurisdikcijos iki galo lieka neaiškus veikos elektroninėje erdvėje padarymo vietos ir fizinės teritorijos ryšys (ypač atsižvelgiant į elektroninės erdvės globalumą ir decentralizaciją). Šią problemą dar labiau išryškina e. veikų „neribotas išsiplėtimas“ ir „abstraktus tarpvalstybinis“[11] pobūdis, galintis lemti daugybines arba net nežinomą skaičių jurisdikcijų – tokiais atvejais paprastai nelieka vienos tradicine prasme suprantamos *locus delicti* (nusikalstamos veikos vietos). Kaip antai, 2017 m. „WannaCry“ (arba „WannaCrypt“) virusas užkrėtė daugiau nei 230 000 kompiuterių 150 valstybių[12]; žinomos 2020 m. AWS DDoS, 2018 m. GitHub DDoS ir daug kitų DDoS atakų buvo vykdomos pasitelkus robotizuotų kompiuterių tinklą (angl. *botnet*), kurį gali sudaryti dešimtys tūkstančių ar daugiau užkrėstų kompiuterių iš viso pasaulio. Atsižvelgiant į tokią e. veikos specifiką, mokslinėje literatūroje pabrėžiama, kad iš pirmo žvilgsnio suprantamos BK 4 straipsnio nuostatos, apibrėžiančios nusikalstamos veikos padarymo vietą, „dėl interneto ateritorialumo tampa daug painesnės ir problemiškesnės“[13].

Kita vertus, e. veikai yra būdingas ir dualumas – nors ji egzistuoja elektroninėje erdvėje, vis tiek yra padaroma panaudojant apčiuopiamas priemones (informacines sistemas) fizinėje erdvėje, taip pat šioje erdvėje gali sukelti ir pavojingų padarinių. Šį dualumą lemia tai, kad informacinė sistema, sudaryta iš tarpusavyje sąveikaujančių

8 Li Jun ir Jia Jidong, *supra note,* 7:51.

9 Adel Azzam Saqf Al Hait, „Jurisdiction in Cybercrimes: A Comparative Study“, *Journal of Law, Policy and Globalization* 22 (2014): 75.

10 Kristin M. Finklea, „The Interplay of Borders, Turf, Cyberspace and Jurisdiction: Issues Confronting U.S. Law Enforcement“, Congressional Research Service Report, 2013 m. sausio 17 d., žiūrėta 2021 m. birželio 5 d., https://fas.org/sgp/crs/misc/R41927.pdf.

11 Li Xiaobing ir Qin Yongfeng, „Research on Criminal Jurisdiction of Computer cybercrime“, *Procedia Computer Science* 131 (2019): 794.

12 Jesse M. Ehrenfeld, „WannaCry, Cybersecurity and Health Information Technology: A Time to Act“, *Journal of Medical Systems* 41 (2017).

13 Valatkevičius, *supra note*, 5: 129.

komponentų, turi tam tikrus fizinius parametrus, veikia fizinėje erdvėje. Kartu ši sistema sukuria elektroninę erdvę, taigi ji – fizinėje erdvėje veikiančios informacinės sistemos veiklos rezultatas. Tačiau elektroninė erdvė nėra analogiška fizinei erdvei, ji tiesiogiai neatkartoja tradicinių fizinės erdvės geografinių ribų. Aptartas dualumas lemia, kad asmuo, atliekantis veiksmus elektroninėje erdvėje, niekada nebus tik elektroninėje erdvėje, o visada bus pagal savo prigimtį skirtingose abiejose erdvėse – realioje ir elektroninėje – tuo pačiu metu[14]. Mokslinėje literatūroje pripažinus, kad teritorinis baudžiamosios jurisdikcijos principas yra dominuojantis (net ir tais atvejais kai turima mintyje elektroninė erdvė), teigiama ir tai, jog yra būtina „rasti būdą kibernetinei veiklai „įžeminti"[15], ją susieti ir su fizine erdve. Būtent šis e. veikos dualumas lemia, kad vis dėlto yra bandoma nustatyti tam tikras ribas – *technologines* arba *fizines* – elektroninei erdvei.

Sprendžiant baudžiamosios jurisdikcijos problemas elektroninėje erdvėje, aktualu ir tai, kad „aplinkos pobūdis"[16] gali turėti reikšmingos įtakos tradicinėms teisės koncepcijoms ir principams. Ne išimtis būtų ir tradicinių baudžiamosios jurisdikcijos principų (ypač teritorinio) aiškinimas ir taikymas elektroninei erdvei. Minėta, kad, išnykus fizinei erdvei būdingos teritorijos koncepcijai elektroninėje erdvėje, šios erdvės ribų idėja tampa gana miglota. Sprendžiant šias problemas, mokslinėje literatūroje bandoma pateikti įvairių elektroninei erdvei pritaikytų ir į teritorinės baudžiamosios jurisdikcijos klausimus leidžiančių atsakyti teorijų. Kartu natūralu, kad dėl virtualaus e. veikos pobūdžio šie požiūriai turi ir tam tikrų ypatumų bei skirtumų, palyginti su tradiciniais nusikalstamos veikos padarymo vietos nustatymo kriterijais fizinėje erdvėje. Kaip antai, mokslinėje literatūroje galima aptikti elektroninės erdvės autonomijos, praplėstos teritorinės jurisdikcijos, ribotos jurisdikcijos (tiesioginio ryšio), fizinio kontakto, šaltinio (tiekėjo) šalies[17] ir daug kitų teorijų. Kita vertus, šių teorijų pritaikymas tiesiogiai priklauso nuo nacionalinių teisės aktų, apibrėžiančių baudžiamojo įstatymo galiojimą erdvėje, o nagrinėjamu Lietuvos teritorinės baudžiamosios jurisdikcijos aspektu – nuo nuostatų, apibrėžiančių baudžiamojo įstatymo galiojimą asmenims, padariusiems nusikalstamą veiką Lietuvos valstybės teritorijoje (BK 4 straipsnis).

2. Elektroninė erdvė ir baudžiamosios jurisdikcijos principai, nustatyti tarptautiniuose bei Europos Sąjungos teisės aktuose. E. veikos padarymo vietos interpretavimas

Analizuojant tarptautinių ir Europos Sąjungos teisės aktų nuostatas, reglamentuojančias valstybių jurisdikciją nusikalstamoms veikoms elektroninėje erdvėje, ak-

14 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 21.

