Renata Marcinauskaitė

NUSIKALSTAMOS VEIKOS ELEKTRONINĖJE ERDVĖJE

MRU
MYKOLO ROMERIO UNIVERSITETAS

NUSIKALSTAMOS VEIKOS ELEKTRONINĖJE ERDVĖJE

MYKOLO ROMERIO
UNIVERSITETAS

RENATA MARCINAUSKAITĖ

NUSIKALSTAMOS VEIKOS ELEKTRONINĖJE ERDVĖJE

Elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje

Monografija

VALSTYBĖS ĮMONĖ
REGISTRŲ CENTRAS
Vilnius, 2019

Recenzavo:

Prof. dr. Armanas Abramavičius,
Vilniaus universiteto Teisės fakulteto Baudžiamosios justicijos katedra

Prof. dr. Rima Ažubalytė,
Mykolo Romerio universiteto Mykolo Romerio teisės mokyklos
Baudžiamosios teisės ir proceso institutas

Prof. dr. Olegas Fedosiukas,
Mykolo Romerio universiteto Mykolo Romerio teisės mokyklos
Baudžiamosios teisės ir proceso institutas

Prof. dr. Jonas Prapiestis,
Vilniaus universiteto Teisės fakulteto Baudžiamosios justicijos katedra

Rekomendavo spausdinti:

Mykolo Romerio universiteto Mykolo Romerio teisės mokyklos Baudžiamosios teisės ir proceso institutas (2018 m. lapkričio 15 d. susirinkimo protokolas Nr. 1BTPI-3)

Mykolo Romerio universiteto Mykolo Romerio teisės mokyklos taryba
(2018 m. lapkričio 26 d. nutarimas Nr. 1T-5)

Mykolo Romerio universiteto Mokslinių–mokomųjų leidinių aprobavimo leidybai komisija (2018 m. gruodžio 11 d. posėdžio protokolas Nr. 2L-25)

Leidinio bibliografinė informacija pateikiama
Lietuvos nacionalinės Martyno Mažvydo bibliotekos
Nacionalinės bibliografijos duomenų banke (NBDB).

ISBN 978-9955-30-281-0 (internete)
ISBN 978-9955-30-282-7 (spausdintas)

Turinys

PRATARMĖ

Besivystančių technologijų ir nusikalstamų veikų padarymo pokyčių sąsaja baudžiamojoje teisėje neturėtų nieko stebinti. Iš tiesų ji ne tiek stebina, kiek verčia susimąstyti apie tas problemas, su kuriomis susiduriama šioje teisės šakoje, pakitus nusikalstamų veikų padarymo galimybėms. Kaip elektroninė erdvė keičia tradicinių nusikalstamų veikų padarymą ir kiek šie pokyčiai turi įtakos aiškinant tokių veikų sudėties požymius ar jas kvalifikuojant, kaip suvokti fizinei erdvei apskritai nebūdingas nusikalstamo elgesio apraiškas – tai tik keletas bendresnių klausimų, galinčių kilti nagrinėjant nusikalstamų veikų elektroninėje erdvėje baudžiamąsias bylas. Be kita ko, minėtųjų teisinio vertinimo problemų kyla dėl to, kad dauguma baudžiamojo įstatymo normų tradiciškai buvo kurtos fizinėje erdvėje padarytoms nusikalstamoms veikoms kvalifikuoti, todėl vis dar įprasta ieškoti materialumo, fizinių parametrų, apčiuopiamumo, buvimo čia ir dabar požymių. Natūralu ir tai, kad siekiant geriau suprasti elektroninę erdvę, joje padaromų nusikalstamų veikų atitikmenų (kartais gal tik abstrakčių ir metaforiškų) bandoma rasti būtent pažinioje fizinėje erdvėje, tarsi kuriant aliuziją į ją.

Atsižvelgiant į technologijų plėtros perspektyvas reikėtų pripažinti, kad fizinės ir elektroninės erdvės atskyrimas daugelyje sričių vis dėlto yra gana sąlyginis. Tikėtina, kad šių erdvių riba ims sparčiai nykti vis daugiau žmogaus gyvenimo sričių ir veiklos rūšių perkeliant į elektroninę erdvę. Rašant monografiją omenyje turėta tai, kad tokia technologijų plėtra – neišvengiama, todėl stengtasi pateikti interpretacijų, kiek įmanoma labiau pritaikytų prie technologijų pokyčių. Ar tai pavyko padaryti, bus galima įvertinti tik bėgant laikui ir stebint, kaip technologijos keičia mūsų erdvės ir laiko sampratą, kaip elektroninė erdvė tampa priimtina egzistuoti. Antai dar 1984 metais romane „Neuromancer“ Williamas Gibsonas vaizdingai rašė: „Dangus virš uosto buvo kaip televizoriaus, perjungto į nebeveikiantį kanalą, ekranas.“

Monografijoje pateikiama tam tikrų elektroninėje erdvėje galimų nusikalstamų veikų aiškinimo ir inkriminavimo problemų sprendimo variantų, todėl ji galės būti naudinga besiformuojančiai šių nusikalstamų veikų doktrinai, be to, padėti praktikoje sprendžiant įvairias tokių nusikalstamų veikų aiškinimo ir kvalifikavimo problemas. Autorė tikisi, kad

atliktas tyrimas paskatins tolesnes diskusijas nusikalstamų veikų elektroninėje erdvėje tema ir apskritai bus įdomus visiems, kuriems rūpi įvairiausi elektroninės erdvės saugumo aspektai.

Dr. Renata Marcinauskaitė

Įvadas

„Elektroninė erdvė. Visų šalių sutarimu priimta kasdien patiriama haliucinacija <...>. Neįsivaizduojamas sudėtingumas.“

Williamas Gibsonas

Plačiausia prasme suvokiamų kompiuterinių informacinių technologijų raida sudarė prielaidas didelės apimties duomenų sklaidai, naujiems prieigos prie duomenų būdams atsirasti; išplėtė šių technologijų funkcionavimo ir taikymo galimybes; privertė įdėmiau pažvelgti į globaliosios transformacijos aspektus bandant nuspėti galimas tokios plėtros perspektyvas. Šie technologiškai ir teisiškai sudėtingi procesai yra susiję ne tik su teigiama elektroninės erdvės vartotojų (ar procesų) sąsaja bei sąveika, bet ir su informacinės visuomenės pažeidžiamumo problemomis. Elektroninėje erdvėje, savo parametrais nors ir nutolusioje nuo fizinės, neišvengiama įvairių grėsmių teisinėms vertybėms, taip pat ir iš esmės naujų arba dėl informacinių technologijų taikymo pakitusių nusikalstamų veikų. Monografijoje yra tiriama viena iš Lietuvos Respublikos baudžiamojo kodekso[1] (toliau – ir BK, 2000 m. BK, baudžiamasis įstatymas) XXX skyriuje įtvirtintų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui rūšių – nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui, taip pat jų baudžiamojo teisinio vertinimo problemos. Neteisėto elektroninių duomenų perėmimo ir panaudojimo (BK 198 straipsnis) ir neteisėto prisijungimo prie informacinės sistemos (BK 198[1] straipsnis) veikos atskiriamos sustruktūrinus BK XXX skyriuje numatytas nusikalstamas veikas: taikant *CIA triadą* į jas žiūrima kaip į konfidencialumo, integralumo ir prieinamumo pažeidimus.

Dėl informacinių technologijų ir nusikalstamų veikų padarymo galimybių sąveikos kaskart kyla kiekybiškai daug ir kokybiškai naujų baudžiamosios teisės problemų, saugant įvairius teisinius gėrius: egzistuojančius tik elektroninėje erdvėje ar kitus, į elektroninę erdvę perkeltus iš fizinės erdvės. Naujo pobūdžio diskusinių klausimų

[1] Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios*, 2000, Nr. 89-2741.

gausa lėmė, kad tiriant pasirinktų nusikalstamų veikų problematiką neapsiribota vien jų sudėties požymių analize, esamo teisinio reguliavimo trūkumų nustatymu ir tuo pagrįstu šių veikų požymių aiškinimo krypčių formulavimu – į elektroninių duomenų ir informacinių sistemų konfidencialumo pažeidimus iš baudžiamosios teisės pozicijų siekiama žvelgti plačiau. Monografijoje stengiamasi ieškoti tokio pobūdžio nusikalstamų veikų ištakų, jų sisteminimo galimybių, kriminalizavimo pateisinimo, atskyrimo nuo kitų panašių nusikalstamų veikų kriterijų. Be to, kuriant principines šių veikų aiškinimo pozicijas ne kartą buvo keliami technologijų ir joms baudžiamajame įstatyme įvardyti vartojamos terminologijos derinimo klausimai. Monografijoje minėtąsias problemas stengiamasi analizuoti technologiškai neutraliu požiūriu – atsisakius technologijų specifiškumo siekiama, kad galimi baudžiamųjų teisinių problemų sprendimo būdai būtų pritaikomi ir dabartinėms, ir ateities technologijoms (kiek tai įmanoma padaryti dėl technologijų plėtros prognozavimo sunkumų).

Sąlygos nacionaliniu lygiu analizuoti nusikalstamas veikas, pažeidžiančias elektroninių duomenų ir informacinių sistemų konfidencialumą, buvo sudarytos įsigaliojus 2000 m. BK, kuriame dėl technologijų pokyčių atsiradusios naujos veikos kriminalizuotos *sui generis* ir nebelaikomos kitų veikų sudedamąja dalimi. Dėl tokių nusikalstamų veikų įtvirtinimo kilo teisėkūros ir baudžiamojo įstatymo normų taikymo (atitinkamai ir jų aiškinimo) problemų. Beje, minėtosios problemos ir jų sprendimo būdai iki šiol išlieka aktualūs, ypač dėl to, kad išsamių diskusijų dėl nustatyto teisinio reguliavimo ir jo tinkamumo Lietuvoje beveik nekyla. Be to, nuo 2000 m. baudžiamojo įstatymo įsigaliojimo praėjęs laikas yra daugiau nei pakankamas tirti ir nustatyto teisinio reguliavimo veiksmingumą, aiškintis, ar iš tiesų atsakomybę už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų konfidencialumui nustatančios normos yra tinkamos ir suprantamos, ar jas taikant buvo pasiekti norimi tikslai bei koks yra realus jų taikymo rezultatas.

Ši monografija – tai disertacinio autorės tyrimo[2] tęsinys, atnaujintas pagal naujausius baudžiamojo įstatymo pakeitimus ir besifor-

[2] Marcinauskaitė, R. Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1] straipsniai): daktaro disertacija, Vilnius: Mykolo Romerio universitetas, 2014.

muojančią teismų praktiką, be to, jame identifikuotos naujai kylančios problemos ir pateikta galimų jų sprendimo būdų. Monografijoje taip pat nagrinėjamos nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui: atskleisti Lietuvos baudžiamosios teisės doktrinoje dar nenagrinėti šių veikų sudėties požymių aspektai, pateikta nuomonė dėl technologinių ir teisinių problemų įtakos aiškinant ir inkriminuojant veikas, sistemiškai analizuojamos tarptautiniu ir Europos Sąjungos lygiu priimtų teisės aktų, užsienio valstybių bei Lietuvos baudžiamojo įstatymo normos. Atsižvelgiant į minėtųjų nusikalstamų veikų sudėties požymių analizę, suformuluoti nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atskyrimo nuo panašių nusikalstamų veikų kriterijai. Be to, atkreiptas dėmesys į technologinio neutralumo ir ekvivalentinio vertinimo principų taikymo baudžiamojoje teisėje galimybes bei kliūtis. Atliekant tyrimą nebuvo apsiribota tik teoriniu lygmeniu – šių nusikalstamų veikų analizei taikyta teismų praktika, ją apibendrinus iškeltos konkrečios minėtųjų veikų kvalifikavimo problemos ir pateikta jų sprendimo variantų. Be to, knygoje remiamasi ir reikšminga užsienio valstybių teismų praktika – nagrinėtos bylos padėjo nustatyti Lietuvoje dar nepasitaikiusius probleminius nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui aspektus.

Lietuvoje nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui nebuvo plačiai nagrinėtos, beveik neanalizuoti ir šių nusikalstamų veikų sudėties požymiai. Bendrąja veikų elektroninėje erdvėje tematika ir galiojant 1961 m., ir įsigaliojus 2000 m. BK domėjosi D. Štitilis. Šio mokslininko 2002 metais apgintoje disertacijoje „Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos“ ir vėlesniuose jo darbuose nemažai dėmesio skiriama bendriesiems tokių veikų aiškinimo klausimams. Atskirais aspektais minėtąsias veikas, dar galiojant 1961 metų baudžiamajam įstatymui, nagrinėjo ir R. Petrauskas. Įsigaliojus 2000 metų BK, kai kurių nusikalstamų veikų elektroninėje erdvėje aiškinimo atvejų neretai pasitaiko mokomuosiuose leidiniuose, pavyzdžiui, 2016 metų vadovėlyje „Interneto ir technologijų teisė“[3],

[3] Štitilis, D.; Kiškis, M.; Limba, T., *et al.* Interneto ir technologijų teisė: vadovėlis. Vilnius: Registrų centras, 2016.

2006 metų vadovėlyje „Teisės informatika ir informatikos teisė“[4] bei 2004 metų leidinyje „Informacinių technologijų teisė“[5]. Apie baudžiamojo įstatymo ir tarptautinių teisės aktų suderinamumą elektroninių nusikalstamų veikų reglamentavimo srityje savo nuomonę yra pareiškęs ir D. Sauliūnas. Kai kurie šių veikų aspektai, remiantis jų tyrimo metodika, aptariami N. Goranino ir D. Mažeikos. Minėtinas ir baudžiamojo įstatymo komentaras, kuriame pateikiamas glaustas teorinis elektroninių duomenų ir informacinių sistemų konfidencialumą pažeidžiančių veikų aiškinimas. Pastaruoju metu mokslinėje literatūroje daugiau dėmesio skiriama tapatybės vagystės (angl. *identity theft)* elektroninėje erdvėje kriminalizavimo klausimams, kuriais domisi D. Štitilis, P. Pakutinskas, M. Laurinaitis ir I. Dauparaitė.

Užsienio valstybių baudžiamosios teisės moksle daug dėmesio skiriama įvairiems nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui bei apskritai nusikalstamų veikų elektroninėje erdvėje aspektams. Bendrojo pobūdžio elektroninių veikų kriminalizavimo ir aiškinimo, elgesio elektroninėje erdvėje vertinimo problemas savo darbuose nagrinėjo J. Cloughas, I. Waldenas, C. Reedas, U. Kohl, S. W. Brenner, M. Schellekensas, R. Ali, I. M. van der Haar, J. B. Koopsas, R. W. Downingas, P. Ohmas, C. A. Kirby ir kt. Neteisėtos prieigos prie informacinės sistemos ar elektroninių duomenų kriminalizavimo, inkriminavimo ir tokių nusikalstamų veikų požymių aiškinimo klausimais savo nuomonę yra pareiškę O. S. Kerris, M. W. S. Wong, M. J. Madisonas, I. Waldenas, D. Bainbridge’as, J. Angelas, G. Thorntonas, J. Cloughas, B. A. Howell, A. S. Blunnas, D. Rowland, E. Macdonald. Dar minėtini ir Rusijos baudžiamosios teisės mokslininkai: N. I. Vetrovas, V. A. Mazurovas, A. V. Naumovas, A. G. Volevodzas, V. E. Kozlovas, O. Ja. Baevas ir V. A. Meshherkovas, S. A. Pashinas ir kt.

Monografijoje aiškinant nusikalstamas veikas elektroninių duomenų ir informacinių sistemų konfidencialumui plačiausiai taikomi analizės ir sintezės metodai. Remiantis *analizės metodu,* šių veikų struktūra skirstoma dalimis ir aiškinami atskiri objektyvieji bei

[4] Kiškis, M., *et al*. Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006.

[5] Civilka, M., *et al*. Informacinių technologijų teisė. Vilnius: NVO teisės institutas, 2004.

subjektyvieji jų požymiai. Be to, šis metodas leido atskleisti atskirų požymių, tiesiogiai susijusių su informacinėmis technologijomis, turinį: atskyrus teisinius ir technologinius požymių aspektus buvo sprendžiamas jų suderinamumo klausimas. Siekiant visapusiškai įvertinti veikas, neapsieita be *sintezės metodo*, padėjusio analizės metu dėl atskirų požymių gautas įžvalgas susieti į visumą, kuri ir suteikė sąlygas nustatyti, kokia minėtųjų veikų koncepcija buvo vadovaujamasi jas apibrėžiant baudžiamajame įstatyme ir kokios yra šių nusikalstamų veikų ribos.

Monografijoje buvo taikomas ir *sisteminės analizės metodas*, pasirinktas dėl nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui specifikos: įvairių šių veikų aspektų pasitaiko tarptautiniu ir Europos Sąjungos (toliau – ES) lygiu priimtuose teisės aktuose, be to, aiškinant šias veikas būtina sieti skirtingose mokslo šakose suformuluotas teorijas. Minėtasis metodas leido nustatyti nagrinėjamų nusikalstamų veikų vietą elektroninių nusikalstamų veikų ir nusikalstamų veikų elektroninių duomenų bei informacinių sistemų saugumui visumoje. Jį taikant buvo sprendžiamos kompleksinės, su technologijomis susijusios problemos, turinčios tiesioginį ryšį su keliamu technologijų ir terminologijos klausimu. Sisteminės analizės metodas suteikė galimybę analizuoti veikų sudėties požymių tarpusavio ryšį, atskleisti šių veikų santykį su panašiomis baudžiamajame įstatyme nurodytomis veikomis ir ieškoti jų atskyrimo kriterijų.

Dėl nagrinėjamų problemų kompleksiškumo kilo būtinybė monografijoje tarpusavyje susieti baudžiamosios teisės ir informacinių technologijų sritis. Siekiant atskleisti technologinį ir teisinį nusikalstamų veikų aspektą, buvo taikomas *apibendrinimo metodas*. Nustatyti bendriausi (esminiai) technologijų srityje analizuojamų objektų požymiai buvo derinami su baudžiamaisiais teisiniais sudėties požymių aspektais. Taip atliekant tyrimą buvo sprendžiama technologijų ir joms įvardyti vartojamos terminologijos pritaikomumo baudžiamajai teisei problema, pateikiamas su technologijomis susijusių požymių aiškinimas.

Nebūtų suklysta teigiant, kad šiuo metu esančio nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui reglamentavimo ištakos yra siejamos su tarptautiniais ir ES teisės aktais, skirtais kovoti su minėtosiomis veikomis elektroninėje erdvėje.

Šie teisės aktai padarė įtaką ne tik Lietuvos, bet ir užsienio valstybių baudžiamųjų įstatymų nuostatoms. Pasirinktas skirtingas minėtųjų teisės aktų nuostatų įgyvendinimo būdas leidžia formuotis ir skirtingoms tokio pobūdžio veikų koncepcijoms. Tokiems skirtumams nustatyti ir analizuoti pasirinktas *lyginamasis metodas* leido gretinti skirtingas veikų koncepcijas, įvairių mokslininkų nuomones, aptikti veikų inkriminavimo problemas ir rasti galimus jų sprendimo būdus bei pan.

Atskleidžiant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui požymių turinį buvo taikomas ir *lingvistinis metodas*. Monografijoje nustatytas įvairių sąvokų interpretavimo trūkumas, todėl šis metodas tapo aktualus bandant nustatyti galimas jų aiškinimo kryptis. Kita vertus, taikant lingvistinį metodą buvo pastebėta, kad vartojamoms baudžiamosios teisės sąvokoms yra būdingas specifinis, nuo šnekamosios kalbos nutolęs turinys, kuris tampa dar savitesnis informacinių technologijų aplinkoje.

Monografijai būdingas ir empirinis *dokumentų analizės metodas*. Jis buvo taikomas apibendrinant besiklostančią teismų praktiką nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui bylose, vadovaujantis teismų sprendimais iškeliant veikų inkriminavimo problemas ir pagrindžiant galimus jų sprendimo būdus. Knygoje remiamasi daugiau kaip septyniasdešimčia Lietuvos teismų sprendimų, kurie buvo atrinkti atsižvelgiant į juose pateiktų išaiškinimų svarbą probleminiams nagrinėjamų nusikalstamų veikų aspektams atskleisti. Be to, analizuojami ir reikšmingiausi užsienio valstybių teismų sprendimai, kuriais remiantis nustatomos naujos, Lietuvoje dar nežinomos problemos ir pateikiama jų sprendimo siūlymų.

Monografiją sudaro keturi skyriai. I skyriuje „Nusikalstamų veikų elektroninėje erdvėje kriminalizavimas, sisteminimas ir aiškinimas“ pateikiami bendrieji elektroninėje erdvėje padaromų nusikalstamų veikų aspektai, susiję su pažeidžiamos baudžiamojo įstatymo saugomos vertybės paieška, ekvivalentinio vertinimo ir technologinio neutralumo principų taikymo galimybėmis bei problemomis baudžiamojoje teisėje.

II skyriuje „Neteisėtas prisijungimas prie informacinės sistemos (BK 198[1] straipsnis)“ atskleidžiami šios informacinės sistemos konfidencialumą pažeidžiančios nusikalstamos veikos sudėties objektyvieji

ir subjektyvieji požymiai, aptariamos galimos tokios veikos teisinio vertinimo kryptys.

III skyriuje „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas (BK 198 straipsnis)“ analizuojami neviešų elektroninių duomenų konfidencialumą pažeidžiančios nusikalstamos veikos sudėties požymiai, pateikiama nuomonė dėl šios nuskalstamos veikos kriminalizavimo apimties ir iš to kylančių jos aiškinimo bei inkriminavimo problemų.

IV skyriuje „Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui atskyrimas nuo panašių nusikalstamų veikų“ formuluojami monografijoje tiriamų nusikalstamų veikų ir nusikalstamų veikų finansų sistemai (BK 214, 215 straipsniai) bei privataus gyvenimo neliečiamumui (BK 166 straipsnis) atskyrimo kriterijai.

Technologijos atskleidžia, pertvarko pasaulį, nuolat projektuodamos ir sukurdamos naujas realybes šiame procese. Jos linkusios pasufleruoti originalias idėjas, formuoti naujas koncepcijas ir kelti beprecedentes problemas.

Luciano Floridi

I SKYRIUS

NUSIKALSTAMŲ VEIKŲ ELEKTRONINĖJE ERDVĖJE KRIMINALIZAVIMAS, SISTEMINIMAS IR AIŠKINIMAS

I SKYRIAUS TURINYS

Informacinių technologijų raida, be teigiamų pokyčių, turėjo įtakos ir nusikalstamų veikų atsiradimui – dėl technologijų taikymo pakito tradicinės veikos, o elektroninėje erdvėje atsirado specifinių, fizinei erdvei nebūdingų nusikalstamų veikų. Dėl šių gana reikšmingų nusikalstamų veikų padarymo galimybių pokyčių kilo nemažai jų kriminalizavimo, sisteminimo, o vėliau ir aiškinimo problemų. Siekiant spręsti šias problemas, teisėkūroje pradėti taikyti elgesio fizinėje ir elektroninėje erdvėje ekvivalentinio (lygiaverčio) vertinimo (angl. *principle of equivalence, principle of online and offline equivalence)* bei technologinio neutralumo (angl. *principle of technological neutrality)* principai. Jie yra aktualūs ir teismų praktikoje, nes padeda atskleisti su technologijomis susijusios teisės normos turinį ir ją tiksliai bei vienodai taikyti. Minėtųjų principų ištakos nėra tiesiogiai susijusios su baudžiamąja teise[6], bet taikant baudžiamąją atsakomybę už nusikalstamas veikas, padarytas elektroninėje erdvėje, jie yra tokie pat svarbūs ir šioje srityje. Ieškant iš šių principų kylančių reikalavimų įgyvendinimo galimybių aktualu ir tai, kad jie *a priori* neturi baudžiamosios teisės specifikos nulemtų apribojimų, todėl ne mažiau yra svarbu nustatyti jų taikymo ribas.

Kriminalizuojant šias veikas, kilo ir jų sisteminimo bei grupavimo klausimų, kurie baudžiamosios teisės srityje dažniausiai sprendžiami ieškant bendros tokiomis veikomis pažeidžiamos baudžiamojo įstatymo saugomos vertybės.

---

[6] Technologinio neutralumo principas gali būti kildinamas iš informacinių technologijų reguliavimo, o ekvivalentinio vertinimo principas pradėtas taikyti visose srityse, kur būtina spręsti kilusias kokybiškai naujas elektroninės erdvės teisinio reguliavimo problemas (pavyzdžiui, autorių teisių ir gretutinių teisių apsauga elektroninėje erdvėje, elektroninių pinigų, elektroninio parašo pripažinimo ir naudojimo galimybės).

1. Nusikalstamų veikų elektroninėje erdvėje sisteminimas ir baudžiamojo įstatymo saugomos vertybės paieška

1.1. Nuo nusikalstamų veikų informatikai iki nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui

Baudžiamojo įstatymo saugomos vertybės, kaip vieno iš pagrindinių nusikalstamos veikos sudėties objektyviųjų požymių, funkcijos yra įvairios – vertybė yra svarbi ne tik taikant baudžiamąjį įstatymą, bet ir teisėkūrai. Teisėkūros metu panašios nusikalstamos veikos, remiantis baudžiamojo įstatymo saugomo teisinio gėrio pagrindu, yra sisteminamos į atskiras rūšis (grupes). Kita vertus, nustatyti baudžiamojo įstatymo saugomą vertybę nusikalstamų veikų elektroninėje erdvėje atveju yra sudėtinga dėl to, kad tokia atskira nusikalstamų veikų rūšis baudžiamajame įstatyme tiesiog nenumatoma. Šios veikos yra gana įvairios – bendriausia prasme tai ne tik nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui (BK XXX skyrius), bet ir visos tradicinės nusikalstamos veikos, kurios pakito dėl informacinių technologijų taikymo. Pastarajai grupei priskiriamos ir tradicinės nusikalstamos veikos, kurios pagal savo pobūdį gali būti padaromos ne tik fizinėje, bet ir elektroninėje erdvėje. Baudžiamajame įstatyme jos yra priskiriamos skirtingoms nusikalstamų veikų rūšims, pavyzdžiui, sukčiavimas elektroninėje erdvėje (BK 182 straipsnis) laikomas nusikalstama veika nuosavybei, turtinėms teisėms ir turtiniams interesams (BK XXVIII skyrius), elektroninio dokumento suklastojimas ar disponavimas suklastotu dokumentu (BK 300 straipsnis) yra nusikalstama veika valdymo tvarkai, susijusi su dokumentų ar matavimo priemonių klastojimu (BK XLIII skyrius), o disponavimas pornografinio turinio dalykais elektroninėje erdvėje (BK 309 straipsnis) – nusikalstama veika dorovei (BK XLIV skyrius). Vadinasi, baudžiamajame įstatyme nėra tiesiogiai įtvirtinta ta baudžiamojo įstatymo saugoma vertybė, kuri leistų į vieną visumą susieti visas elektroninėje erdvėje daromas nusikalstamas veikas – ir tas, kuriomis pažeidžiamas elektroninių duomenų ar informacinių sistemų saugumas (ar jam ke-

liama grėsmė), ir įvairias elektroninėje erdvėje padaromas tradicines nusikalstamas veikas.

Atsižvelgiant į nusikalstamų veikų elektroninėje erdvėje vidinę struktūrą matyti, kad nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui sudaro tik dalį visų elektroninėje erdvėje padaromų nusikalstamų veikų. Jas nuo kitų veikų leidžia atskirti būtent BK XXX skyriaus pavadinime nurodyta rūšinė baudžiamojo įstatymo saugoma vertybė – elektroninių duomenų ir informacinių sistemų saugumas. Šios vertybės tinkamo nustatymo ir aiškinimo svarba pabrėžiama ne atsitiktinai. Galiojant 1961 m. BK, nusikalstamos veikos elektroninių duomenų ir informacinių sistemų saugumui kaip atskira nusikalstamų veikų rūšis nebuvo kriminalizuotos, todėl baudžiamojo įstatymo saugomos vertybės, kuriai šiomis veikomis būtų padaroma žalos (arba keliama tokios žalos atsiradimo grėsmė), įvairūs įvardijimo aspektai Lietuvos baudžiamosios teisės doktrinoje tuo metu dar nebuvo nagrinėjami. Pirmųjų teisinio gėrio nustatymo nacionaliniu lygiu problemų kilo šias nusikalstamas veikas kaip atskirą rūšį įtvirtinus 2000 m. BK ir jas laikant nebe sudėtine kitų veikų dalimi, o atskirą baudžiamąją teisinę reikšmę turinčiomis veikomis. Tinkamos baudžiamojo įstatymo saugomos vertybės, leidžiančios atskleisti tokių nusikalstamų veikų esmę ir atskirti jas kaip tam tikrą rūšį, parinkimas sukėlė nemažai sunkumų – bet kokie jos formulavimo bandymai neturėjo tvirto teorinio pagrindimo. Nemažai kritikos tuo metu buvo pareikšta ne tik dėl šių nusikalstamų veikų aprašymo BK (per trumpo jų sąrašo, numatytų nusikalstamų veikų sudėties požymių neišsamumo ir kt.), bet ir dėl pačios baudžiamojo įstatymo saugomos vertybės formuluotės. Pirminis 2000 m. BK XXX skyriaus pavadinimas, kuriame buvo pateikiamas oficialus vertybės variantas, buvo *Nusikaltimai informatikai*. Toks pasirinkimas ne veltui buvo kritikuojamas mokslinėje literatūroje[7]. Iš tikrųjų *informatika* gali būti apibūdinama labai įvairiai[8], bet bendriausia prasme ji visada bus laikoma mokslo šaka,

[7] Civilka, M., *et al*. Informacinių technologijų teisė. Vilnius: NVO teisės institutas, 2004, p. 528. Goranin, N.; Mažeika, D. Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos: mokomoji knyga. Kaunas: TEV [i.e. Technologija], 2011, p. 23.

[8] Pavyzdžiui, informatika „tai integracinė mokslo šaka, tirianti visų rūšių informacijos tvarkymą (rinkimą, registravimą, apdorojimą ir kt.) ir panaudojimą, taikant kompiuterius ir kitas technines priemones informacijos vartotojų poreikiams kuo geriau tenkinti, įvairioms sistemoms valdyti“ (Domeika, P. Apskaitos informacinė sistema. Kaunas:

nagrinėjančia informaciją, jos kūrimą ir apdorojimą bei šiuos procesus atliekančias sistemas. Akivaizdu, kad dėl informacinių technologijų plėtros atsiradusiomis nusikalstamomis veikomis negali būti kėsinamasi į informatiką kaip mokslą, todėl šiuos BK numatytos vertybės netikslumus siūlyta šalinti *informatikos* terminą aiškinant plačiąja prasme. Taip jis būtų interpretuojamas kaip su informatikos mokslu susijusi praktinė veikla, o vertybė suvokiama kaip „netrukdomas, nekliudomas, neslopinamas automatinis ir paprastas informacijos apdorojimas ir (ar) nekliudomas informacinės sistemos valdymas ir kontrolė“[9]. Nors sprendimas vertybę aiškinti plačiau iš dalies padėjo spręsti šio objektyviojo sudėties požymio netikslumo problemą, bet nepaslėpė jo trūkumų. Šiuo laikotarpiu, be kitų bandymų aiškinimu koreguoti vertybės požymį, siekiant išvengti dviprasmybių teisinį gėrį dar siūlyta įvardyti kaip *kompiuterinės informacijos saugumą*[10].

Visi vėlesni BK XXX skyriaus nusikalstamų veikų sudėčių keitimai buvo susiję su tarptautiniais Lietuvos įsipareigojimais ratifikavus Konvenciją dėl elektroninių nusikaltimų ir ES lygiu priėmus Europos Sąjungos Tarybos 2005 m. vasario 24 d. pagrindų sprendimą 2005/222/TVR dėl atakų prieš informacines sistemas[11] (toliau – ir Tarybos pamatinis sprendimas 2005/222/TVR) bei vėliau jį pakeičiančią Europos Parlamento ir Tarybos direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (toliau – ir Direktyva 2013/40/ES)[12].

Spalvų kraitė, 2008, p. 13); „Mokslo ir technikos sritis, nagrinėjanti informacijos kaupimo, perdavimo ir apdorojimo dėsningumus, metodus ir technines priemones“ (Jonušauskas, S.; Bilevičienė, T.; Kažemikaitis, V. Įvadas į informatiką. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002, p. 5); „Mokslas apie informaciją ir informacinius procesus“ (Kompiuterija. Burgis, B.; Kulikauskas, A. (red.). Kaunas: Naujasis lankas, 2000, p. 13); „Mokslo ir technikos sritis, nagrinėjanti informacijos kaupimo, perdavimo ir apdorojimo dėsningumus, metodus ir technines priemones“ (Žilinskas, A.; Leonavičius, G.; Valavičius, E. Informatika. Vilnius: Aldorija, 2000, p. 5) ir kt.