15 Frances P. Bernat ir Nicholas Godlove, „Understanding 21st Century Cybercrime for the 'Common' Victim", *Criminal Justice Matters* 89, 1 (2012): 5.

16 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford: Oxford University Press, 2007), 297.

17 Jun ir Jidong, *supra note*, 7: 52–53; Xiaobing ir Yongfeng, *supra note*, 11: 795–796.

tualu tai, kad e. veikos šiuo aspektu turėtų būti apibrėžiamos pačia plačiausia prasme. Taigi tinkamas baudžiamosios jurisdikcijos nustatymas yra aktualus nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui (BK XXX skyrius) atveju, taip pat tuo atveju, kai padaryta tradicinė, tačiau dėl informacinių technologijų panaudojimo pakitusi nusikalstama veika (pavyzdžiui, sukčiavimas, dokumento suklastojimas ar disponavimas suklastotu dokumentu, šmeižimas, neapykantos, teroristinių nusikaltimų kurstymas elektroninėje erdvėje). Baudžiamosios jurisdikcijos kontekste paminėtina ir tai, kad tarptautiniai bei Europos Sąjungos teisės aktai nustato tik bendrus minimalius standartus, atspindi minimalų susitarimą, todėl šie teisės aktai neatmeta platesnio reglamentavimo galimybės nacionaliniuose įstatymuose. Pavyzdžiui, 2001 m. Konvencija dėl elektroninių nusikaltimų[18] (toliau – ir Konvencija) įtvirtina, kad ji „nepašalina jokios baudžiamosios jurisdikcijos, vykdomos pagal vidaus teisę“ (22 straipsnio 4 dalis).

Taigi valstybių baudžiamosios jurisdikcijos taisykles nusikalstamos veikos elektroninėje erdvėje atveju, be kita ko, nustato minėta Konvencija, 2003 m. Konvencijos dėl elektroninių nusikaltimų Papildomas protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo[19] (ratifikuota 2006 m.), 2008 m. lapkričio 28 d. Tarybos pamatinis sprendimas 2008/913/TVR dėl kovos su tam tikromis rasizmo ir ksenofobijos formomis bei apraiškomis baudžiamosios teisės priemonėmis[20], Europos Parlamento ir Tarybos 2011 m. gruodžio 13 d. direktyva 2011/93/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR[21] (toliau – ir Direktyva 2011/93/ES), Europos Parlamento ir Tarybos 2013 m. rugpjūčio 12 d. direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR[22] (toliau – ir Direktyva 2013/40/ES). Apibendrinus šiuos teisės aktus, reikėtų akcentuoti, kad jie e. veikas reglamentuoja skirtinga apimtimi. Kaip antai, Konvencija nustato nusikaltimus kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui (1 dalis), kompiuterinius nusikaltimus (2 dalis), turinio nusikaltimus (3 dalis) ir nusikaltimus, susijusius su autorių teisių ir gretutinių teisių pažeidimais (4 dalis), taigi ne tik specifines e. veikas (pavyzdžiui, neteisėta prieiga, neteisėta perimtis ar poveikis sistemai), bet ir tradicines

18 „Konvencija dėl elektroninių nusikaltimų“, *Valstybės žinios*, 2004-03-07, Nr. 36-1188, žiūrėta 2021 m. birželio 5 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.228195.

19 „Konvencijos dėl elektroninių nusikaltimų Papildomas protokolas dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo“, *Valstybės žinios*, 2006-07-05, Nr. 75-2850, žiūrėta 2021 m. birželio 5 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.279838?positionInSearchResults=12&searchModelUUID=7f9214d5-c85a-48c3-b26b-1142e7592c90.

20 OL 2008 L 328, 55–58.

21 OL 2011 L 335, 1.

22 OL 2013 L 218, 8.

nusikalstamas veikas, pakitusias dėl informacinių technologijų panaudojimo (pavyzdžiui, kompiuterinė klastotė, kompiuterinis sukčiavimas, nusikaltimai, susiję su vaikų pornografija). O Direktyva 2013/40/ES, skirtingai nei Konvencija, nustato tik išimtinai dėl informacinių technologijų raidos atsiradusias nusikalstamas veikas (pavyzdžiui, neteisėtą įsikišimas į sistemą ar duomenis, neteisėtą duomenų perėmimą), tradicinių nusikalstamų veikų, padarytų elektroninėje erdvėje, ji nereglamentuoja. Atitinkamai į minėtus skirtumus turėtų būti atsižvelgiama analizuojant šiuose tarptautiniuose ir Europos Sąjungos teisės aktuose nurodytas jurisdikcijos taisykles.

Konvencijoje jurisdikcijos taisyklės įtvirtintos nurodant, kad turi būti priimti teisės aktai ir kitos priemonės, „kurių gali prireikti nustatyti jurisdikciją šios Konvencijos 2–11 straipsniuose nurodytiems nusikaltimams, kai nusikaltimas padarytas: a) jos teritorijoje; b) laive, plaukiojančiame su tos Šalies vėliava; c) orlaivyje, įregistruotame pagal tos Šalies įstatymus; d) tos Šalies piliečio, jeigu padarius nusikaltimą yra baudžiama pagal baudžiamuosius įstatymus arba jeigu toks nusikaltimas yra padarytas už bet kurios valstybės teritorinės jurisdikcijos“ (3 skirsnio 22 straipsnio 1 dalis). Konvencijos aiškinamajame rašte[23] atkreipiamas dėmesys į tai, kad minėtas a punktas yra grindžiamas teritoriniu principu, todėl valstybė turi bausti už Konvencijoje minimą nusikalstamą veiką, jei ji padaryta tos valstybės teritorijoje. Pavyzdžiui, teritorinė jurisdikcija būtų įgyvendinama tiek tada, kai abu – kaltininkas ir neteisėtai veikiama informacinė sistema – yra valstybės teritorijoje, tiek ir tada, kai jos teritorijoje yra tik informacinė sistema, nors kaltininko joje ir nėra (233 punktas).