[9] Civilka, M., *et al*. Informacinių technologijų teisė. Vilnius: NVO teisės institutas, 2004, p. 529.

[10] *Ibidem*.

[11] Europos Sąjungos Tarybos 2005 m. vasario 24 d. pagrindų sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas [2005] OL L 69/67.

[12] Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR [2013] OL L 218/8.

Konvencijos dėl elektroninių nusikaltimų preambulėje ir II skyriaus 1 skirsnio 1 dalyje, įtvirtinančioje įvairias su materialiąja baudžiamąja teise susijusias nuostatas, buvo pateiktas tikslesnis baudžiamojo įstatymo saugomos vertybės pavadinimas – *kompiuterinių duomenų ir sistemų konfidencialumas, vientisumas ir prieinamumas*, bet šiuo požiūriu baudžiamojo įstatymo nuostatos 2004 metų pakeitimais nebuvo koreguotos[13]. Netinkama teisinio gėrio formuluotė pakeista tik 2007 metais[14], kai į nacionalinę teisę buvo perkeltos Tarybos pamatinio sprendimo 2005/222/TVR nuostatos ir su jomis suderinti įvairūs baudžiamosios atsakomybės už BK XXX skyriuje numatytų nusikalstamų veikų padarymą aspektai. Pertvarkius BK XXX skyriuje įtvirtintas nusikalstamų veikų apibrėžtis, kartu pakeistas ir šias veikas į atskirą rūšį susiejančios vertybės pavadinimas, suformuluojant kur kas tikslesnį jos pavadinimą – *elektroninių duomenų ir informacinių sistemų saugumas*. Ši vertybė liko nepakitusi ir 2015 metais BK įgyvendinus Direktyvos 2013/40/ES nuostatas. Būtent šis teisinis gėris leidžia aiškiau suvokti BK XXX skyriuje esančių nusikalstamų veikų ištakas, jų vidinę struktūrą ir suteikia galimybę kalbėti apie įvairius elektroninių duomenų ir informacinių sistemų saugumo pažeidimų aspektus. Tokia baudžiamojo įstatymo saugoma vertybė yra artimesnė ir Konvencijoje dėl elektroninių nusikaltimų minimai kompiuterinių duomenų ir sistemų konfidencialumo, vientisumo ir prieinamumo triadai (II skyriaus 1 skirsnio 1 dalies pavadinimas).

Be abejo, toks požiūris į baudžiamojo įstatymo saugomą vertybę nėra vienintelis, jų įvairovė ypač atsiskleidžia analizuojant užsienio valstybių baudžiamuosius įstatymus. Pavyzdžiui, Vokietijos baudžiamajame įstatyme[15] kai kurios veikos, siejamos su elektroninių

---

[13] Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo 198^1 ir 198^2 straipsniais įstatymas. *Valstybės žinios*, 2004, Nr. 25-760.

[14] Lietuvos Respublikos baudžiamojo kodekso 7, 38, 47, 63, 66, 70, 75, 82, 93, 129, 166, 167, 172, 178, 180, 181, 182, 183, 184, 185, 189, 194, 196, 197, 198, 198^1, 198^2, 199, 202, 213, 214, 215, 225, 227, 228, 231, 233, 235, 252, 256, 257, 262, 284, 285, 312 straipsnių, priedo pakeitimo ir papildymo XXVI, XXX skyrių pavadinimų pakeitimo ir kodekso papildymo 256^1, 257^1 straipsniais įstatymas. *Valstybės žinios*, 2007, Nr. 81-3309.

[15] Criminal Code of the Federal Republic of Germany [interaktyvus. Žiūrėta 2018-04-23]. Prieiga per internetą: <*http://www.gesetze-im-internet.de/englisch_stgb/index.html*>.

duomenų ir informacinių sistemų konfidencialumo pažeidimais, yra įtrauktos į baudžiamojo įstatymo skyrių, kur numatomos įvairios su privatumo pažeidimais susijusios veikos[16]. Kitos iš jų, rodančios neteisėtą poveikį elektroniniams duomenims ir informacinei sistemai, yra priskiriamos žalą sukeliančioms nusikalstamoms veikoms[17]. Panašų požiūrį į šias veikas galima matyti ir Prancūzijos[18] baudžiamajame įstatyme. Šioje šalyje kai kurios konfidencialumą pažeidžiančios veikos yra įtrauktos į sekciją, kurioje numatomi slaptumo pažeidimai, o tiksliau – į šios sekcijos paragrafą, kuriame numatomi susirašinėjimo slaptumo pažeidimai[19]. Tos veikos, kuriomis yra daromas neteisėtas poveikis elektroniniams duomenims ar informacinei sistemai, yra priskiriamos prie kitų nusikaltimų nuosavybei, t. y. nusikalstamoms veikoms, susijusioms su neteisėta prieiga prie automatizuotos duomenų apdorojimo sistemos[20]. Kitose valstybėse minėtoji nusikalstamų veikų grupė į atskiras dalis neskaidoma: visos šios veikos yra nustatytos tame pačiame baudžiamojo įstatymo skyriuje. Pavyzdžiui, Lenkijos baudžiamajame įstatyme[21] minėtosios veikos yra kriminalizuotos

---

[16] Vokietijos baudžiamojo įstatymo specialiosios dalies penkioliktajame skyriuje numatytos šios veikos: duomenų šnipinėjimas (202a straipsnis), duomenų perėmimas (202b straipsnis) ir duomenų šnipinėjimo bei perėmimo parengiamieji veiksmai (202c straipsnis).

[17] Vokietijos baudžiamojo įstatymo specialiosios dalies dvidešimt septintajame skyriuje numatytos šios veikos: duomenų pakeitimas (303a straipsnis) ir kompiuterio sabotažas (303b straipsnis).

[18] Penal Code of the French Republic [interaktyvus. Žiūrėta 2018-04-23]. Prieiga per internetą: <*http://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations*>.

[19] Prancūzijos baudžiamojo įstatymo II knygos (Nusikaltimai ir nusižengimai prieš asmenį) II antraštinės dalies (Veikos prieš asmenį) VI skyriaus (Veikos asmenybei) IV sekcijos (Slaptumo pažeidimai) II paragrafe (Susirašinėjimo slaptumo pažeidimai) numatyta neteisėtą perimtį atitinkanti nusikalstama veika (226-15 straipsnis).

[20] Prancūzijos baudžiamojo įstatymo III knygos (Nusikaltimai ir nusižengimai nuosavybei) II antraštinės dalies (Kiti nusikaltimai nuosavybei) III skyriuje (Neteisėta prieiga prie automatizuotos duomenų apdorojimo sistemos) numatytos neteisėtą prieigą, neteisėtą poveikį duomenims ir sistemai (323-1 straipsnis) ir netinkamą įtaisų naudojimą (323-3-1 straipsniai) atitinkančios nusikalstamos veikos.

[21] Criminal Code of the Republic of Poland [interaktyvus. Žiūrėta 2018-04-23]. Prieiga per internetą: <*http://www.legislationline.org/documents/section/criminal-codes/country/10*>.

XXXIII skyriuje *Nusikaltimai informacijos apsaugai*. Rusijos baudžiamajame įstatyme[22] jos numatytos IX dalies *Nusikaltimai visuomenės saugumui ir tvarkai* 28 skyriuje *Nusikaltimai kompiuterinės informacijos srityje*. Šie skirtumai yra svarbūs, nes leidžia suprasti ir nustatyti kitų valstybių doktrinoje susiformavusių požiūrių taikymo ribas atskleidžiant Lietuvos BK XXX skyriaus rūšinės vertybės – elektroninių duomenų ir informacinių sistemų saugumo – turinį. Vadinasi, užsienio mokslininkų nuomonės, kokia vertybė yra pažeidžiama dėl informacinių technologijų plėtros atsiradusiomis nusikalstamomis veikomis, turėtų būti vertinamos atsižvelgiant į konkrečios valstybės baudžiamojo įstatymo nuostatas. Tokiu atveju bet kokios idėjos atspindėtų konkrečios valstybės baudžiamojo įstatymo struktūrą ir kriterijus, kuriais remiantis ji buvo sudaryta. Taigi nereikėtų stebėtis, kad tam tikrais atvejais vertybių aiškinimai, atsižvelgiant į tai, kokios valstybės atstovai juos pateikia, gali būti tik iš dalies pritaikomi atskleidžiant Lietuvos BK XXX skyriuje numatytos vertybės turinį.

1.2. Elektroninės erdvės ir elektroninių duomenų bei informacinių sistemų saugumas

Siekiant nustatyti baudžiamojo įstatymo saugomą vertybę, pažeidžiamą nusikalstamomis veikomis elektroninėje erdvėje, mokslinėje literatūroje galima rasti keletą saugumo koncepcijų: *elektroninės erdvės saugumo* (angl. *cyber security)* ir *techninio kompiuterių saugumo* (angl. *technical computer security)*[23]. Šios savo apimtimi skirtingos koncepcijos susiformavo dėl įvairių elektroninėje erdvėje kylančių grėsmių ir atitinkamai skirtingų prevencijai taikytinų būdų bei priemonių parinkimo problemų. *Elektroninės erdvės saugumo,* arba plačiausią prasmę saugumui suteikianti koncepcija, dažniausiai minima tais atvejais, kai yra pabrėžiami įvairūs nacionalinio saugumo aspektai. Dėl to elektroninės erdvės saugumo terminas yra vartojamas kaip

[22] Criminal Code of the Russian Federation [interaktyvus. Žiūrėta 2018-04-23]. Prieiga per internetą: <*http://www.russian-criminal-code.com*>.

[23] Marcinauskaitė, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos*, 2011, 3(3); *Cybercrime: Digital Cops in a Networked Environment*. Balkin, J., *et al*. (ed.). New York (N.Y.): New York University Press, 2007, p. 63.

viską apimantis[24] ir susijęs su visko, kas funkcionuoja elektroninėje erdvėje arba gali būti per šią erdvę pasiekiama, apsauga nuo joje kylančių grėsmių[25]. Atitinkamai baudžiamosios teisės srityje elektroninės erdvės saugumas gali būti laikomas papildoma baudžiamajame įstatyme tiesiogiai neįvardyta vertybe, kuri yra pažeidžiama (arba jai keliama grėsmė) bet kuria iš elektroninėje erdvėje padaromų nusikalstamų veikų.

Minėtoji vertybė galėtų būti laikoma ir kriterijumi, kuriuo remiantis nusikalstamą veiką būtų galima priskirti elektroninėje erdvėje padaromų veikų kategorijai, nes, be kita ko, ji parodo dėl informacinių technologijų, sudarančių elektroninės erdvės pagrindą, plėtros atsiradusias grėsmes. Tokios vertybės identifikavimas yra svarbus ne tik teoriškai, bet ir taikant baudžiamąjį įstatymą. Pavyzdžiui, atskleidžiant BK 198^2 straipsnyje numatytos nusikalstamos veikos sudėties požymius būtina nustatyti, ar nusikalstama veika yra padaryta elektroninėje erdvėje. Iš šio BK straipsnio neaišku, kokioms konkrečiai nusikalstamoms veikoms daryti gali būti naudojami jame minimi įrenginiai ar programinė įranga, taigi ir kaip plačiai taikytinas minėtasis BK straipsnis. Atsižvelgiant į šių priemonių (įrankių) specifiką, jų paskirtį ir veikimo ypatybes, galima teigti, kad jos yra skirtos ne bet kokioms, o būtent nusikalstamoms veikoms elektroninėje erdvėje daryti. Vadinasi, nustačius, kad nusikalstama veika buvo padaryta elektroninėje erdvėje, ir radus įrenginius ar programinę įrangą, kuri buvo naudojama tokiai veikai padaryti, kaskart spręstina, ar kaltininko veikoje nėra ir BK 198^2 straipsnyje numatytos nusikalstamos veikos sudėties požymių. Kaip matyti, minėtaisiais atvejais nusikalstamų veikų elektroninėje erdvėje identifikavimas (taikant atitinkamus kriterijus) yra neatsiejamas nuo teisingo padarytų nusikalstamų veikų kvalifikavimo.

Minėtoji siauresnė *techninio kompiuterių saugumo* koncepcija dažniausiai yra siejama tik su elektroninių duomenų ir informacinių sistemų saugumo užtikrinimu, todėl yra aktuali bandant suvokti ne visas, o tik BK XXX skyriuje įtvirtintas, elektroninėje erdvėje padaromas

[24] Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Computers & security*, 2013, 38: 97; Kettemann, M. C. Ensuring Cybersecurity through International Law. *REDI*, 2017, 69(2): 282.

[25] Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Computers & security*, 2013, 38: 101.

nusikalstamas veikas. Šiuo požiūriu baudžiamojoje teisėje svarbu tai, kad elektroninės erdvės ir techninis kompiuterių saugumas kaip saugotinos vertybės nėra tapačios – nusikalstamomis veikomis elektroninėje erdvėje (ypač kalbant apie tradicines į šią erdvę perkeltas veikas) gali būti keliama grėsmė įvairioms vertybėms, ne tik minėtajam elektroninių duomenų ar informacinių sistemų saugumui. Kaip antai neteisėto turinio informacijos (sprogstamųjų, radioaktyviųjų medžiagų, sprogmenų ar jų gamybos instrukcijų, pornografinio turinio dalykų platinimas, neapykantos prieš bet kokios tautybės, rasės, etninę ar kitokią žmonių grupę ar terorizmo kurstymas ir pan.) platinimas elektroninėje erdvėje, atsižvelgiant į tokių veiksmų *modus operandi,* poveikio BK XXX skyriuje nurodytai vertybei gali ir neturėti. Kita vertus, bendriausia prasme, be žalos (ar grėsmės) pagrindinei vertybei, tokiomis tradicinėmis veikomis, jei jos padarytos elektroninėje erdvėje, visada pažeidžiamas elektroninės erdvės saugumas.

BK XXX skyriuje minimos vertybės pavadinime tiesiogiai nurodytas saugumas, be abejo, gali būti atskleidžiamas taikant lingvistinį aiškinimą. Tokiu atveju užtektų nurodyti, kad elektroniniai duomenys ir informacinės sistemos yra saugios, kai joms nekeliamas pavojus arba jos yra apsaugotos nuo pavojų[26]. Kita vertus, tokia bendrojo pobūdžio saugumo samprata yra neinformatyvi – iš jos netampa aišku, apie kokias grėsmes ir kokias elektroninių duomenų bei informacinių sistemų saugotinas ypatybes yra kalbama. Dėl to doktrinoje, aiškinant įvairius saugumo aspektus, yra einama kita linkme – vietoj bendrosios saugumo koncepcijos dažniausiai yra pateikiama gana detali, saugumo modelius atspindinti jos samprata. Saugumo koncepcijos ištakų ieškant saugumo politikos, o konkrečiau – saugumo modelių srityje, galima nustatyti tris elektroninių duomenų ir informacinių sistemų saugumą apibūdinančias kategorijas: jų konfidencialumas (angl. *confidentiality)*, integralumas (angl. *integrity)* ir prieinamumas (angl. *availability)*. Kone analogiškos informacijos saugotinos ypatybės minimos ir viename iš svarbiausių priimtų saugumo standartų *LST ISO/IEC 27001:2006 lt – Informacijos technologija – Saugumo metodai – Informacijos saugumo valdymo sistemos – Reikalavimai* (toliau – ISO/IEC 27001 standartas). Jame informacijos saugumas apibūdintas kaip

[26] Dabartinės lietuvių kalbos žodynas. 4-asis leidimas. Keinys, S., *et al*. (red). Lietuvių kalbos institutas, 2000, p. 677.

informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimas[27]. Nors šie techninio kompiuterio saugumo elementai gali būti vadinami skirtingai – pagrindinėmis saugumo koncepcijomis[28], principais[29] ar siekiais[30], dažniausiai jie yra siejami su konfidencialumo, integralumo ir prieinamumo triada, mokslinėje literatūroje sutrumpintai vadinama *CIA triada*. Remiantis šia triada, baudžiamosios teisės srityje nustatomi elektroninių duomenų ir informacinių sistemų saugumo turinį sudarantys elementai, be to, BK XXX skyriuje įtvirtintos nusikalstamos veikos skaidomos į smulkesnes grupes.