Direktyva 2013/40/ES taip pat nustato panašias jurisdikcijos taisykles, taigi jurisdikcija direktyvoje įtvirtintoms nusikalstamoms veikoms turi būti nustatyta tais atvejais, „kai: a) nusikalstama veika arba jos dalis padaryta jų teritorijoje; arba b) nusikalstamą veiką padarė vienas iš jų piliečių, bent tais atvejais, kai veiksmas yra nusikalstama veika toje vietoje, kurioje jis buvo įvykdytas“ (12 straipsnio 1 dalis). Kaip matyti, minėtas a punktas įtvirtina valstybės teritorinę jurisdikciją, kuri, vadovaujantis Direktyvos 2013/40/ES nuostatomis, turėtų būti taikoma tiek tais atvejais, kai „a) pažeidėjas nusikalstamą veiką įvykdo fiziškai būdamas jos teritorijoje, nepriklausomai nuo to, ar nusikalstama veika yra nukreipta ar nenukreipta prieš jos teritorijoje esančią informacinę sistemą; arba b) nusikalstama veika yra nukreipta prieš jos teritorijoje esančią informacinę sistemą nepriklausomai nuo to, ar pažeidėjas nusikalstamą veiką daro fiziškai būdamas jos teritorijoje“ (12 straipsnio 2 dalis). Šiuo aspektu atkreiptinas dėmesys į tai, kad Europos Sąjungos teisės aktai paprastai palieka galimybę nacionalinei teisei nustatyti *locus delicti*. Tačiau galimos ir retos išimtys, kaip, pavyzdžiui, minėtuoju atveju atsižvelgiama „į priemones, kurias panaudojus buvo padaryta nusikalstama veika“[24].

---

23 „Explanatory Report to the Convention on Cybercrime“, *European Treaty Series – No. 185*, žiūrėta 2021 m. birželio 5 d., https://rm.coe.int/16800cce5b.

24 Klip, *supra note*, 3: 209.

Apibendrinus minėtas Konvencijos ir Direktyvos 2013/40/ES nuostatas, matyti, kad nusikalstamos veikos padarymo vietos aiškinimas šiomis nuostatomis išplečiamas, todėl nusikalstamos veikos padarymo vieta yra siejama ne tik su kaltininko, bet ir su informacinės sistemos fizinio buvimo vieta. Į tokią e. veikos padarymo vietos nustatymo specifiką atkreiptas dėmesys ir mokslinėje literatūroje, kurioje teigta, kad kompiuterinių nusikaltimų padarymo vieta, be kita ko, yra „kompiuterinės įrangos ar elektroninių ryšių buvimo vieta“[25]. Šis *informacinės sistemos buvimo vietos kriterijus*, be kita ko, gali būti išvedamas iš anksčiau aptarto e. veikai būdingo dualumo – nors ji padaroma elektroninėje erdvėje, tačiau šią erdvę sukuria informacinės sistemos, esančios fizinėje erdvėje. Taigi informacinės sistemos buvimo vieta leidžia susieti e. veiką su fizine erdve, su tam tikra teritorija ir sudaro galimybių atrasti fizinei erdvei būdingus baudžiamosios jurisdikcijos nustatymo kriterijus bei juos taikyti e. veikos padarymo atveju. Šiuo aspektu svarbu ir tai, kad toks nusikalstamos veikos padarymo vietos aiškinimas turėtų būti taikomas e. veikoms, suvokiamoms plačiąja prasme, todėl yra aktualus tiek, pavyzdžiui, kompiuterinio sukčiavimo (BK 182 straipsnis) ar klastotės (BK 300 straipsnis) atvejais, tiek ir tada, kai padarytas neteisėtas poveikis sistemai (BK 197 straipsnis) ar prie jos neteisėta gauta prieiga (BK 198[1] straipsnis).

Sprendžiant dėl teritorinės baudžiamosios jurisdikcijos taisyklių taikymo tais atvejais, kai nusikalstama veika padaryta elektroninėje erdvėje, aktuali įžvalga, kad „Lietuvos Respublikos tarptautinių sutarčių ir ES teisės aktų įgyvendinimas nacionalinėje baudžiamojoje teisėje galimas tik suderinus nacionalinio baudžiamojo įstatymo nuostatas su tarptautinės sutarties ar ES teisės aktų reikalavimais“[26]. Su tokiu suderinamumu siejamas ir tinkamas šių teisės aktų vykdymas. Pavyzdžiui, Lietuvai 2004 m. ratifikavus Konvenciją, taip pat perkėlus Direktyvos 2013/40/ES nuostatas į nacionalinę teisę baudžiamojo įstatymo galiojimo asmenims, padariusiems nusikalstamas veikas Lietuvos valstybės teritorijoje (BK 4 straipsnis), nuostatos nebuvo keistos. Atitinkamai galima būtų teigti, kad, įstatymo leidėjo nuomone, Lietuvos BK, reglamentuojantis teritorinį baudžiamosios jurisdikcijos principą ir su juo susijusius nusikalstamos veikos padarymo vietos nustatymo klausimus, atitinka minėtų tarptautinių ir Europos Sąjungos teisės aktų reikalavimus. Atsižvelgiant į tai, Lietuva, be kita ko, turėtų užtikrinti savo teritorinės jurisdikcijos taikymą, jeigu kaltininkas padarė e. veiką būdamas fiziškai jos teritorijoje; jei jos teritorijoje buvo neteisėtą poveikį patirianti informacinė sistema (gali sutapti su fizinio asmens buvimo vieta arba ne). Kartu galėtų būti sprendžiama, ar e. veikos padarymo vieta negalėtų būti laikoma ir ta vieta, kurioje kaltininkas panaudojo e. veikos padarymo priemones (įrankius) (pavyzdžiui, informacinę sistemą). Šių tiesiogiai panaudotų priemonių (įrankių) buvimo vieta dėl informacinių sistemų veikimo ypatumų ir elektroninės erdvės globalumo gali nesutapti su kaltininko ar puolamos informacinės sistemos buvimo vieta.

---

25 Valatkevičius, *supra note*, 5: 136.

26 Gintaras Švedas ir kt., *Lietuvos Respublikos baudžiamojo kodekso bendrosios dalies vientisumo ir naujovių (su)derinimo iššūkiai* (Vilnius: Vilniaus universiteto leidykla, 2017), 39.

Pavyzdžiui, nustatoma, kad valstybės teritorijoje yra tik informacinė sistema, kurioje laikoma kenkimo programinė įranga, slaptažodžiai, kodai ar kitokie panašūs duomenys (BK 1982 straipsnis); tradicinės nusikalstamos veikos atveju gali būti turima žinioje įvairi neteisėto turinio informacija, pavyzdžiui, pornografinio turinio dalykai, kuriuose vaizduojamas vaikas ar asmuo pateikiamas kaip vaikas (BK 300 straipsnis), dalykai, kuriuose, be kita ko, kurstoma diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl amžiaus, lyties ir kt. (BK 170 straipsnis).

Tai, kad e. veikos padarymo vieta yra tiek kaltininko, tiek informacinės sistemos buvimo vieta, patikslinta ir Lietuvos teismų praktikoje taikant baudžiamojo įstatymo nuostatas. Kaip antai, Lietuvos Aukščiausiojo Teismo 2015 m. gegužės 12 d. nutartyje baudžiamojoje byloje Nr. 2K-188-489/2015 išspręstas neteisėto poveikio informacinei sistemai (BK 197 straipsnis) vykdant DDoS (paskirstyto atsisakymo aptarnauti) ataką padarymo vietos klausimas. Teismas šioje byloje priėjo išvadą, kad Lietuva tinkamai taikė savo baudžiamąją jurisdikciją, nes minėtos kaltininko organizuotos atakos įvykdytos iš Lietuvos, nors ir buvo nukreiptos prieš informacinę sistemą Švedijoje:

„Nuteistojo A. V. gynėja nurodo, kad pagal BK 4 straipsnio 2 dalies nuostatas nuteistajam inkriminuotos nusikalstamos veikos, numatytos BK 197 straipsnyje, padarymo vieta yra ta, kurioje sutriko ar nutrūko informacinės sistemos darbas. Šioje byloje nustatyta, kad sistemos darbo sutrikdymas buvo fiksuotas Švedijoje. Taigi, kasatorės nuomone, kyla abejonių, ar Lietuvos Respublikos teismai turėjo jurisdikcijos teisę nagrinėti baudžiamąją bylą dėl A. V. padarytos nusikalstamos veikos. Su šiais kasatorės argumentais teisėjų kolegija neturi pagrindo sutikti.

Iš tiesų, sprendžiant dėl BK 197 straipsnyje numatytų nusikalstamų veikų padarymo vietos, yra aktuali BK 4 straipsnio 2 dalis, kurioje nurodoma, kad nusikalstamos veikos padarymo vieta yra vieta, kurioje asmuo veikė arba turėjo ir galėjo veikti, arba vieta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai. Taigi, nusikalstamo neteisėto poveikio informacinei sistemai padarymo vieta yra tiek ta, iš kurios buvo trikdomas tinklalapių darbas, tiek ir ta, kurioje kilo BK 197 straipsnyje nurodyti padariniai.

Aiškinant baudžiamosios jurisdikcijos taikymo galimybes, aktualios į Lietuvos nacionalinę teisę perkelto Pagrindų sprendimo 2005/222/TVR nuostatos, be kita ko, numatančios ir minimalius reikalavimus valstybės jurisdikcijai. Pagrindų sprendimo 2005/222/TVR 10 straipsnyje nurodoma, kad valstybės nustato savo jurisdikciją nusikalstamoms veikoms, inter alia, tais atvejais, kai nusikalstama veika buvo visiškai arba iš dalies įvykdyta jų teritorijoje. Šią nuostatą tikslinančioje Pagrindų sprendimo 2005/222/TVR 10 straipsnio 2 dalyje nurodoma, kad valstybės užtikrina, kad jos jurisdikcijai priklausytų atvejai kai: 1) kaltininkas nusikaltimą veiką įvykdo fiziškai būdamas jos teritorijoje, nepriklausomai nuo to, ar nusikalstama veika yra nukreipta ar nenukreipta prieš jos teritorijoje esančią informacinę sistemą; 2) nusikalstama veika yra nukreipta prieš jos teritorijoje esančią informacinę sistemą, nepriklausomai nuo to, ar kaltininkas įvykdo nusikalstamą veiką fiziškai būdamas ar nebūdamas jos teritorijoje. Byloje nustatyta, kad A. V. organizuotos DDoS atakos prieš tinklala-

pius www.t.lt ir www.tv.lt buvo įvykdytos Lietuvos Respublikoje, UAB „R.“ tarnybinėse patalpose, esančiose Vilniuje.

Atsižvelgiant į tai, kas išdėstyta, teisėjų kolegija konstatuoja, kad Lietuvos Respublikos jurisdikcija šioje byloje įgyvendinta tinkamai, BK 4 straipsnio nuostatos joje nebuvo pažeistos.“[27]

3. Esminio ryšio kriterijus ir jo svarba

Vis dėlto reikėtų pripažinti, kad minėti Europos Sąjungos ir tarptautiniai teisės aktai neišsprendžia visų galimų baudžiamosios jurisdikcijos problemų, ypač turint mintyje galimas komunikavimo elektroninėje erdvėje situacijas. Šiuo aspektu yra taikliai pastebima, kad galimybės įgyvendinti baudžiamąją jurisdikciją dėl elektroninėje erdvėje padarytos nusikalstamos veikos „priklausys nuo nacionalinių teisės aktų, kurie gali būti <...> sunkiai pritaikomi už valstybės teritorijos ribų“[28].

Atsižvelgiant į tai, kad elektroninėje erdvėje bendriausia prasme yra sąveikaujama dviem pagrindiniais būdais, kai duomenys (informacija) pateikiami elektroninėje erdvėje ir duomenys paimami iš elektroninės erdvės, galima kalbėti apie du savarankiškus komunikavimo elektroninėje erdvėje dalyvius – „duomenis įkeliantį ir duomenis parsisiųsdinantį“[29]. Pirmu atveju duomenis įkeliantis komunikacijos dalyvis gali būti pakankamai aktyvus, todėl duomenys yra siunčiami duomenų gavėjui. Tokie kaltininko veiksmai yra „siejami tarsi su informacijos „stūmimu“ iš siuntėjo šios informacijos gavėjui“[30]. Lietuvos baudžiamosios jurisdikcijos įgyvendinimo galimybės neturėtų kelti didesnių problemų, jei toks komunikavimo turinys duomenų gavėją pasiekė jos teritorijoje. Šie aktyvūs duomenų siuntėjo veiksmai paprastai leidžia konstatuoti kažkurio iš nusikalstamos veikos sudėties požymių realizavimą Lietuvos teritorijoje, nes šioje teritorijoje veika buvo pradėta, baigta arba nutrūko (BK 4 straipsnio 3 dalis). Kaip antai, sukčiavimo elektroninėje erdvėje atveju (BK 182 straipsnis) nukentėjusį asmenį klaidinanti informacija siunčiama elektroniniu paštu, todėl šio asmens suklaidinimas (apgaulės realizavimas) gali būti konstatuojamas ir ten, kur elektroniniai laiškai buvo gauti; turto prievartavimo (BK 181 straipsnis) ar grasinimo nužudyti ar sunkiai sutrikdyti žmogaus sveikatą arba žmogaus terorizavimo (BK 145 straipsnis) atvejais atitinkamo turinio grasinimų realizavimas taip pat gali būti konstatuojamas elektroninių laiškų gavimo vietoje. Taigi, kai nusikalstamos veikos požymiai yra realizuojami panaudojant elektroninių duomenų perdavimą, nusikalstamos veikos padarymo vieta gali būti laikoma