Analizuojant mokslinėje literatūroje pateikiamus saugumo aiškinimo variantus, be klasikinio požiūrio į *CIA triadą*[31], galima įžvelgti ir siekį savaip interpretuoti minėtąją triadą sudarančius elementus[32] bei bandymus išplėsti jos turinį, įtraukiant daugiau saugumą apibūdinančių požymių[33]. Kita vertus, kad ir kokia būtų interpretacijų įvai-

[27] Be to, papildomai nurodoma, kad informacijos saugumui priskiriamos ir šios informacijos savybės: autentiškumas, atskaitingumas, negalėjimas išsižadėti ir patikimumas.

[28] Sumit, K.; Nishit, N.; Sumita, N. Communication networks: principles and practice. New York: McGraw-Hill, 2007, p. 336.

[29] Vacca, J. R. (ed.) Computer and Information security handbook. Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 256.

[30] Stoneburner, G. Underlying Technical Models for Information Technology Security: recomendations of the National Institute of Standards and Technology [interaktyvus. Žiūrėta 2018-07-06]. Prieiga per internetą: <*http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf*>.

[31] Whitman, M. E., *et al*. Principles of information security. 3-ioji laida. Boston: Thomson: Course Technology, 2009, p. 10; Computer and Information security handbook. Vacca, J. R. (ed.) Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 256; Bishop, M. Computer Security: Art and Science. Addison Wesley Professional, 2003, p. 4; Skersys, G. Informacijos sauga: mokomoji knyga. Kaunas: TEV [i.e. Technologija], 2011, p. 11; Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 9.

[32] Sumit, K.; Nishit, N.; Sumita, N. Communication networks: principles and practice. New York: McGraw-Hill, 2007, p. 336.

[33] Bene radikaliausiu požiūriu į *CIA triados* elementų visumą gali būti laikoma D. Parkerio suformuluota šešių elementų sistema, kuri dažniausiai vadinama *D. Parkerio heksada*. Remiantis šia naująja techninio kompiuterių saugumo struktūra, nustatomi tokie elementai: konfidencialumas, integralumas, prieinamumas, autentiškumas, naudingumas ir nuosavybės teisių išsaugojimas. Kaip teigiama, minėtieji elementai turėtų pakeisti klasikinę *CIA triadą* kaip nepakankamą užtikrinant elektroninių duomenų saugumą *(Computer security handbook)*. 4-oji laida. Hutt, A. E.; Bosworth, S.; Hoyt, D. B. (ed.). New York, *et al*. Wiley, 2002).

rovė, reikėtų pripažinti, kad techninio kompiuterių saugumo šerdimi išlieka *CIA triada* – elektroninių duomenų ir informacinių sistemų konfidencialumas, integralumas bei prieinamumas. Šie kaip klasikiniai pripažįstami elektroninių duomenų ir informacinių sistemų saugumo aspektai minimi ir Konvencijos dėl elektroninių nusikaltimų 1 skirsnio 1 dalyje, kurioje pateikiamos nusikaltimų kompiuterinių duomenų ir sistemų konfidencialumui, vientisumui ir prieinamumui apibrėžtys.

Vadinasi, galima teigti, kad elektroninių duomenų ir informacinių sistemų saugumo turinį atskleisti ir sustruktūrinti BK XXX skyriaus nusikalstamas veikas padeda *CIA triados* modelis. Juo remiantis, veikos elektroninių duomenų ir informacinių sistemų saugumui gali būti suskirstytos į elektroninių duomenų ir informacinės sistemos konfidencialumo, integralumo bei prieinamumo pažeidimus. Su elektroninių duomenų konfidencialumo pažeidimais tiesiogiai yra susijusi BK 198 straipsnyje numatyta veika, o su informacinės sistemos konfidencialumo pažeidimais – BK 198[1] straipsnyje numatyta veika.

1.3. Elektroninių duomenų ir informacinių sistemų konfidencialumas

Jau minėta, kad klasikiniu požiūriu pagrįstam elektroninių duomenų ir informacinių sistemų saugumo reikalavimui įgyvendinti būtina išlaikyti tris svarbiausias jų savybes – konfidencialumą, integralumą[34] ir prieinamumą[35]. Kaip vieną iš konfidencialumo elektroninėje erdvėje

[34] Elektroninių duomenų ir informacinių sistemų integralumas rodo elektroninių duomenų ir informacinių sistemų vidinės struktūros užbaigtumą bei vientisumą. Elektroninių duomenų integralumas reiškia, kad duomenys per visą jų tvarkymo laiką be atitinkamų teisėtų įgaliojimų nebuvo pakeisti. Informacinės sistemos integralumas reiškia, kad duomenų apdorojimo funkcijas atliekančios sistemos nebuvo neteisėtai keičiamos ar modifikuojamos (Plačiau žr. Marcinauskaitė, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos*, 2011, 3(3); Bishop, M. Computer Security: Art and Science. Addison Wesley Professional, 2003, p. 5; Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 9 ir kt.).

[35] Elektroninių duomenų ir informacinių sistemų prieinamumas padeda užtikrinti, kad teisėtiems vartotojams elektroniniai duomenys ir informacinės sistemos yra be trukdžių ar kliūčių prieinamos bet kuriuo užklausos pateikimo metu (Plačiau

apsaugos būdų pasirinkus baudžiamosios teisės priemones, tokios vertybės pažeidimai tiesiogiai kriminalizuojami BK 198 ir 198[1] straipsniuose. Pirmajame iš jų aprašyti neviešų elektroninių duomenų konfidencialumo pažeidimai neteisėtai jais disponuojant – stebint, fiksuojant, perimant, įgyjant, laikant, pasisavinant, paskleidžiant ar kitaip panaudojant. Antrajame atskirai kriminalizuojami informacinės sistemos konfidencialumo pažeidimai dėl neteisėto prisijungimo prie jos (jei buvo pažeistos sistemos apsaugos priemonės). Baudžiamosios atsakomybės už šias veikas nustatymo BK XXX skyriuje ypatybė yra ta, kad jos yra kriminalizuojamos kaip atskiros nusikalstamos veikos. Tai verčia atskirti elektroninių duomenų ir informacinių sistemų konfidencialumą bei šią vertybę analizuoti atskirai iš neviešų elektroninių duomenų ir apribotą (atsietą) prieigą turinčių informacinių sistemų saugumo pozicijų.

Analizuojant BK XXX skyriuje numatyto rūšinio teisinio gėrio formuluotę matyti, kad jai priskiriamas ne tik teisinis (konfidencialumo), bet ir technologinis (elektroninių duomenų ir informacinės sistemos) aspektas. Pačia bendriausia lingvistine prasme konfidencialumą galima sieti su slaptumu ir pasitikėjimu. Pavyzdžiui, *konfidencialus* žodynuose apibrėžiamas kaip viešai neskelbtinas, slaptas[36], skirtas būti laikomas paslaptyje[37], taip pat pasakytas arba parašytas slaptai ir ketinamas laikyti paslaptyje[38] arba perduotas pasitikint, slaptai[39]. Toks požiūris, be abejo, rodo galimą vertybės aiškinimo kryptį, bet siekiant ją interpretuoti tiksliau būtina suderinti minėtuosius teisinius ir technologinius aspektus.

žr.: Computer and Information security handbook. Vacca, J. R. (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 256; Whitman, M. E., *et al*. Principles of information security. 3-ioji laida. Boston: Thomson: Course Technology, 2009, p. 9).

[36] Dabartinės lietuvių kalbos žodynas. 7-asis pataisytas ir papildytas leidimas. Keinys, S. (vyr. red.). Vilnius: Lietuvių kalbos institutas, 2012, p. 324.

[37] Khokins, Dzh. M. The Oxford Dictionary of the English Language. Moskva: OOO «Izdatelstvo Actrel», OOO «Izdatelstvo AST», 2001, p. 149.

[38] Longman dictionary of Contemporary English. Summers, D. (edit. director). Berlin; München: Langenscheidt. Longman, 1987, p. 212.

[39] Funk & Wagnalls standard dictionary of the English language: combined with Britannica world language dictionary. I tomas. Chicago (Ill.): Encyclopaedia Britannica, 1960, p. 274.

Elektroninių duomenų konfidencialumas panašiai suvokiamas ir literatūroje[40], bendriausia prasme jis yra siejamas su draudimu atskleisti duomenis tiems asmenims ar sistemoms, kurie neturi prieigos prie šių duomenų teisės. Dėl to teigiama, kad „informacija išsaugo konfidencialumą, kai ji apsaugota nuo atskleidimo neautorizuotiems asmenims ar sistemoms“[41], kai „informacija yra neprieinama neįgaliotiems asmenims ar procesams“[42]. Atitinkamai konfidencialumas padeda užtikrinti, „kad slapti duomenys bus prieinami tik tiems vartotojams, kuriems ši prieiga leista (tokie vartotojai vadinami autorizuotaisiais)“[43], t. y. „informacija turi būti pateikta tik tam, kam priklauso, ir niekam kitam“[44]. Beje, šie požiūriai artimi konfidencialumo sampratai, suformuluotai ISO/IEC 27001 standarte, pagal kurį informacijos konfidencialumas yra ypatybė, reiškianti, kad informacija „nebus prieinama ar pateikiama neįgaliotiems fiziniams ar juridiniams asmenims arba procesams“. Panašiai minėtasis *CIA triados* elementas aiškinamas ir specializuotuose žodynuose, kuriuose konfidencialumas apibūdinamas pabrėžiant galimybę užtikrinti, „kad duomenys yra neprieinami neįgaliotiems vartotojams“[45]. Į tokius duomenų konfidencialumo aspektus atkreiptas dėmesys ir teismų praktikoje išaiškinant, kad konfidencialumas – tai *duomenų savybė, reiškianti tai, kad jie nebus prieinami ar pateikiami asmenims, kuriems nesuteikiama tokia teisė*[46] arba jis *reiškia,*

[40] Whitman, M. E., *et al*. Principles of information security. 3-ioji laida. Boston: Thomson: Course Technology, 2009, p. 10; Computer and Information security handbook. Vacca, J. R. (red), Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 256.; Bishop, M. Computer Security: Art and Science. Addison Wesley Professional, 2003, p. 4; Skersys, G. Informacijos sauga: mokomoji knyga. Kaunas: TEV [i.e. Technologija], 2011, p. 11; Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 9.

[41] Whitman, M. E., *et al*. Principles of information security. 3-ioji laida. Boston: Thomson: Course Technology, 2009, p. 10.

[42] Richardson, V. J.; Chang, C. J.; Smith, R. Accounting information systems. New York (N.Y.): McGraw-Hill: Education, 2014, p. 222.

[43] Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 9.

[44] Plėštys, R., *et al*. Tinklų sauga. Kaunas: Vitae Litera, 2008, p. 17.

[45] Dictionary of Information Science and Technology. I tomas. Khosrow-Pour, M. (ed.). Hershey, Pa., et al: Idea Group Reference, 2007, p. 152.

[46] Kauno apygardos teismo 2017 m. rugsėjo 27 d. nuosprendis baudžiamojoje byloje Nr. N1-173-319/2017.

kad duomenys nėra atskleidžiami ar pasiekiami vartotojams bei procesams, kuriems nesuteikta tokia teisė[47]. Duomenų neatskleidimo svarba išlieka aktuali viso duomenų tvarkymo metu, todėl ir prie sistemoje laikomų, ir prie joje perduodamų duomenų prieigą gali turėti tik tokią teisę turintys asmenys[48].

BK 198[1] straipsnyje numatoma atsakomybė už neteisėto prisijungimo prie informacinės sistemos veiką, todėl svarbu nustatyti, kaip slaptumo aspektai atsispindi būtent informacinių sistemų apsaugos srityje. Tiesa, apie informacinių sistemų konfidencialumą literatūroje užsimenama gana retai, toks poreikis dažniausiai yra susijęs su sistemose esančios informacijos (duomenų) saugumo svarba. Vadinasi, siekiant apsaugoti informacinio saugumo interesus, be kitko, būtina išlaikyti ir informacijos bei jos apdorojimo sistemų konfidencialumą, t. y. „subjektyviai nustatomą (priskiriamą) informacijos charakteristiką (savybę), nurodančią būtinumą įvesti apribojimus subjektams, turintiems prieigą prie tos informacijos, ir sistemos (aplinkos) užtikrinamą galimybę saugoti nurodytą informaciją paslaptyje nuo subjektų, neturinčių įgaliojimų prie jos prieiti“[49]. Informacijos konfidencialumą galima apsaugoti priemonėmis, kuriomis „nustatomos informacinių sistemų vartotojų prieigos teisės, t. y. prie kokių informacinių išteklių (duomenų, katalogų ar sistemų) konkretus vartotojas turi prieigos teisę“[50]. Kaip matyti, apie informacinės sistemos konfidencialumą dažniausiai užsimenama tada, kai ši sistema turi padėti užtikrinti joje esančių duomenų slaptumą, neleisdama prie jų prieiti, jei tam nėra suteikta teisė. Be abejo, vienas iš sistemų konfidencialumo užtikrinimo tikslų yra jose esančių elektroninių duomenų apsauga, nes neteisėta prieiga prie sistemos neretai gali būti tik tarpinis etapas kaltininkui siekiant joje atlikti tolesnius veiksmus. Kita vertus, žiūrint iš baudžiamosios teisės pozicijų, reikėtų atkreipti dėmesį, kad BK 198[1] straipsnyje nurodytas neteisėtas prisijungimas prie informa-

[47] Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendis baudžiamojoje byloje Nr. 1-234-825/2017.

[48] Beynon-Davies, P. Business information systems. Basingstoke; New York (N.Y.): Palgrave Macmillan, 2013, p. 193.

[49] Kazanavičius, E., *et al*. Informacijos saugos vadyba. Kaunas: Vitae Litera, 2008, p. 10.

[50] Budnikas, A., *et al*. Elektroninės valdžios sauga. Kaunas: Vitae Litera, 2008, p. 51.

cinės sistemos yra kriminalizuojamas kaip atskira nusikalstama veika, kuri nesiejama su tolesniais kaltininko veiksmais sistemoje. Dėl to apibrėžiant informacinės sistemos konfidencialumą siūlytina jį aiškinti nepateikiant nuorodų į elektroninių duomenų neviešumo apsaugą – toks požiūris į baudžiamojo įstatymo saugomą vertybę būtų artimesnis įstatymo leidėjo pasirinktai neteisėto prisijungimo prie informacinės sistemos koncepcijai. Tokiu atveju informacinės sistemos konfidencialumas reikštų, kad sistemos, atliekančios duomenų apdorojimo funkcijas, yra prieinamos tik prieigos teisę prie jų turintiems asmenims (ar procesams) ir tik tiek, kiek apima ši jiems suteikta teisė.

Kadangi aptartųjų elektroninių duomenų ir informacinių sistemų konfidencialumo sąvokų ištakos nėra tiesiogiai susijusios su baudžiamąja teise, vadinasi, nėra jai tiesiogiai pritaikytos, todėl analizuojant šį *CIA triados* elementą kaip baudžiamojo įstatymo saugomą vertybę būtina pabrėžti keletą svarbių aspektų:

Pirma, kaip minėta, konfidencialumas laikytinas ne tik vienu iš elektroninių duomenų, bet atskirai ir informacinės sistemos saugumo elementu. Kalbėti apie tokį atskyrimą leidžia BK XXX skyriuje nurodyto teisinio gėrio konstrukcija – jo su technologijomis susijusioje dalyje šalia elektroninių duomenų kaip atskiras elementas minima ir informacinė sistema. Techninis kompiuterių saugumas nėra vienalytis, todėl apie elektroninių duomenų ir informacinių sistemų saugumą galima kalbėti atskirai[51]. Vadinasi, visi saugumo elementai (konfidencialumas, integralumas ir prieinamumas) atskirai analizuotini ir iš informacinės sistemos, ir iš elektroninių duomenų pozicijų. Beje, ir mokslinėje literatūroje atkreiptas dėmesys į elektroninių duomenų bei informacinių sistemų saugumo atskyrimą. Joje pabrėžiama, kad elektroninių duomenų saugumas yra susijęs su saugių duomenų savybėmis, kaip antai konfidencialumu, integralumu, prieinamumu ir pan., o informacinių technologijų saugumo prioritetas – technologijomis pagrįstų sistemų, apdorojančių duomenis, saugumas[52]. Atsižvelgiant į tai, baudžiamojo įstatymo saugomos vertybės išaiškinimai galėtų būti tikslinami ir teismų praktikoje. Pavyzdžiui, teismų sprendimuose nustačius, kad BK 198[1] straipsnyje numatytos nusikalstamos

[51] Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Computers & security*, 2013, 38: 98.