27 „Lietuvos Aukščiausiojo Teismo 2015 m. gegužės 12 d. nutartyje baudžiamojoje byloje Nr. 2K-188-489/2015“.

28 Gregor Urbas, „Criminalizing Computer Misconducts: Some Legal and Philosophical Problems“, *Asia Pacific Law Review* 14, 1 (2016): 107.

29 Darrel C. Menthe, „Jurisdiction in Cyberspace: A Theory of International Spaces“, *Michigan Telecommunication and Technology Law Review* 4, 1 (1998): 73.

30 Renata Marcinauskaitė, *Nusikalstamos veikos elektroninėje erdvėje: elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje* (Vilnius: Registrų centras, 2019), 215.

tiek ta, iš kurios kaltininkas atitinkamo turinio duomenis išsiuntė, tiek ir ta, kurioje tokie duomenys buvo gauti, t. y. kur elektroninės komunikacijos turinys pasiekė gavėją.

Duomenų perdavai (angl. *traffic*) elektroninėje erdvėje būdinga tai, kad duomenys „keliauja *greičiausiu* maršrutu, kuris ne visuomet gali būti *tiesioginis* maršrutas geografine prasme“[31]. Atsižvelgiant ir į tai, kad elektroninis laiškas iki adresato keliauja padalytas į duomenų paketus, šie paketai gali būti siunčiami visiškai skirtingais maršrutais, taigi gali kirsti skirtingų valstybių teritorijas. Šie maršrutai yra nepastovūs ir nenuspėjami, todėl galima būtų teigti, kad, priešingai nei keliaujant fizinėje erdvėje, asmuo, siųsdamas duomenis elektroninėje erdvėje paprastai maršrutų nenumato ir negali jų sąmoningai susieti su kuria nors kertamos valstybės teritorija[32]. Tokiais atvejais, sprendžiant baudžiamosios jurisdikcijos klausimą, manytina, kad duomenų perdavimas turėtų būti vertinamas kaip vientisas procesas, todėl esminė reikšmė nustatant, kur buvo padaryta nusikalstama veika, teiktina elektroninio laiško išsiuntimo ir jo gavimo vietoms. Kartu reikėtų atkreipti dėmesį į tai, kad šis požiūris nepaneigia elektroninių įrodymų rinkimo vietų įvairovės[33], o tik nustato galimas nusikalstamos veikos padarymo vietas BK 4 straipsnio prasme. Kita vertus, neatmestinas ir platesnis požiūris, jei nacionaliniai teisės aktai tokią galimybę nustato. Kaip antai, teritorinis reikalavimas gali būti grindžiamas nacionaliniuose teisės aktuose įtvirtintu „bet kieno vietos“[34] (angl. *location of anything*) požiūriu, todėl teritorinė jurisdikcija įgyvendinama ir tais atvejais, kai, pavyzdžiui, elektroniniai duomenys kirto valstybės teritoriją tranzitu[35]. Iš esmės tai situacijos, kai valstybės teritorijoje yra elektroninių ryšių tinklai, kuriais šie duomenys buvo siunčiami.

Kiek sudėtingesnė problema kyla sprendžiant dėl valstybės baudžiamosios jurisdikcijos įgyvendinimo galimybių, kai duomenis įkeliantis asmuo yra pasyvus komunikavimo elektroninėje erdvėje dalyvis. Su tokiu pasyviu elgesiu yra susijęs galimybių prieiti prie duomenų suteikimas, kai duomenys tampa prieinamais, pavyzdžiui, juos paskelbus tinklapyje ir nesiimant aktyvių veiksmų susisiekti su potencialiu duomenų gavėju. Šioje situacijoje aktyviu tampa būtent duomenų gavėjas, pats radęs prieigą prie elektroninėje erdvėje paskleistos informacijos ir atlikęs tarsi duomenų „traukimo“[36] veiksmus. Kaip antai, neteisėto turinio nusikalstamos veikos[37] atveju

---

31 Alexandra Perloff-Giles, „Transnational Cyber Offenses: Overcoming Jurisdictional Challenges“, *The Yale Journal of International Law* 43, 191 (2018): 196.

32 *Ibid*, 206.

33 Jei, pavyzdžiui, informacinės sistemos, dalyvavusios duomenų perdavime, galėjo atlikti duomenų fiksavimo ir saugojimo funkciją.

34 Susan W. Brenner ir Bert-Jaap Koops, „Approaches to Cybercrime Jurisdictions“, *Journal of Hight Technology Law* 4, 1 (2004): 20.