[52] *Ibidem*.

veikos dalykas yra informacinė sistema ar jos dalis, siūlytina vertybe laikyti ne *informacinių sistemų bei jose esančių elektroninių duomenų saugumą*[53] ar teisėtų vartotojų interesą *šiomis sistemomis naudotis konfidencialiai, taip pat disponuoti elektroniniais duomenimis*[54], o būtent *informacinės sistemos ar jos dalies konfidencialumą*. Žalos ar jos grėsmės sukėlimą informacinėje sistemoje ar jos dalyje esantiems ar perduodamiems elektroniniams duomenims rodo kiti BK straipsniai, kuriuose numatoma atsakomybė būtent už tokių vertybių (pavyzdžiui, elektroninių duomenų konfidencialumo, integralumo ar prieinamumo) pažeidimus.

Antra, neviešų elektroninių duomenų konfidencialumo išsaugojimas svarbus viso duomenų tvarkymo proceso metu, todėl, apibrėžiant šį duomenų požymį, neturėtų būti pabrėžiamas duomenų neviešumo užtikrinimas atliekant tik kokį nors vieną elektroninių duomenų tvarkymo veiksmą.

Trečia, nustatant konfidencialumo apsaugos ribas, didelę reikšmę turi terminų *informacija* ir *duomenys* skirtumai. Nors jie, atsižvelgiant į kontekstą, dažniausiai vartojami kaip sinonimai, bet baudžiamojoje teisėje aiškinant ir baudžiamojo įstatymo saugomos vertybės, ir dalyko požymius dėl tikslumo siūlytina vartoti *duomenų* terminą. Tai padėtų išvengti abejonių, ar baudžiamosios teisės priemonėmis iš tikrųjų pakankamai užtikrinamas duomenų, esančių *priešinformaciniame etape*, konfidencialumas.

Ketvirta, atsižvelgiant į tai, kad informacinių procesų dalyviai yra ne tik žmonės, bet ir informacinės sistemos, konfidencialumo apibrėžimuose šalia neleistinos asmenų prieigos būtina paminėti ir neįgaliotuosius procesus arba neautorizuotą sistemų prieigą. Nors toks skirstymas leidžia aiškiau suvokti nusikalstamos veikos padarymo mechanizmą, bet iš baudžiamosios teisės pozicijų sprendžiant, kas gali

---

[53] Pavyzdžiui, Kauno apygardos teismo 2015 m. gegužės 7 d. nutartis baudžiamojoje byloje Nr. 1A-432-594/2015; Šiaulių apylinkės teismo 2017 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-148-771/2017; Šiaulių apylinkės teismo 2016 m. gruodžio 21 d. nuosprendis baudžiamojoje byloje Nr. 1-957-771/2016.

[54] Pavyzdžiui, Šiaulių apylinkės teismo 2018 m. kovo 5 d. nuosprendis baudžiamojoje byloje Nr. 1-506-771/2018; Šiaulių apylinkės teismo 2017 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-148-771/2017; Tauragės rajono apylinkės teismo 2017 m. birželio 15 d. nuosprendis baudžiamojoje byloje Nr. 1-70-607/2017.

pažeisti elektroninių duomenų ir informacinių sistemų konfidencialumą, jis kol kas aktualus tik nustatant asmens kaltę. Konstatavus, kad kaltininkas veikė tyčia, informacinė sistema ar jos dalis, kuri buvo panaudota konfidencialumo pažeidimams padaryti, galėtų būti pripažįstama tik nusikalstamos veikos padarymo priemone ar įrankiu.

2. Nusikalstamų veikų elektroninėje erdvėje kriminalizavimas ir ekvivalentinio vertinimo principas

2.1. Ekvivalentinio vertinimo principas ir jo įgyvendinimo būdai

Dėl informacinių technologijų raidos atsiradę nauji tarpusavio sąveikos būdai padeda atskleisti elektroninės erdvės ypatumus, neretai apibūdinamus „dematerializacijos“ (angl. *dematerialisation)*, „skaitmeninimo“ (angl. *digitisation)*, „beribiškumo“ (angl. *borderless)*[55], „automatizacijos“[56] ir kitais požymiais. Vadinasi, nereikėtų stebėtis, kad nusikalstamos veikos, iki šiol egzistavusios tik fiziniame pasaulyje, perkeltos į elektroninę erdvę įgijo „tam tikrą specifiką, atsižvelgiant į jų elektroninę formą, komunikavimo internete būdus ir interneto globalumą bei kitus specifinius elektroninės komunikacinės erdvės požymius“[57]. Be to, elektroninėje erdvėje paplito ir anksčiau nežinomos nusikalstamos veikos, kurios galėtų būti laikomos išimtinai informacinių technologijų plėtros rezultatu. Siekiant nustatyti tokių nusikalstamų veikų sudėties požymius, jas kvalifikuoti ir apskritai suvokti, svarbu nuspręsti, ar esamos baudžiamojo įstatymo normos yra suderinamos su elektroninės erdvės ypatybėmis, ar jos yra pakankamos

[55] Reed, C. Online and Offline Equivalence: Aspiration and Achievement. *International Journal of Law and Information Technology*, 2010, 18(3): 258.

[56] Civilka, M., *et al*. Informacinių technologijų teisė. Vilnius: NVO teisės institutas, 2004, p. 511.

[57] Štitilis, D. Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos: daktaro disertacija: socialiniai mokslai, teisė (01 S), Vilnius: LTU, 2002, p. 19.

nusikalstamoms veikoms, padarytoms elektroninėje erdvėje, kvalifikuoti. Būtent tai sudaro prielaidas kelti daug kokybiškai naujų teisinių problemų[58].

Sprendžiant minėtuosius klausimus, derinant įvairius technologijų ir teisės aspektus, teisėkūroje pradėtas taikyti ekvivalentinio vertinimo principas, leidžiantis elektroninei erdvei tinkamai sukurti naują arba daugeliu atveju pritaikyti jau esamą teisinį reguliavimą. Šis apie „technologinį abejingumą“[59] (angl. *technology indifference)* verčiantis mąstyti principas bendriausia prasme atspindi idėją, kad esamos ar kuriamos teisės normos turėtų padėti nustatyti vienodus reikalavimus ir fizinėje, ir elektroninėje erdvėje atliekamiems veiksmams – tai, „kas galioja fizinėje, galioja ir elektroninėje erdvėje“[60]. Baudžiamojoje teisėje tai reikštų, kad ta pati nusikalstama veika turėtų būti kvalifikuojama vienodai, neatsižvelgiant į tai, kurioje – fizinėje ar elektroninėje – erdvėje ji yra padaryta. Taip suvokiamas ekvivalentinio vertinimo principas baudžiamojoje teisėje tampa aktualus dėl to, kad stabdo „natūralią žmogiškąją tendenciją elektroninę erdvę vertinti kaip kažką *kito*, kur leidžiami skirtingi ir neretai žemesni elgesio standartai“[61]. Siekiant lygiaverčio teisinio nusikalstamų veikų vertinimo, baudžiamuoju įstatymu turėtų būti užtikrinamas ir vienodas teisinių vertybių apsaugos lygis fizinėje bei elektroninėje erdvėje, nes nebebūtų svarbu, kurioje iš jų nusikalstama veika buvo padaryta. Ir priešingai – ekvivalentaus vertinimo pažeidimai lemtų analogiškų veikų, padarytų skirtingose erdvėse, nevienodą kvalifikavimą, vadinasi, ir skirtingus teisinius jų padarymo padarinius. Pavyzdžiui, jei elektroninių dokumentų klastojimui, dėl kurio nebuvo padaryta didelė žala, kvalifikuoti būtų taikoma ne BK 300 straipsnio 1 dalis, o BK 196 straipsnio 3 dalis, – tokia veika būtų laikoma baudžiamuoju nusižengimu, o ne nusikaltimu.

---

[58] Kohl, U. Legal Reasoning and Legal Change in the Age of the Internet – Why the Ground Rules are still Valid. *International Journal of Law and Information Technology*, 1999, 7(2): 126–128.

[59] Reed, C. Taking Sides on Technology Neutrality. *SCRIPTed*, 2007, 4(3): 269.

[60] Schellekens, M. What holds Off-Line, also holds On-Line? [interaktyvus. Žiūrėta 2018-04-05]. Prieiga per internetą: *<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952275>*.

[61] Reed, C. Online and Offline Equivalence: Aspiration and Achievement. *International Journal of Law and Information Technology*, 2010, 18(3): 253.

Kita vertus, kyla ir nemažai praktinių ekvivalentinio vertinimo principo idėjos įgyvendinimo sunkumų. Kaip antai, iš paties principo netampa aišku, kokiomis priemonėmis šis vienodas vertinimas turėtų būti pasiekiamas, – dėl to jo įgyvendinamumo klausimas vis dar lieka atviras. Tokiais atvejais teisės norma yra kaip „juodoji dėžė“[62] – nors jos turinys turėtų atitikti minėtuosius reikalavimus, bet kaip tai padaryti, paliekama spręsti teisėkūrai ir praktikai. Vis dėlto šiuo klausimu doktrinoje įmanoma rasti keletą atspirties taškų. Pavyzdžiui, šis reikalavimas gali būti suprantamas taip, kad ieškant elektroninei erdvei tinkamos teisės normos pirmiausia reikėtų bandyti rasti analogišką normą fizinėje erdvėje, kuri tiktų ir elektroninėje erdvėje susiklosčiusiai situacijai. Vadinasi, veiksmams elektroninėje erdvėje vertinti pirmiausia siūloma taikyti tas teisės normas, kurios yra tinkamos analogiškiems (ar panašiems) veiksmams fizinėje erdvėje. Taigi ir elektroninėje, ir fizinėje erdvėje susiklosčiusios lygiavertės situacijos turėtų būti sprendžiamos vienodai, bet, jei situacijos skiriasi, dėl jų gali būti priimami nevienodi sprendimai, bet tik tiek, kiek skiriasi pačios situacijos[63]. Tokia pozicija leidžia išvengti ir bereikalingos teisėkūros, nes ekvivalentinio vertinimo atveju pirmiausia turėtų būti gana plačiai interpretuojama jau įtvirtinta teisės norma, o ne kuriamos naujos. Atitinkamai tokia pat norma, anksčiau taikyta tik fizinėje erdvėje daromiems veiksmams reguliuoti, bus kaskart „naujai atrandama“[64] ją taikant ir veiksmams elektroninėje erdvėje. Tiesa, tokio požiūrio ištakų galima rasti ir atsižvelgiant į pačios teisės normos prigimtį, kuri leidžia jai išlikti net ir pasikeitus aplinkybėms – „jeigu be žvilgsnio atgal teisės norma kaip atsakas į nuolat besikeičiančią visuomenę irgi būtų nuolat besikeičianti, jos iš viso nebūtų. <...> Jeigu taisyklė nuolat kistų <...> teisės norma negalėtų atlikti savo pagrindinių funkcijų, konkrečiai – užtikrinti tikrumo, numatomumo, tvarkos ir saugumo“[65].

---

[62] Schellekens, M. What holds Off-Line, also holds On-Line? [interaktyvus. Žiūrėta 2018-04-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952275*>.

[63] *Ibid*., p. 5.

[64] *Ibid*., p. 7.

[65] Kohl, U. Legal Reasoning and Legal Change in the Age of the Internet – Why the Ground Rules are still Valid. *International Journal of Law and Information Technology*, 1999, 7(2): 133.

Remiantis ekvivalentiniu vertinimu, „naujai atrandamomis“ galėtų būti laikomos baudžiamojo įstatymo normos, kuriomis nustatoma atsakomybė už tradicines nusikalstamas veikas, jei jos yra pritaikomos elektroninėje erdvėje padarytoms nusikalstamoms veikoms kvalifikuoti. Tokiais atvejais baudžiamajame įstatyme numatyti minėtųjų veikų sudėties požymiai yra iš naujo permąstomi, į jų turinį įtraukiama naujų aspektų ir suteikiama kitų prasmių. Vadinasi, nebūtų klaidinga teigti, kad baudžiamajame įstatyme yra įtvirtinta nemažai „užslėptų“ elektroninėje erdvėje padaromų nusikalstamų veikų, jei tradicinių nusikalstamų veikų sudėtys gali būti išaiškintos ir pritaikomos nusikalstamoms veikoms elektroninėje erdvėje kvalifikuoti.

Kita vertus, toks gana ekonomiškas požiūris turi ir trūkumų. Dėl fizinės ir elektroninės erdvės (pastarajai netaikytini fizinės erdvės mato kriterijai[66]) esminių skirtumų neretai gali būti neįmanoma palyginti ir analogiškai įvertinti jose atliekamų veiksmų. Atitinkamai neįmanoma rasti ir tokioms situacijoms taikytinos tos pačios teisės normos. Doktrinoje teigiama, kad elektroninėje erdvėje atliekami veiksmai ne visada turi atitikmenį fizinėje erdvėje, todėl ekvivalentiškumo įgyvendinimas „gali pasirodyti neįvykdomu siekiu“[67]. Vadinasi, teisės normos paieška gali baigtis tuo, kad elektroninei erdvei tinkama ir pritaikoma norma išvis nebus rasta[68]. Dėl to, remiantis ekvivalentinio vertinimo (funkcinio ekvivalentiškumo) principu, kiek įmanoma mažinami veiksmų fizinėje ir elektroninėje erdvėje teisinio vertinimo skirtumai ir neatmetamos specialiųjų normų kūrimo galimybės[69]. Bet tik tais išskirtiniais atvejais, kai siekiant lygiavertiškumo neįmanoma taikyti tos pačios normos. Baudžiamosios teisės srityje tai reikštų, kad specialiųjų normų kūrimas yra būtinas tais atvejais, kai nėra analogiškų (ar tinkamų) pavojingos veikos elektroninėje erdvėje atitikmenų fizinėje erdvėje, todėl jai kvalifikuoti negali būti taikomos esamos

---

[66] Mitra, A. From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces. *Journal of Computer – Mediated Communication*, 2001, 7(1).

[67] Reed, C. Taking Sides on Technology Neutrality. *SCRIPTed*, 2007, 4(3): 277.

[68] Schellekens, M. What holds Off-Line, also holds On-Line? [interaktyvus. Žiūrėta 2018-04-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952275*>, p. 5.

[69] Reed, C. Online and Offline Equivalence: Aspiration and Achievement. *International Journal of Law and Information Technology*, 2010, 18(3): 251.

baudžiamojo įstatymo normos. Šie ekvivalentinio vertinimo principo taikymo ypatumai yra aktualūs svarstant įvairius nusikalstamų veikų elektroninėje erdvėje kriminalizavimo būdus.

2.2. Lietuvos baudžiamasis įstatymas ir ekvivalentinio vertinimo principas

Ekvivalentinio vertinimo principo taikymas baudžiamosios teisės srityje, be kita ko, padeda atskleisti elektroninės erdvės ir baudžiamosios teisės šakos sąveiką. Nusikalstamų veikų elektroninėje erdvėje kriminalizavimas taikant šį principą – tai tarsi fizinėje erdvėje padarytų nusikalstamų veikų „vertimas“[70] (angl. *translation)*, elektroninėje ir fizinėje erdvėje ieškant panašios interesų pusiausvyros. Kita vertus, sprendžiant elektroninių nusikalstamų veikų kriminalizavimo problemas, neturėtų būti pamirštama, kad jų visumą sudaro įvairios veikos – ir turinčios aiškų atitikmenį fizinėje erdvėje, ir neturinčios tiesiogiai pritaikomų atitikmenų. Atsižvelgiant į tai, 2000 m. BK atsakomybė už šias veikas nustatyta dviem skirtingais būdais: 1) tradicinių nusikalstamų veikų, padaromų fizinėje ir elektroninėje erdvėje, ekvivalentus vertinimas užtikrinamas joms kvalifikuoti taikant tą patį BK straipsnį (pavyzdžiui, baudžiamoji atsakomybė pagal BK 309 straipsnį turėtų kilti neatsižvelgiant į tai, ar pornografinio turinio dalykai platinami fizinėje ar elektroninėje erdvėje); 2) išimtinai dėl informacinių technologijų raidos atsiradusioms veikoms kvalifikuoti BK įtvirtintos atskiros nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtys (BK XXX skyrius).

Pirmuoju atveju parenkant atitinkamą BK straipsnį į elektroninę erdvę perkeltoms tradicinėms nusikalstamoms veikoms kvalifikuoti, įtaką daro įstatymų leidėjo požiūris, ar informacinių technologijų taikymas iš esmės galėjo pakeisti tradicinių nusikalstamų veikų sudėties požymių aiškinimą, tokių nusikalstamų veikų pobūdį ir esmę[71]. Pri-

[70] Hughes, J. The Internet and the Persistence of Law. *Boston College Law Review*, 2003, 44(359): 364.

[71] Ši problema vaizdžiai perteikiama posakiais „jaunas vynas, nėra taros“ (angl. *new wine, no bottles)* ir „senas vynas naujoje taroje“ (angl. *old wine in new bottles)*. Posakis „jaunas vynas, nėra taros“ vartojamas norint pabrėžti išskirtines elektroninės erdvės ypatybes ir parodyti, kad joje atsiranda visiškai naujų nusikalstamo elgesio apraiškų (plačiau žr. Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford

tariant požiūriui, kad tradicinės veikos perkėlimas į elektroninę erdvę yra aplinkybė, leidžianti kalbėti apie iš esmės naują nusikalstamų veikų, kurioms vertinti nepakanka esamos sudėties, rūšį, pasirenkamas specialiųjų normų kūrimo būdas. Pavyzdžiui, kompiuterinis sukčiavimas kaip specialioji sukčiavimo norma numatyta Latvijos (177[1] skyrius), Estijos (213 paragrafas), Lenkijos (287 straipsnis) ir Vokietijos (263a skyrius) baudžiamuosiuose įstatymuose.

Kitas galimas variantas yra lankstesnis, leidžiantis formuojant tradicinių nusikalstamų veikų sudėtis atsisakyti tiesioginių nuorodų į informacines technologijas. Bendriausia prasme tai reikštų, kad baudžiamojo įstatymo normos, taikomos fizinėje erdvėje padarytoms nusikalstamoms veikoms kvalifikuoti, be pakeitimų taikytinos ir analogiškoms veikoms elektroninėje erdvėje. Tokiu atveju teisinio reguliavimo pakankamumas yra užtikrinamas plačiai interpretuojant tradicinių nusikalstamų veikų sudėties požymius ir taip tarsi sukuriant šių veikų „atspindį“ elektroninėje erdvėje. Tokiais atvejais išvada, kad baudžiamajame įstatyme yra numatyta atsakomybė už tradicines, elektroninėje erdvėje padarytas veikas, dažniausiai pagrindžiama baudžiamosios teisės teorijos ir teismų praktikos analize. Tik dėl specialiųjų normų trūkumo šiuo atveju negalima nieko pasakyti apie tinkamą arba netinkamą tradicinių nusikalstamų veikų, pakitusių dėl informacinių technologijų taikymo, kriminalizavimą.

Iš Lietuvos BK specialiosios dalies nuostatų matyti, kad įstatymų leidėjas yra pasirinkęs antrąjį (lankstesnį) minėtųjų nusikalstamų veikų įtvirtinimo baudžiamajame įstatyme variantą. Pavyzdžiui, 2004 m. sausio 22 d. ratifikavus Konvenciją dėl elektroninių nusikaltimų, BK nebuvo numatytos specialios kompiuterinės klastotės, kompiuterinio sukčiavimo, nusikalstamų veikų, susijusių su vaikų pornografija ar autorių teisių ir gretutinių teisių pažeidimais, sudėtys. Šioms veikoms kvalifikuoti ir toliau yra taikomi BK 182, 192, 300

University Press, 2007, p. 19; Cybercrime and Jurisdiction: a global survey. Koops, B. J.; Brenner, S. (eds). The Hague: T.M.C. Asser Press, 2006, p. 26–29). Priešingai nuomonei išsakyti vartojamas posakis „senas vynas naujoje taroje“, kuris reiškia, kad informacinių technologijų taikymas neturi esminės įtakos nusikalstamoms veikoms. Šios technologijos reiškia ne ką kitą, o tik naujų tos pačios nusikalstamos veikos padarymo būdų atsiradimą (plačiau žr. Brenner, S. W. Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology*, 2004, 9(13).

ir 309 straipsniai. Nors BK 309 straipsnis palaipsniui buvo papildomas su informacinėmis technologijomis susijusiais požymiais[72], bet dėl jų šios veikos suvokimas nepasikeitė, šie požymiai atspindi tik kai kurias specifines elektroninei erdvei būdingas situacijas. Be to, BK yra numatyta ir daugiau tradicinių nusikalstamų veikų, kurios pagal savo pobūdį galėtų būti padaromos ir fizinėje, ir elektroninėje erdvėje, bet į jų sudėtį neįtraukiami požymiai, vienu ar kitu aspektu susiję su informacinių technologijų taikymu (pavyzdžiui, BK 154, 170, 211, 250[1] ir daugelis kitų straipsnių). Vadinasi, tradicinių nusikalstamų veikų sudėčių taikymas naujoms su elektroninės erdvės specifika susijusioms situacijoms neišvengiamai yra pavedamas teismų praktikai. Būtent jai palikta galimybė pereiti nuo elektroninės erdvės kaip „nepaprastos“ supratimo prie „įprastos“ ir „kasdienės“[73]. Be abejo, toks įstatymo leidėjo pasirinkimas priklauso nuo to, ar iš tiesų yra įmanomas toks platus tradicinių nusikalstamų veikų sudėties požymių aiškinimas. Šiuo požiūriu svarbu atkreipti dėmesį į tai, ar tradicinių veikų sudėtyse nenumatyta tiesioginę sąsają su fizine erdve turinčių požymių, ar į sudėtį yra įtraukta alternatyvių materialiosios išraiškos nežyminčių požymių, ar sudėties požymiams nustatyti netrukdo tai, kad informacinėms technologijoms nebūdinga fiziniam asmeniui priskiriama sąmonė ir pan. Dėl to kai kuriais atvejais akivaizdu, kad baudžiamojo įstatymo normos kol kas negalima taikyti elektroninėje erdvėje padarytoms nusikalstamoms veikoms kvalifikuoti dėl joje numatytų požymių tiesioginės sąsajos su fizine erdve (pavyzdžiui, BK 165, 178, 180, 187 straipsniai). Kitais atvejais toks klausimas dar nėra kilęs ir lieka neišspręstas (pavyzdžiui, BK 284 straipsnis)[74].

---

[72] Pagal BK 309 straipsnio 2 dalį, baudžiamoji atsakomybė kyla ir tais atvejais, kai asmuo, taikydamas informacines ir ryšių technologijas ar kitas priemones, įgijo (ar suteikė) prieigą prie pornografinio turinio dalykų, kuriuose vaizduojamas vaikas arba asmuo, pateikiamas kaip vaikas. Šių požymių įtvirtinimas BK 309 straipsnyje yra siejamas su 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvos 2011/93/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR, nuostatų įgyvendinimu.

[73] Brian, Ch. J. The Online/Offline Cognitive Divide: Implications for Law. *SCRIPTed*, 2016, 13(1): 87.

[74] Šiuo požiūriu ypač aktualu, kad internetas yra tapęs „viešu elektroniniu susirinkimu“, sujungiančiu žmones ir įmones, užtikrinančiu žodžio, spaudos, susirinkimų

Teismų praktikoje pasitaiko nemažai sėkmingo baudžiamojo įstatymo normų taikymo pavyzdžių kvalifikuojant tradicines į elektroninę erdvę perkeltas nusikalstamas veikas. Teismų praktikoje pateikti išaiškinimai yra svarbūs dėl to, kad suteikia galimybę nusikalstamomis veikomis laikyti ir tokias veikas, kurių *modus operandi* būdingas „žmogaus ir mašinos“ arba „mašinos ir mašinos“[75] kontaktas. Pavyzdžiui, dėl praktikoje išplėstos klasikinės apgaulės sampratos atsiranda galimybė BK 182 straipsnį taikyti kvalifikuojant sukčiavimą elektroninėje erdvėje, kaip antai sukčiavimą elektroninės bankininkystės srityje atliekant negrynųjų pinigų pervedimą iš vienos sąskaitos į kitą ar pasiimant grynuosius pinigus iš bankomato. Galimybę kalbėti apie apgaulės rūšį, peržengiančią klasikinės apgaulės ribas[76], suteikė Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2001 m. spalio 9 d. nutartis baudžiamojoje byloje Nr. 2K-682/2001, kurioje prieita prie išvados, kad tyčia gali būti suklaidinamas ne tik asmuo, bet ir elektroninė sistema:

<...> elektroninėje bankininkystėje visos operacijos su piniginėmis lėšomis yra tvarkomos žmogaus sudarytų kompiuterinių programų pagrindu. Klientas su banku bendrauja ne tiesiogiai, o per elektroninę sistemą. Sistema sudaryta tokiu būdu, kad ji priima komandą ir atlieka operaciją, jei surinkti tinkami sąskaitų turėtojų identifikaciniai kodai. Būtent kodas pagal programos veikimo principus identifikuoja asmens, kaip sąskaitos turėtojo, tapatybę ir pažymi teisę atlikti operacijas su sąskaitoje esančiomis piniginėmis lėšomis. Jei kodą surenka ir komandą duoda asmuo, neturintis teisės atlikti operacijų su sąskaitoje esančiomis piniginėmis lėšomis, jis pateikia operacinei sistemai ir bankui save kaip kitą asmenį, turintį tokią teisę, bei taip suklaidina elektroninę sistemą ir tuo pačiu banką. Pastarieji dėl klaidos įtakos nusprendę, kad toks asmuo teisėtai duoda komandą atlikti operaciją, dėl suklydimo įtakos savanoriškai perleidžia teisę į turtą, t. y. perveda pinigines lėšas kitam sąskaitos turėtojui, o vėliau išduoda pinigus.

---

laisvę (Linzer, P. From the Gutenberg Bible to Net Neutrality - How Technology Makes Law and Why English Majors Need to Understand It. *McGeorge Law Review*, 2008, 39: 3–21).

[75] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 59.

[76] Pranka, D. Nusikalstamos veikos ir civilinės teisės pažeidimo atribojimo koncepcija Lietuvos baudžiamojoje teisėje: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: MRU, 2012, p. 54–55.

Toks apgaulės išaiškinimas yra aktualus visais atvejais, kai asmens tapatybė patvirtinama ir dėl jos suklaidinama būtent elektroninėje erdvėje. Dėl to šios praktikos tęstinumas yra svarbus konstatuojant, pavyzdžiui, kredito teikimo įmonių esminę apgaulę kaltininkui elektroninėje erdvėje prisistačius kitu asmeniu: <...> *apgaulė prieš kredito įstaigas pasireiškė tuo, kad nuteistieji kartu su nenustatytu asmeniu neteisėtai įgijo S. Č. elektroninės bankininkystės prisijungimo duomenis ir juos pateikė kredito įstaigoms elektroninėje erdvėje prisistatydami kaip S. Č. Tokiu būdu kredito įstaigos buvo suklaidintos ir apgaule įtikintos, jog paraišką paskolai gauti pateikė būtent S. Č. Įtikintos, jog paraišką gauti paskolai pateikė S. Č., kredito įstaigos pervedė atitinkamas kaltinime nurodytas sumas, kurias nuteistieji užvaldė. Taigi apgaulė pasireiškė duomenų, kuriuos gavo neteisėtai, pateikimu kredito įstaigoms.*

Atmestini apeliacinio skundo argumentai, kad apgaulė prieš kredito įstaigas nebuvo esminė ir nelėmė kredito įstaigų apsisprendimo suteikti kreditus. Teigiama, jog visi kreditai buvo išduoti dėl pačių kredito įstaigų neatsakingo elgesio. Kredito įstaigos, anot apelianto, paskolas S. Č. būtų išdavusios net ir tada, jei visus duomenis būtų pildęs ir pateikęs pats S. Č. Tačiau toks aiškinimas visiškai prieštarauja teisinei logikai. Nuteistųjų nusikalstama veika (sukčiavimas) šiuo atveju pasireiškė tuo, kad jie suklaidino (apgavo) S. Č. dėl to, kam bus naudojama jo sąskaita, ir apgaule neteisėtai įgiję elektroninės bankininkystės duomenis, juos panaudojo prieš S. Č. valią jo vardu paimdami paskolas, taip apgaudami ir paskolos davėjus – kredito įmones. Tokia apgaulė laikytina esminė, nes, priešingu atveju, kredito įstaigoms jokios paraiškos išduoti paskolas S. Č. vardu nebūtų pateiktos ir kredito įstaigos jokių paskolų jo vardu nebūtų suteikusios. Tik panaudojus apgaulę prieš kredito įstaigas, buvo įgytas joms priklausantis turtas[77].

Nemažai klausimų kasacinėje jurisprudencijoje yra išspręsta aiškinant ir taikant BK 300 straipsnį (Dokumento suklastojimas ar disponavimas suklastotu dokumentu). Praktikoje atkreiptas dėmesys į tai, kad pripažįstant dokumentą BK 300 straipsnyje numatytos nusikalstamos veikos dalyku, yra svarbus jo turinys, bet ne forma (pavyzdžiui, ar tai materialusis, ar elektroninis dokumentas):

[77] Klaipėdos apygardos teismo 2018 m. kovo 1 d. nutartis baudžiamojoje byloje Nr. 1A-9-651/2018.

Įstatymas nenustato reikalavimų dokumento formai. Dokumentu gali būti pripažįstamas bet kokia forma ant popieriaus, elektroninėje erdvėje ar kompiuterinėje laikmenoje padarytas įrašas, tačiau keliami reikalavimai dokumento turiniui. Dokumentas turi suteikti informacijos apie įvykį, veiksmą ar asmenį. Dokumentas – tai tam tikra forma padarytas įrašas, kuris nustato, pakeičia ar panaikina teisiškai reikšmingą faktą (juridinį faktą). Tai įrašas, kurio panaudojimas gali sukelti fiziniam ar juridiniam asmeniui ar valstybei teisiškai reikšmingus padarinius <...> (kasacinės nutartys baudžiamosiose bylose Nr. 2K-263/2010, 2K-57/2014). Šis išaiškinimas, be kita ko, gali būti siejamas su elektroninės formos nediskriminavimo principu, kuris reiškia, kad informacijos teisinė galia negali būti paneigta tik dėl to, kad „ši informacija yra sukurta, išsiųsta, gauta ar išsaugota elektroninėmis priemonėmis“[78], ypač tais atvejais, kai elektroniniai ir rašytiniai dokumentai atlieka tas pačias funkcijas. Toks platus išaiškinimas kasacinės instancijos teismo praktikoje dokumentu leidžia pripažinti ir, pavyzdžiui, elektroninį mokėjimo nurodymą: *Nors pirmosios instancijos teismas R. K. išteisinimą motyvavo tuo, kad elektroninis mokėjimo nurodymas nėra dokumentas BK 300 straipsnio prasme, teisėjų kolegija sprendžia, kad elektroninis mokėjimo nurodymas yra dokumentas BK 300 straipsnio prasme, nes jis nustato teisiškai reikšmingą faktą (juridinį faktą) ir jo panaudojimas sukelia arba gali sukelti fiziniam ar juridiniam asmeniui, ar valstybei teisiškai reikšmingus padarinius* (kasacinė nutartis baudžiamojoje byloje Nr. 2K-56-696/2018)[79].

---

[78] Štitilis, D.; Kiškis, M.; Limba, T., *et al.* Interneto ir technologijų teisė: vadovėlis. Vilnius: Registrų centras, 2016, p. 23.