35 Brenner ir Koops, *supra note*, 33.

36 Marcinauskaitė, *supra note*, 29: 214–215.

37 Pavyzdžiui, disponavimas pornografinio turinio dalykais, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas (BK 309 straipsnis), kurstymas prieš bet kokios tautos, rasės, etninę, religinę

tinklapis ir jame esanti informacija gali būti prieinama Lietuvos teritorijoje (kaip ir daugelyje kitų valstybių), nors pats tinklapis yra užsienyje esančiame serveryje, t. y. informacinėje sistemoje, kurios buvimo vieta yra už Lietuvos teritorijos ribų. Toks išsidėstymas geografiniu aspektu yra galimas ir daugelio kitų e. veikų padarymo atveju, pavyzdžiui, sukčiaujant elektroninėje erdvėje, tinklapyje yra pateikiama asmenį klaidinanti informacija, siekiant apgaule įgyti svetimą turtą (turtinę teisę) (BK 182 straipsnis); šmeižiant žmogų tinklapyje, paskleidžiama tikrovės neatitinkanti informacija, galinti jį paniekinti, pažeminti ar pakirsti pasitikėjimą juo (BK 154 straipsnis) ir pan. Anksčiau aptarto *informacinės sistemos buvimo vietos kriterijaus* absoliutus taikymas šiose situacijose vestų prie vienintelio atsakymo, kad nusikalstamos veikos padarymo vieta yra ne Lietuvos teritorija, atitinkamai dėl tokios veikos Lietuva negali įgyvendinti savo baudžiamosios jurisdikcijos. Kita vertus, akcentuotina, kad atitinkamo turinio informacijos prieinamumas elektroninėje erdvėje gali reikšti, jog nusikalstamas poveikis yra sąmoningai nukreiptas, be kitų, ir į Lietuvos teritoriją, net jei šioje teritorijoje nėra dominančios informacinės sistemos ar fizinio asmens. Identifikavus tokį galimą e. veikos padarymo mechanizmą, mokslinėje literatūroje, atsižvelgiant į besivystančią teismų praktiką, yra plėtojamas *esminio ryšio kriterijus* (angl. *substantial, significant link*). Jį taikant vertinama, kiek esminis (svarbus) ryšys su konkrečios valstybės teritorija turi būti nustatytas, kad ji galėtų konstatuoti savo baudžiamąją jurisdikciją dėl atitinkamos elektroninėje erdvėje padarytos veikos.

Prieš aptariant minėtą *esminio ryšio kriterijų*, reikėtų atkreipti dėmesį į tai, kad valstybės baudžiamosios jurisdikcijos įgyvendinimo klausimas minėtos neteisėto turinio nusikalstamos veikos padarymo atveju gali būti sprendžiamas įvairiai. Vadovaujantis plačiausiu požiūriu, valstybės baudžiamajai jurisdikcijai konstatuoti pakanka to, kad dominantis tinklapis ir jame esanti informacija yra prieinama tos valstybės teritorijoje. Atitinkamai toks požiūris vestų prie išvados, kad „paskleidimo veiksmai yra padaryti kiekvienoje vietoje, kurioje medžiaga gali būti gauta ir peržiūrėta“[38], neatsižvelgiant į tai, kad tinklapyje pateikta informacija gali neturėti jokio ryšio su valstybe. Kitas – riboto taikymo – požiūris taip pat laikytinas pakankamai radikaliu, atmetančiu bet kokias baudžiamosios jurisdikcijos įgyvendinimo galimybes, jei asmuo, pavyzdžiui, „tiesiog įkėlė pornografinio pobūdžio <...> medžiagą užsienio žiniatinklio serveryje“[39]. Pripažinus šių teorijų trūkumus, mokslinėje literatūroje[40] pabrėžiamas esminio, tiesioginio, numatomo poveikio valstybės teritorijai nustaty-

ar kitokią žmonių grupę (BK 170 straipsnis), viešas pritarimas tarptautiniams nusikaltimams, SSRS ar nacistinės Vokietijos nusikaltimams Lietuvos Respublikai ar jos gyventojams, jų neigimas ar šiurkštus menkinimas (BK 170[2] straipsnis).

38 Brenner ir Koops, *supra note*, 33: 15.

39 Ulrich Sieber, „Cybercrime and Jurisdiction in Germany. The present situation and the need for new solutions“, iš *Cybercrime and Jurisdiction: A Global Survey*, Bert-Jaap Koops, Susan W. Brenner (The Hague: T.M.C. Asser Press, 2006), 190.

40 Sieber, *supra note*, 38: 191–192; Walden, *supra note*, 16: 300–304.

mo poreikis. Toks požiūris gali būti laikomas kompromisiniu, nes yra pagrįstas tam tikrų objektyvių ir subjektyvių kriterijų[41] taikymu, racionalumo reikalavimu valstybei apsisprendžiant dėl savo baudžiamosios jurisdikcijos įgyvendinimo. Kaip antai, tokiais atvejais, be informacinės sistemos buvimo vietos, gali būti vertinama, kiek esmingai veika yra susieta su atitinkamos valstybės teritorija (pavyzdžiui, kokia kalba pateikta informacija, ar ši kalba leidžia susieti veiką su valstybės teritorija, kokia yra pateikiamos informacijos tikslinė auditorija, kokio tai pobūdžio informacija ir kt.); koks yra kaltininko, nukentėjusio asmens, žiniatinklio svetainės administratoriaus ir konkrečios valstybės ryšys; kur informacija buvo sukurta ir parsisiųsdinta; kaltininko suvokimas ar siekis, kad atitinkamo turinio informacija būtų pasiekiama konkrečios valstybės teritorijoje; baudžiamosios jurisdikcijos įgyvendinimo svarba valstybei, tarptautinei bendruomenei (siejama su tarptautiniu solidarumu), politinei, teisinei ar ekonominei sistemai ir pan. Kaip antai, minėta, kad sukčiavimo elektroninėje erdvėje atveju interneto puslapyje gali būti pateikiama asmenis klaidinanti informacija, nors pats tinklapis kaip apgaulės panaudojimo priemonė paprastai yra užsienyje esančiuose serveriuose, taip pat jokios sąsajos su atitinkama valstybe gali neturėti ir užsienyje esantis kaltininkas. Tokiais atvejais, taikant *esminio ryšio kriterijų*, nusikalstamos veikos (sukčiavimo) sąsają su geografinėmis valstybės ribomis gali rodyti daug aplinkybių: interneto puslapis yra žinomas, lengvai prieinamas valstybės teritorijoje; jame informacija pateikiama tos valstybės ar kita gyventojams suprantama kalba; tinklapyje pateikiamos nuorodos, turinčios sąsajų su valstybe; naudojamos tai valstybei žinomų asmenų nuotraukos, įvairūs faktai ar įvykiai; numatyta galimybė žadamas prekės siųsti (gabenti), paslaugas suteikti valstybės teritorijoje, jei sukčiavimas siejamas su prekių ar paslaugų užsakymu; iš valstybės teritorijos priimami mokėjimai; sąsają su konkrečios valstybės teritorija gali rodyti ir bet kokie kiti kaltininko veiksmai, liudijantys jo ketinimus bendrauti su atitinkamos valstybės teritorijoje esančiu asmeniu. Būtent tokių aplinkybių visuma rodo, kad veika (be kita ko, apgaulė) yra akivaizdžiai nukreipta į konkrečios valstybės teritoriją net ir tuo atveju, jei kaltininko ir informacinės sistemos buvimo vieta yra už šios valstybės teritorijos ribų.