[79] Kitas svarbus ekvivalentinio vertinimo principo taikymo aspektas – vienodas padarytos nusikalstamos veikos pavojingumo vertinimo kriterijų taikymas ir fizinio, ir elektroninio dokumento suklastojimo ar disponavimo suklastotu dokumentu atveju. Veikos pavojingumo nuostata šios kategorijos baudžiamosiose bylose gali būti siejama su tuo, kad baudžiamojoje teisėje numatoma atsakomybė tik už pavojingas veikas, o ne formalius pažeidimus (pavyzdžiui, kasacinės nutartys baudžiamosiose bylose Nr. 2K-161-696/2017, 2K-424-696/2016, 2K-508/2013, 2K-7-251/2013). Atsižvelgiant į byloje nustatytų aplinkybių visumą, šioje kasacinėje nutartyje konstatuota, kad padaryta veika – dokumentų suklastojimu elektroniniame mokėjimo pavedime nurodant netikrą mokėjimo paskirtį – nebuvo pažeistos fizinių ar juridinių asmenų teisės ir minėtiesiems asmenims ar valstybei nesukelta teisiškai reikšmingų padarinių, jokių ginčų dėl įvykusių pinigų pervedimų tarp pervedimuose nurodytų ar kitų

Kasacinės instancijos teismo praktikoje yra išspręstas ir BK 168 straipsnio taikymo klausimas kvalifikuojant elektroninėje erdvėje padarytus asmens privataus gyvenimo neliečiamumo pažeidimus. Žvelgiant iš elektroninės erdvės saugumo perspektyvos, įvairus neteisėtas kišimasis į asmens privatumo sritį, t. y. tiek, kiek šie pažeidimai padaromi elektroninėje erdvėje, yra kriminalizuotas ir BK 166, 167, 168 straipsniuose – tai asmens susižinojimo neliečiamumo pažeidimai, neteisėtas informacijos apie privatų asmens gyvenimą rinkimas, taip pat neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas. Iš Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2013 m. lapkričio 20 d. nutarties baudžiamojoje byloje Nr. 2K-138/2015 matyti, kad informacija apie kito žmogaus privatų gyvenimą gali būti ir fizinės, ir elektroninės formos, todėl ir pati veika – tokios informacijos atskleidimas – gali būti padaroma ir fizinėje, ir elektroninėje erdvėje. Atsižvelgiant į tai, papildomas padarytos veikos kvalifikavimas ir pagal BK 198 straipsnį tokiais atvejais laikytinas pertekliniu: <...> *svarbu yra tai, kad viešas informacijos apie kito žmogaus privatų gyvenimą paskelbimas galimas ne tik fizinėje, bet ir elektroninėje erdvėje, todėl šioje erdvėje (pvz., elektroniniu paštu) paskelbta informacija turi ir visus elektroninių duomenų požymius. Taigi BK 198 straipsnio taikymas vien dėl to, kad nusikalstamos veikos dalykas, t. y. informacija apie kito žmogaus privatų gyvenimą, yra elektroninių duomenų formos, nepagrįstas. Įvertinusi tai, teisėjų kolegija sprendžia, kad L. B. veiksmų – privataus D. Č. ir D. J. susirašinėjimo išsiuntimo šešiais elektroninio pašto adresais, kvalifikavimas pagal idealiąją nusikalstamų veikų sutaptį, t. y. pagal BK 168 ir 198 straipsnius, yra netinkamas (perteklinis). Šie veiksmai kvalifikuotini tik pagal BK 168 straipsnio 1 dalį.* Šiuo atveju būtent ekvivalentinio vertinimo principas leidžia užtikrinti ne tik BK 168, bet ir, pavyzdžiui, BK 166 ir 167 straipsnių pritaikomumą nusikalstamoms veikoms, kuriomis kėsinamasi į asmens privatumo neliečiamumą jau ne fizinėje, o elektroninėje erdvėje, kvalifikuoti.

---

asmenų ir tarp pervedimuose nurodytų asmenų ir juridinių asmenų (bankų) nekilo. Be to, būtent mokėjimo paskirties nurodymo mokėjimo pavedime neatitiktis realiam pinigų pervedimo tikslui tapo vienu iš įrodymų konstatuojant turto pasisavinimo (BK 183 straipsnis) padarymą. Būtent šios aplinkybės teismui leido padaryti išvadą, kad BK 300 straipsnis byloje taikytas nepagrįstai.

Vertinant tokį tradicinių nusikalstamų veikų, padarytų elektroninėje erdvėje, kriminalizavimo variantą, svarbu pabrėžti, kad pačioje Konvencijoje dėl elektroninių nusikaltimų[80] nereikalaujama pažodinio jos nuostatų įgyvendinimo nacionalinėje teisėje. Konvencijos aiškinamosios ataskaitos[81] 79 punkte teigiama, kad Konvencijos 7–10 straipsniai yra susiję su tradicinėmis nusikalstamomis veikomis (nusikaltimais), kurios padaromos naudojantis kompiuterine sistema. Kadangi dauguma valstybių yra kriminalizavusios analogiškas tradicines veikas, dėl to jau esamos sudėtys gali būti (arba nėra) pakankamai plačios, kad būtų pritaikomos naujoms situacijoms. Dėl to valstybės, įgyvendindamos minėtosios konvencijos nuostatas, turėtų įvertinti esamas teisės normas ir nustatyti, ar įrodžius kompiuterinės sistemos ar kompiuterių tinklo panaudojimo faktą, šios normos galėtų būti taikomos. Jei esamos teisės normos yra pritaikomos ir tokio pobūdžio pavojingoms veikoms, Konvencijoje nenustatomas reikalavimas keisti tradicinių nusikalstamų veikų sudėtis arba baudžiamajame įstatyme numatyti naujas nusikalstamas veikas (nusikaltimus). Kaip matyti, Konvencijos aiškinamojoje ataskaitoje pateikiamas gana lankstus ir valstybių nacionalinės teisės tradicijų neneigiantis požiūris. Šis požiūris yra pažangus ir tuo, kad juo pripažįstamas teisės normos atsparumas pokyčiams, pačioms valstybėms paliekant pasirinkti, kaip jos savo baudžiamojoje teisėje užtikrins darnų fizinės ir elektroninės erdvės ryšį. Dėl to abejonių kelia literatūroje išdėstytos idėjos, kad Konvencijoje dėl elektroninių nusikaltimų numatoma pareiga baudžiamaja-

[80] Konvencijos dėl elektroninių nusikaltimų 7–10 straipsniuose numatytos šios tradicinės, bet dėl informacinių technologijų taikymo pakitusios nusikalstamos veikos: kompiuterinės klastotės (7 straipsnis), kompiuterinis sukčiavimas (8 straipsnis), nusikaltimai, susiję su vaikų pornografija (9 straipsnis), nusikaltimai, susiję su autorių teisių ir gretutinių teisių pažeidimais (10 straipsnis). Vis dėlto tradicinių nusikalstamų veikų, pakitusių dėl informacinių technologijų taikymo, sąrašas neturėtų būti apribojamas tik Konvencijoje dėl elektroninių nusikaltimų nurodytomis veikomis. Šioms nusikalstamoms veikoms priskirtinos visos tradicinės veikos, kurios pagal savo pobūdį gali būti padaromos ne tik fizinėje, bet ir elektroninėje erdvėje. Netikslinga sudaryti baigtinio tokių veikų sąrašo, nes dėl informacinių technologijų raidos vis daugiau anksčiau tradicinėmis laikytų nusikalstamų veikų bus perkelta į elektroninę erdvę. Pakitus technologijų taikymo galimybėms, šis sąrašas itin greitai prarastų savo aktualumą.

[81] Convention on Cybercrime Explanatory Report [interaktyvus. Žiūrėta 2018-04-07]. Prieiga per internetą: <*http://conventions.coe.int/Treaty/en/Reports/Html/185.htm*>.

me įstatyme *expressis verbis* įtvirtinti specialiąsias normas, pavyzdžiui, kriminalizuojant kompiuterinį sukčiavimą kaip specifinę sukčiavimo rūšį[82].

Sprendžiant nusikalstamų veikų elektroninėje erdvėje kriminalizavimo problemas, BK XXX skyriuje taip pat įtvirtintos atskiros nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėtys. Baudžiamajame įstatyme jos buvo būtinos, nes elektroninėje erdvėje atsirado specifinių, fizinei erdvei nebūdingų, veikos rūšių. Šių veikų pobūdis lėmė, kad joms kvalifikuoti negalėjo būti taikomos jau esamos baudžiamojo įstatymo normos. Teisės normų, kuriomis numatoma baudžiamoji atsakomybė už tradicines nusikalstamas veikas, taikymas tokiais atvejais keltų abejonių arba būtų visiškai netinkamas. Pavyzdžiui, doktrinoje yra atkreipiamas dėmesys, kad DDoS atakai (angl. *Distributed Denial of Service attack)* neįmanoma pritaikyti jokios tradicinių nusikalstamų veikų kategorijos – „tai nėra vagystė, turto prievartavimas ar vandališki veiksmai. Todėl teisėje turėtų būti pateikiamos definicijos šioms naujos rūšies nusikalstamoms veikoms apibrėžti“[83]. Beje, tą patį galima pasakyti ir apie kenkimo programinės įrangos platinimą, neteisėtą prisijungimą prie informacinės sistemos ir neteisėtą poveikį elektroniniams duomenims bei daugelį kitų veikų, kurios dėl savo ypatybių negali būti padaromos fizinėje erdvėje, todėl ir neturi joje atitikmenų. Būtent tokia padėtis ir leidžia kalbėti apie svarbius veikų, padarytų fizinėje ir elektroninėje erdvėje, skirtumus, atitinkamai ir atskirų baudžiamojo įstatymo normų poreikį.

Kita vertus, į nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui neturėtų būti žvelgiama pernelyg paprastai – net jei šios BK XXX skyriuje numatytos veikos iš pirmo žvilgsnio gali atrodyti visiškai neturinčios analogų fizinėje erdvėje, naujos ir sunkiai paaiškinamos, vis dėlto kai kurie jų aspektai leidžia įžvelgti ir tam tikrų panašumų su tradicinėmis veikomis. Pavyzdžiui, neteisėto įsibrovimo doktrinos plėtojimą „skaitmeninėje aplinkoje“

[82] Sauliūnas, D. Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime. *Jurisprudencija*, 2010, 4(122): 215.

[83] The History of Information Security: A Comprehensive Handbook. Leeuw, D. K.; Bergstra, J. (eds). Amsterdam, *et al*. Elsevier, 2007, p. 706.

rodo neteisėto prisijungimo prie informacinės sistemos veika (BK 198[1] straipsnis), o į neteisėto disponavimo neviešais elektroniniais duomenimis (BK 198 straipsnis) dalyką metaforiškai bandoma pažvelgti kaip į asmens „kvazifizinius daiktus“ elektroninėje erdvėje, kurie kaip ir materialieji gali būti slepiami, laikomi arba perkeliami, perduodami. Ieškant BK 198[2] straipsnyje numatyto dalyko: įrenginių, programinės įrangos, slaptažodžių, prisijungimo kodų ir kitokių duomenų atitikmens fizinėje erdvėje, dažniausiai nurodoma tokių dalykų sąsaja su įsibrovimui į patalpas (ketinant padaryti nusikalstamą veiką) naudojamais įrankiais (angl. *burglary tools)*[84]. Kita vertus, akivaizdu, kad tokios nusikalstamos veikos, nors ir labai plačiai aiškinamos, negali būti laikomos neteisėtu asmens būsto neliečiamumo pažeidimu (BK 165 straipsnis), vagyste (BK 178 straipsnis), pasikėsinimu įvykdyti vagystę (BK 22 straipsnis, 178 straipsnis) ar kita tradicine nusikalstama veika. Kadangi nebuvo įmanoma rasti šioms veikoms galinčios tikti baudžiamojo įstatymo normos, jame įtvirtintos specialiosios, būtent šioms nusikalstamoms veikoms kvalifikuoti, taikytinos normos. Susidūrus su tokiomis situacijomis, teisėkūros procese pirmiausia yra rekomenduojama rasti tinkamiausią tokių elektroninėje erdvėje padarytų veikų atitikmenį fizinėje erdvėje ir kurti naujas normas, atsižvelgiant į šių tradicinių veikų ypatumus baudžiamajame įstatyme. Būtent taip, koncentruojantis į „panašumus nepaisant skirtumų“[85], gali būti įgyvendintas ekvivalentiškumo reikalavimas. Pavyzdžiui, už teritorinio privatumo pažeidimus fizinėje erdvėje baudžiamoji atsakomybė yra nustatyta BK 165 straipsnyje, kuriame kriminalizuoti neteisėti asmens būsto neliečiamumo pažeidimai. Neteisėto įsibrovimo į svetimą valdą (angl. *trespass)* doktrina leidžia, atsižvelgiant į vietos pobūdį, nustatyti bendrąsias patekimo į tam tikrą teritoriją taisykles: „kai kurios erdvės yra atviros, kai kurios uždaros, kai kurios atviros vieniems, bet uždaros kitiems.“[86] Nebūtų klaidinga teigti, kad šis požiūris yra aktualus ir aiškinantis, pavyzdžiui, neteisėto prisijungimo

---

[84] Comprehensive Study on Cybercrime, 2013 [interaktyvus. Žiūrėta 2018-07-01]. Prieiga per internetą: <*https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf* >, p. 92.

[85] Reed, C. Online and Offline Equivalence: Aspiration and Achievement. *International Journal of Law and Information Technology*, 2010, 18(3): 265.

[86] Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review*, 2016, 116: 1152.

prie informacinės sistemos veiką bei apibrėžiant BK 198[1] straipsnio taikymo galimybes – juk iš tiesų „skirtingoms erdvėms būdingos skirtingos neteisėto įsibrovimo normos“[87]. Vadinasi, tinkamiausias šios veikos atitikmuo, leidžiantis aiškiau suvokti neteisėtos prieigos elektroninėje erdvėje kriminalizavimo ištakas ir tokio kriminalizavimo poreikį, yra būtent asmens būsto neliečiamumo pažeidimai fizinėje erdvėje. Kaip teigiama doktrinoje, „internetas turi savitas neteisėto įsibrovimo normas, kurios yra labai panašios į jų fizinio pasaulio giminaitį“[88]. Šis požiūris dar svarbus ir dėl to, kad pateikia užuominų apie elektroninės erdvės ribas, tik šiuo atveju virtualias, peržengiamas kitaip nei fizinėje erdvėje.

Aptartieji iš ekvivalentinio vertinimo principo kylantys reikalavimai nėra baigtiniai – jie yra kur kas įvairesni ir sistemiškai nenagrinėti. Plintant nusikalstamoms veikoms elektroninėje erdvėje, tikėtina, kad lygiaverčio vertinimo idėja taps vis aktualesnė kalbant ir apie nusikalstamų veikų kvalifikavimą, jų sudėties požymių aiškinimą, ir apie teisinius padarinius, taikytinus už tokių veikų padarymą. Vadovaujantis ekvivalentinio vertinimo principu ir praktiškai įgyvendinant lygiavertį veikų vertinimą, tradicinėms nusikalstamoms veikoms, padarytoms elektroninėje erdvėje, kvalifikuoti taikytinas tas pats BK straipsnis, pagal kurį kvalifikuojamos analogiškos veikos fizinėje erdvėje[89]. Kita vertus, baudžiamoji atsakomybė už išimtinai tik elektroninėje erdvėje padaromas nusikalstamas veikas nustatoma taikant atskiras baudžiamojo įstatymo normas, įtvirtintas BK XXX skyriuje.

---

87 *Ibidem*.

88 Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review*, 2016, 116: 1153.

89 Fedosiuk, O.; Marcinauskaitė, R. Criminalization of Cybercrime and Principle of Equivalence. *Administratīvā un krimināla justīcija*, 2013, No. 2(63): 8.

3. Nusikalstamų veikų elektroninėje erdvėje sudėties požymių aiškinimas ir technologinio neutralumo principas

3.1. Technologinio neutralumo principas ir jo taikymas baudžiamojoje teisėje

Aiškinant nusikalstamų veikų elektroninėje erdvėje sudėties požymius, įtakos turi tai, kaip yra suvokiamos informacines technologijas įvardijančios sąvokos, ypač tais atvejais, kai sąsaja su technologijomis yra tiesiogiai įtvirtinta baudžiamojo įstatymo straipsnio dispozicijoje. Kadangi dėl sparčios informacinių technologijų raidos neišvengiamai kinta ir nusikalstamos veikos elektroninėje erdvėje, šių veikų kriminalizavimo pakankamumo, sudėties požymių aprašymo baudžiamajame įstatyme atitikties besikeičiančioms aplinkybėms klausimas išlieka vienas aktualesnių. Bendriausia prasme tokie gana painūs technologiniai ir baudžiamieji teisiniai sudėties požymių įtvirtinimo bei aiškinimo sunkumai gali būti įvardyti kaip doktrinoje minimas „technologijų ir terminologijos klausimas“[90]. Šis klausimas yra siejamas su ribų, šviesiosios linijos[91] (angl. *bright line),* nustatymu ir iš to logiškai išvedamu baudžiamojoje teisėje itin svarbiu teisinio tikrumo principu[92].

Kadangi su informacinėmis technologijomis susijusių nusikalstamų veikų sudėties požymių turinys yra gana dinamiškas, tai kelia nemažai tinkamos terminijos parinkimo, nusikalstamos veikos sudėties požymių aiškinimo ir jų apibrėžtumo problemų. Išvada, kas BK yra suprantamas kaip vieną ar kitą technologinį aspektą turintis sudėties požymis (atitinkamai, kokios yra jo turinio ribos), priklauso nuo pasirinkto vieno iš galimų tokiems požymiams interpretuoti taikytinų

[90] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 13.

[91] *Šviesiąja linija* vadinama taisyklė (angl. *bright-line rule)*, kuri nepalieka dviprasmybių, yra paprastai ir aiškiai pateikta, suformuluota sprendžiant ginčą (*Black's Law Dictionary*. 9-asis leidimas. Garner, B. A. (ed. in chief). St. Paul (Minn.): West: Thomson Reuters business, 2009, p. 219).