Nagrinėjamu esminio ryšio su valstybės teritorija aspektu gali būti aktualus ir *mutatis mutandis* (su būtinais (atitinkamais) pakeitimais) baudžiamosiose bylose (be kita ko, šmeižimo) pritaikomas išaiškinimas, pateiktas Lietuvos Aukščiausiojo Teismo 2021 m. balandžio 14 d. nutartyje civilinėje byloje Nr. e3K-3-89-916/2021[42]: *Atsižvelgiant į didelį žmonių mobilumą ir tai, kad veiksmų atlikimas internete mažai koreliuoja su fizine asmens buvimo vieta, taip pat į tai, kad internetinės publikacijos įprastai turi savo tikslinę auditoriją, tokia vieta taip pat gali būti pripažįstama ir (ii) valstybė, į kurią yra nukreipta atitinkama publikacija. Ši vieta dažniausiai bus ieškovo*

41 Sieber, *supra note*, 38: 191.

42 Šioje byloje Ukrainos pilietis, gyvenantis Lietuvoje, kreipėsi į teismą, be kita ko, dėl Rusijoje gyvenančio asmens socialinio tinklo „Twitter“ paskyroje paskleistos galbūt tikrovės neatitinkančios, garbę ir orumą žeminančios žinios.

gyvenamoji (buveinės) vieta. Informacijos nukreipimo aplinkybę gali rodyti atitinkamo interneto resurso lankytojų pasiskirstymo geografija, lankomumo statistika, informacijos kalba, informacijos turinys, aktualumas tam tikrai vietai ar regionui ir kt. Galiausiai, kadangi paskleidimo būtinoji sąlyga yra tai, kad informacija būtų sužinota, o žala reputacijai galima tik kitam asmeniui sužinojus atitinkamą informaciją, reikia pripažinti, kad tokia vieta gali būti ir (iii) valstybė, kurioje atitinkama informacija buvo jos adresatų sužinota, nes būtent šioje vietoje dažniausiai atsiras žala. Sužinojimas atitinka „kitos aplinkybės, tapusios pagrindu reikalauti atlyginti žalą" sąvoką. Šis jurisdikcijos pagrindas taip pat dažniausiai atitiks nukentėjusio asmens gyvenamąją (buveinės) vietą.

Ar esminio ryšio kriterijus yra pritaikomas sprendžiant dėl Lietuvos teritorinės baudžiamosios jurisdikcijos įgyvendinamumo galimybių, vertintinos ubikvitacinę teoriją įtvirtinančios BK 4 straipsnio 2 ir 3 dalių nuostatos. Pagal šią teoriją, nusikalstamos veikos padarymo vieta yra 1) asmens veikimo vieta (arba vieta, kurioje asmuo turėjo ir galėjo veikti) arba 2) vieta, kurioje atsirado baudžiamojo įstatymo numatyti padariniai. Tradicinis šių normų aiškinimas yra pagrįstas nusikalstamos veikos sudėties skirstymu į formalią ir materialią: formalios nusikalstamos veikos sudėties atveju veikos padarymo vieta yra siejama su veiksmų (neveikimo) vieta; materialios – su BK nustatytų padarinių atsiradimo vieta[43]. Šiuo aspektu aktualu, kad minėtos neteisėto turinio e. veikos yra formalios sudėties, jos dažnai vadinamos „grėsmės" veikomis, ginančiomis abstraktų teisinį gėrį[44], arba „abstraktaus pavojingumo veikomis"[45], kurios teisine prasme neturi aiškių jų sukelto rezultato vietos nustatymo kriterijų. Akcentuotina, kad tokiu atveju mintyje turimi ne padariniai (suprantami BK prasme), o e. veikos padarytas neigiamas *poveikis*[46] tam tikros valstybės teritorijoje. Atsižvelgiant į tai, akivaizdu, kad, nustatant tokios nusikalstamos veikos padarymo vietą, „interpretavimo keblumų neišvengiamai kils ypač tose valstybėse, kuriose nėra specialių nusikalstamų veikų elektroninėje erdvėje jurisdikcijos nustatymo sąlygų"[47]. Minėtos Lietuvos BK nuostatos tiesioginio atsakymo į šį klausimą nesuteikia, todėl neturėtų stebinti tai, kad, esant neaiškiam reglamentavimui, gali skirtis ir praktika nustatant e. veikos padarymo vietą, taip pat sprendimai dėl teritorinio principo taikymo.

Sprendžiant šią problemą, verta apsvarstyti lankstesnio BK 4 straipsnio aiškinimo galimybes, ypač atsižvelgiant į Lietuvos BK įgyvendintų Europos Sąjungos teisės aktų nuostatas. Pavyzdžiui, Direktyvoje 2011/93/ES įtvirtintos plačios baudžiamosios

43 Gintaras Švedas, Armanas Abramavičius, Jonas Prapiestis ir Egidijus Bieliūnas, *Lietuvos baudžiamoji teisė: bendroji dalis: Vilniaus universiteto vadovėlis*. Knyga 1 (Vilnius: Vilniaus universiteto leidykla, 2019), 125; Sud. Jonas Prapiestis, *Lietuvos Respublikos baudžiamojo kodekso komentaras: Bendroji dalis (1–98 straipsniai)* (Vilnius: Teisinės informacijos centras, 2004), 48.

44 Namavičius, *supra note*, 2: 108–109.

45 Sieber, *supra note*, 38: 189.

46 Brenner ir Koops, *supra note*, 33: 15.

47 *Ibid.*

jurisdikcijos ribos, atsižvelgiant į vaikų pornografijos, kitų itin sunkių formų seksualinės prievartos prieš vaikus ir jų seksualinio išnaudojimo atvejų pokyčius dėl naujųjų technologijų ir interneto naudojimo (Preambulės 3 punktas). Ši direktyva įpareigoja užtikrinti jurisdikciją, be kitų, ir tais atvejais, kai nusikalstama veika, susijusi su vaikų pornografija (5 straipsnis) ir ryšių mezgimas su vaikais seksualiniais tikslais (6 straipsnis)[48] „padaromos naudojant informacines ir ryšių technologijas, prieiga prie kurių yra jų teritorijoje, nepaisant to, ar tos technologijos yra jų teritorijoje“ (17 straipsnio 3 dalis). Tai reikštų, kad Lietuva turėtų įgyvendinti baudžiamąją jurisdikciją ir tais atvejais, kai, pavyzdžiui, prieiga prie atitinkamo neteisėto turinio (pavyzdžiui, pornografinio turinio medžiagos, kurioje vaizduojamas vaikas) yra galima jos teritorijoje, net jei informacinės technologijos, kuriose ši medžiaga laikoma (saugoma), yra už jos teritorijos ribų. Įgyvendinus šias direktyvos nuostatas BK, baudžiamojo įstatymo galiojimo erdvėje taisyklės nebuvo keistos, todėl teigtina, kad, įstatymo leidėjo nuomone, esamos normos gali būti pritaikytos ir tokioms situacijoms. Atsižvelgiant į tai, spręstina, ar neturėtų kisti BK 4 straipsnio 2 dalies, nustatančios nusikalstamos veikos padarymo vietą, aiškinimas, kiek tai yra susiję su elektronine erdve ir joje padaromomis atitinkamomis nusikalstamomis veikomis. Pavyzdžiui, pripažinus, kad fizinio asmens ir informacinės sistemos buvimas teritorijoje nėra būtinas, svarstytina, ar asmens veikimo vieta negalėtų būti laikoma ir ta teritorija, į kurią tiesiogiai, naudojantis technologijų galimybėmis, buvo nukreipti kaltininko veiksmai, šioje teritorijoje yra informacijos pasiekimo vieta ir joje buvo padarytas neigiamas poveikis (tai leistų taikyti ir *esminio ryšio kriterijų*). Taip pat diskusijos vertas klausimas, ar e. veikų atitinkamoje teritorijoje sukeliamas „abstraktus pavojus“49 (poveikis) neturėtų būti atskirtas nuo *baudžiamojo įstatymo numatytų padarinių atsiradimo vietos* ir interpretuojamas atskirai. Tačiau tikėtina, kad šis variantas yra galimas tik padarius atitinkamus BK 4 straipsnio 2 ir 3 dalių pakeitimus.

Išvados

1. Nors elektroninei, priešingai nei fizinei, erdvei nebūdingas materialumas, sprendžiant baudžiamosios jurisdikcijos nustatymo problemą e. veikų atveju, pirmumas yra teikiamas teritoriniam baudžiamosios jurisdikcijos principui. Toks požiūris reikalauja identifikuoti kriterijus, kurie leistų nusikalstamą veiką elektroninėje erdvėje susieti su tam tikros valstybės teritorija. Galimybes tam suteikia e. veikų dualumas, reiškiantis, kad asmuo, atlikdamas veiksmus elektroninėje erdvėje, bus tiek elektroninėje, tiek fizinėje erdvėje tuo pačiu metu.

48 Taip pat, jei *modus operandi* leidžia padaryti su seksualine prievarta susijusią nusikalstamą veiką (3 straipsnis), kurstymą, bendrininkavimą ir kėsinimąsi (7 straipsnis) panaudojant informacines technologijas.

49 Sieber, *supra note*, 38: 192, 197.

2. Teritorinė baudžiamoji jurisdikcija gali būti nustatoma, vadovaujantis kriterijais, suformuluotais Europos Sąjungos ir tarptautiniuose teisės aktuose. Atitinkamai nusikalstamos veikos padarymo vieta valstybės teritorijoje gali būti konstatuota, jei joje yra e. veiką padaręs fizinis asmuo arba informacinė sistema, prieš kurią buvo nukreipti nusikalstami veiksmai. Fizinio asmens ir informacinės sistemos buvimo vieta gali nesutapti, tačiau valstybė gali įgyvendinti savo teritorinę baudžiamąją jurisdikciją, jei bent vienas jų e. veikos padarymo metu buvo tos valstybės teritorijoje.
3. Atsižvelgiant į įvairius komunikavimo elektroninėje erdvėje variantus ir sprendžiant dėl valstybės teritorinės baudžiamosios jurisdikcijos, suformuluotas ir esminio ryšio su valstybės teritorija kriterijus. Įvertinus įvairius objektyvius ir subjektyvius požymius bei nustačius e. veikos glaudų, aiškiai susietą ryšį su valstybės teritorija, darytina išvada, kad ši valstybė gali įgyvendinti savo teritorinę baudžiamąją jurisdikciją dėl minėtos e. veikos padarymo.

CYBERCRIME AND TERRITORIAL CRIMINAL JURISDICTION

Renata Marcinauskaitė
Mykolas Romeris University, Lithuania

Summary. *This article examines the application problems of the principle of territorial criminal jurisdiction and related aspects of the determination of the place of commission of a criminal offense in cyberspace. Attention is drawn to the fact that the provision established in Article 4 (2) of the Criminal Code of the Republic of Lithuania (hereinafter – the CC), that the place of commission of a criminal act shall be the place in which a person acted (or ought to have acted or could have acted) or the place in which the consequences provided for by a criminal law occurred, is applied in determining the place of commission of the act not only in terms of physical location but also in cyberspace. Considering the peculiarities of cyberspace, this article discusses the criteria that could link cybercrime to the territory of physical space. The European Union and international legal acts, the provisions of which Lithuania has implemented in the CC, are also used for this analysis.*

This article discusses the criteria of the location of a natural person and the location of an information system, and provides explanations as to why such criteria have been chosen to link cybercrime to physical space. Considerable attention is also paid to the criterion of an essential link with the territory of the state. This article concludes that the provisions of the CC establishing the principle of territorial criminal jurisdiction should be harmonized with the changed understanding of the place of commission of a criminal offense in cyberspace.

Keywords: *cybercrime, criminal jurisdiction, territorial principle, information system, substantial link criteria.*

Renata Marcinauskaitė, Mykolo Romerio universiteto Teisės mokyklos Baudžiamosios teisės ir proceso instituto docentė, daktarė. Mokslinių tyrimų kryptys: nusikalstamos veikos elektroninėje erdvėje, jurisdikcija.

Renata Marcinauskaitė, doctor of social sciences, associate professor at the Institute of Criminal Law and Procedure at the Law School at Mykolas Romeris University. Research interests: cybercrime, jurisdiction.