[92] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 13.

principų – technologinio neutralumo (angl. *technological neutrality)* arba technologinio tikslumo (angl. *technological specific)*. Vieno iš šių principų pasirinkimas priklauso nuo to, ar teisės aktų turinys turi būti siauras, susijęs su konkrečiomis technologijomis (tikslus), ar platus, kuriuo remiantis nustatomos tik bendrosios jų ypatybės (neutralus). Nors abu minėtieji principai yra taikomi su technologijomis susijusios teisėkūros srityje, vis dėlto dominuojančiu[93], nors ir taikant tam tikras išimtis bei kritikuojant[94], gali būti laikomas lygiavertį technologijų vertinimą padedantis užtikrinti technologinio neutralumo principas. Toks pasirinkimas, be kita ko, gali būti grindžiamas tuo, kad smarkiai pasikeitus technologijoms įstatymų leidėjas gali pernelyg užtrukti atnaujindamas teisės normas. Nors ir labai keista, bet tokia situacija iš tiesų yra galima, nes „nenuspėjamas naujovių pobūdis pasunkina galimybes numatyti technologijų ateitį“[95]. Kuo savitesnes technologijas įtvirtina teisės norma, tuo sunkiau ji bus pritaikoma nenumatytoms naujovėms. Dėl to technologiškai neutralus požiūris leidžia užtikrinti juo remiantis sukurtų „ateičiai atsparių“[96] teisės normų ilgaamžiškumą.

Technologinio neutralumo kaip *gerojo* reguliavimo principas ES lygiu daugiausia dėmesio sulaukė peržiūrint telekomunikacijų reguliavimą (vėliau – ir kitose srityse). Kaip vienas iš penkių reguliavimo principų jis apibūdinamas remiantis technologijų diskriminavimo draudimu, t. y. teisinis reguliavimas „neturi nei nustatyti, nei diskriminuoti, teikdamas pirmenybę konkrečios rūšies technologijoms, o tik užtikrinti, kad ta pati paslauga būtų reguliuojama lygiaverčiu

---

93 Koops, B. J. Should ICT regulation be Technology-Neutral? [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746*>.

Downing, R. W. Shoring up the Weakest Link: What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. *Columbia Journal of Transnational Law*, 43(3): 705.

Kirby, C. A. Defining Abusive Software to Protect Computer Users from the Threat of Spyware. *Science and Law Review*, X(3): 287.

94 Ohm, P. The Arguments against Technology-Neutral Surveillance Laws. *Texas Law Review*, 2010, 88(7); Reed, C. Taking Sides on Technology Neutrality. *SCRIPTed*, 2007, 4(3).

95 Brad, A. Greenberg, Rethinking Technology Neutrality. *Minnesota Law Review*, 2016, 100(1495): 1525.

96 *Ibid*., p. 1512.

būdu, neatsižvelgiant į būdus, kuriais ji yra teikiama“[97]. Atkreipiant dėmesį į teisės normos tikslus, o ne konkrečias technologijas (technologinį tikslumą), šis principas yra panašiai suformuluotas ir Lietuvos Respublikos elektroninių ryšių įstatymo 2 straipsnio 2 dalyje. Minėtajame įstatyme, atskleidžiant jo reikšmę, nurodoma, kad „teisės normos turi būti taikomos atsižvelgiant į tikslus, kurių siekiama atitinkamomis teisės normomis, ir stengiantis, kad, kiek tai pagrįsta, vien tik dėl jų taikymo nebūtų skatinamas arba diskriminuojamas konkrečių technologijų naudojimas, taip pat teisės normos turėtų būti taikomos kiek įmanoma neatsižvelgiant į technologijas, kurios naudojamos su konkrečiu teisiniu santykiu susijusiems elektroninių ryšių tinklams ar elektroninių ryšių paslaugoms teikti“. Galimybę iš baudžiamosios teisės pozicijų kalbėti apie technologinio neutralumo principą, be kita ko, suteikia Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje nurodytas nacionalinėje teisėje įgyvendintinų ir su materialiąja baudžiamąja teise susijusių nuostatų interpretavimo būdas. Šioje konvencijoje, nustačius minimalius nusikalstamų veikų elektroninėje erdvėje sudėties požymiams keliamus reikalavimus, neišvengta ir su informacinėmis technologijomis susijusios terminijos. Atsižvelgiant į tai, Konvencijos aiškinamosios ataskaitos 36 punkte pateiktas jai įgyvendinti svarbus išaiškinimas: „nors materialinės baudžiamosios teisės nuostatos yra susietos su nusikaltimais, padaromais taikant informacines technologijas, Konvencijoje vartojama technologiškai neutrali kalba, kad teisės pažeidimai, už kuriuos baudžiama pagal baudžiamuosius įstatymus, galėtų būti taikomi abiem – ir dabartinėms, ir būsimosioms technologijoms“ (36 punktas)[98].

Į technologinio neutralumo principo taikymo galimybes, užtikrinant lygiavertį technologijų vertinimą, atkreipiamas dėmesys ir

---

[97] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions of 10 November 1999. Towards a new framework for Electronic Communications infrastructure and associated services - The 1999 Communications Review (COM/99/0539 final) [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:1999:0539:FIN*>.

[98] The Explanatory Report to the Convention on Cybercrime [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*http://conventions.coe.int/Treaty/en/Reports/Html/185.htm*>.

įvairiuose šį principą tyrinėjusių mokslininkų darbuose[99]. Juose technologijoms neutralus teisinis reguliavimas yra siejamas su tokio reguliavimo pastovumu bei efektyvumu, nes jis šių savybių neprarastų ir pakitus technologijoms. Toks teisinis reguliavimas yra mažiau veikiamas „technologinių neramumų“[100]. Kadangi technologijos plėtojasi kur kas greičiau nei su jomis susijusios teisės normos, galima būtų pritarti nuomonei, kad „reguliavimas turėtų būti lankstus, nekintantis ilgesnį laiką ir atviras technologijų pokyčiams“[101]. Pastovumą tokiais atvejais padeda užtikrinti vietoj nekintamų specifines technologijas nurodančių teisės normų kuriamos dinamiškos, galinčios plėtotis kartu su technologijomis normos[102]. Remiantis technologinio tikslumo principu, tokio lankstumo užtikrinti negalima – dėl nuolatinių inovacijų teisinis reguliavimas bet kuriuo momentu gali prarasti savo efektyvumą. Taigi ne veltui doktrinoje šis reguliavimas yra siejamas su „technologijų saulėlydžio“[103] terminu. Žiūrint iš baudžiamosios teisės pozicijų, technologinio neutralumo principas tampa aktualus dėl to, kad jis, *pirma*, leidžia išvengti dėl informacinių technologijų kaitos galinčių kilti nusikalstamų veikų sudėties požymių nepritaikomumo problemų (ypač nustačius reikšmingų technologijų pokyčių); *antra*, padeda nuspręsti, kaip turėtų būti aiškinami įvairūs nusikalstamų veikų sudėtyse nurodyti ir su informacinėmis technologijomis susiję terminai (pavyzdžiui, informacinė sistema, šios sistemos apsaugos prie-

---

[99] Ohm, P. The Arguments against Technology-Neutral Surveillance Laws. *Texas Law Review*, 2010, 88(7); Ali, R. Technological Neutrality. *Lex Electronica*, 2009, 14(2); Van der Haar, I. M. Technological Neutrality: What Does It Entail? [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=985260*>; Koops, B. J. Should ICT regulation be Technology-Neutral? [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746*>.

[100] Greenberg, B. A. Rethinking Technology Neutrality. *Minnesota Law Review*, 2016, 100(1495): 1513.

[101] Ali, R. Technological Neutrality. *Lex Electronica*, 2009, 14(2): 12.

[102] Van der Haar, I. M. Technological Neutrality: What Does It Entail? [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=985260*>.

[103] Ohm, P. The Arguments against Technology-Neutral Surveillance Laws. *Texas Law Review*, 2010, 88(7): 1686.

monės, elektroniniai duomenys). Juo labiau kad BK nepateikiamas autentiškas šių sąvokų išaiškinimas.

Kadangi sudėtinga tiksliai numatyti ateities technologijas, baudžiamojo įstatymo normos turėtų būti kuriamos taip, kad galėtų būti pritaikomos ir dar „nenumatytam“[104]. Kaip teigiama doktrinoje, „jei įstatymų leidėjas nusprendė uždrausti atlikti konkrečius veiksmus su prie interneto prijungtu namų kompiuteriu, tai *technologiškai neutrali* strategija įpareigotų tokią pat veiką laikyti nusikalstama, jei ji būtų padaryta naudojantis asmeniniu delniniu kompiuteriu, mobiliuoju telefonu ar naujosios kartos skaitmeniniais prietaisais“[105]. Tokiais atvejais skirtingos technologijos būtų vertinamos vienodai, atsižvelgiant į tuos pačius jiems būdingus veikimo principus[106]. Taigi technologinio neutralumo principą grindžiant technologijų diskriminavimo draudimu, jis iš esmės reiškia draudimą teikti prioritetą kuriai nors iš technologijų. Juo remiantis, nusikalstamos veikos sudėties požymiai turėtų būti formuluojami ir aiškinami taip, kad netaptų priklausomi nuo informacinių technologijų pokyčių ir specifinių jų ypatybių, jei toks priklausomumas nėra įstatymo leidėjo valia. Atsisakant technologijų specifiškumo, baudžiamajame įstatyme reikėtų vengti ir nuorodų į konkrečius nusikalstamų veikų padarymo būdus elektroninėje erdvėje (pavyzdžiui, kaip buvo prisijungta ar kokiu būdu buvo padarytas neteisėtas poveikis informacinei sistemai). Kvalifikuojant veiką, svaresnis yra pats rezultatas (pavyzdžiui, nustatytas neteisėto prisijungimo prie informacinės sistemos atvejis, sistema tapo neprieinama teisėtiems vartotojams), o ne nurodomas technologiškai konkretus būdas, kaip tai buvo padaryta.

Kaip specifinių terminų vartojimo atvejį, dėl kurio kilo nepakankamo nusikalstamų veikų elektroninėje erdvėje kriminalizavimo problema, galima būtų paminėti valstybių kaimynių (Latvijos ir Estijos) ankstesnius bandymus nustatyti baudžiamąją atsakomybę už

---

[104] Greenberg, B. A. Rethinking Technology Neutrality. *Minnesota Law Review*, 2016, 100(1495): 1526.

[105] Downing, R. W. Shoring up the Weakest Link: What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. *Columbia Journal of Transnational Law*, 43(3): 716.

[106] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 60.

disponavimą kenkimo programine įranga. Šių valstybių baudžiamuosiuose įstatymuose įtvirtinus kompiuterinio viruso[107] terminą, liko nekriminalizuotas, pavyzdžiui, Trojos arklių (angl. *Trojan horse)* ir kitų kenkimo programų kūrimas bei platinimas[108]. Tam tikrų nesklandumų neišvengta ir Lietuvos baudžiamajame įstatyme nustatant atsakomybę už nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui. 2003 m. įsigaliojus naujajam BK, jo XXX skyriuje aprašant nusikalstamas veikas vartotas terminas *kompiuterinė informacija*, taip paliekant neaiškumų, ar terminai *informacija* ir *duomenys*, anot įstatymo leidėjo, turėjo būti laikomi sinonimais, ar iš tikrųjų tarp jų buvo sąmoningai daromas skirtumas. Atskirti šiuos terminus yra gana svarbu[109], taigi mokslinėje literatūroje vis dėlto buvo daroma prielaida, kad šių terminų skirtumo įstatymo leidėjas tuo metu neįžvelgė, atitinkamai jie vartotini kaip sinonimai[110].

3.2. Technologinio neutralumo principo taikymo sunkumai baudžiamojoje teisėje ir galimi jų įveikimo būdai

Užtikrinus technologijoms neutralų teisinį reguliavimą, inkriminuojant nusikalstamas veikas elektroninėje erdvėje neturėtų kilti sunkumų dėl informacinių technologijų, taikomų kaip nusikalstamos veikos priemonė ar įrankis, galinčių būti nusikalstamos veikos dalyku ir pan., įvairovės bei šių technologijų pokyčių. Viena vertus, toks požiūris iš tiesų padeda išspręsti gana daug teisėkūros ir teisės normų aiškinimo problemų, kita vertus, kelia ir nemažai technologinio neutralumo praktinio įgyvendinimo klausimų. Baudžiamosios teisės srityje bene

[107] Kompiuterinis virusas yra tik viena iš kenkimo programinės įrangos (angl. *malicious software)* rūšių (plačiau žr. Computer and Information security handbook. Vacca, J. R. (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 56–57).

[108] Štitilis, D. Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: LTU, 2002, p. 145.

[109] Informacinių sistemų vartotojui elektroniniai duomenys gali būti nematomi ir nesuprantami (pavyzdžiui, duomenų apdorojimo ar jų perdavimo procese), o informacija jie tampa tada, kai įgyja tam tikrą prasmę (plačiau žr. Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008, p. 7–8).

[110] Civilka, M., *et al*. Informacinių technologijų teisė. Vilnius: NVO teisės institutas, 2004, p. 529.

svarbiausi iš jų būtų šie: *pirma*, kaip užtikrinti technologijoms neutralų nusikalstamos veikos sudėties požymių aprašymą ir interpretavimą; *antra*, kaip pasiekti, kad toks technologijoms neutralus reglamentavimas būtų suderinamas su baudžiamojoje teisėje svarbiais legalumo ir teisinio tikrumo principais.

Atsakymą į pirmąjį klausimą galima rasti remiantis teisėkūros lygmeniu – technologijoms neutralių požymių įtvirtinimas BK straipsnio dispozicijose suteikia galimybę šiuos požymius taip interpretuoti ir praktikoje. Taigi neutralumas technologijų atžvilgiu įgyvendinamas tinkamai parenkant bendruosius informacines technologijas apibrėžiančius terminus (pavyzdžiui, informacinė sistema, šios sistemos apsaugos priemonės, elektroniniai duomenys) ir vėliau atitinkamai juos aiškinant. Technologinį neutralumą teisėkūros lygmeniu leidžia užtikrinti ne konkrečios rūšies technologijų nustatymas, o „plačios, atviros tekstūros terminai, kurie nusako tikslus, poveikį, funkcijas ir kitas bendrąsias savybes“[111]. Jeigu nusprendžiama formuluoti sąvokas, pasirinktinos „į funkcijas nukreiptos definicijos, kurios, į jas neįtraukus užuominų apie pačias technologijas, būtų priklausomos tik nuo funkcijas žyminčių sąvokų“[112]. Iš tiesų sudėtinga nuspėti, „kaip atrodys kita technologijų karta“[113], todėl baudžiamajame įstatyme numatytų su informacinėmis technologijomis susijusių sudėties požymių aiškinimas teisės taikymo lygmeniu turėtų būti orientuojamas į technologijų funkcionavimo ypatybes, o ne pačias technologijas. Taikant tokią baudžiamojo įstatymo normų kūrimo ir aiškinimo strategiją, būtų galima išvengti galimų baudžiamosios teisės spragų reikšmingai pakitus vienai ar kitai technologijai.

Vienas iš tokios definicijos pavyzdžių – Konvencijos dėl elektroninių nusikaltimų 1 straipsnyje pateikiamas kompiuterinės sistemos apibrėžimas. Juo remiantis, „kompiuterinė sistema – tai įtaisas arba tarpusavyje sujungtų ar susijusių įtaisų grupė, iš kurių vienas ar dau-

---

111 Ohm, P. The Arguments against Technology-Neutral Surveillance Laws. *Texas Law Review*, 2010, 88(7): 1687.

112 Van der Haar, I. M. Technological Neutrality: What Does It Entail? [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=985260*>.

113 Linford, J. Improving Technology Neutrality through Compulsory Licensing. *Minnesota Law Review*, 2016, 100 (126): 132–133.

giau pagal programą automatiškai apdoroja duomenis“[114]. Konvencijos aiškinamosios ataskaitos 23 punkte šis apibrėžimas dar detalizuojamas: „Konvencijoje kompiuterinė sistema yra prietaisas, sudarytas iš aparatinės ir programinės įrangos, sukurtos apdoroti skaitmeninius duomenis. Jis gali apimti įvesties, išvesties ir saugojimo priemones. Jis gali būti vienas arba sujungtas tinklu su kitais panašiais prietaisais.“[115] Kaip matyti, minėtojoje konvencijoje pateikiamu kompiuterinės sistemos apibūdinimu nebuvo siekiama visiškai išspręsti šios sąvokos apibrėžties problemos – kompiuterinė sistema apibrėžiama remiantis gana abstrakčiais požymiais ir jos atliekamomis funkcijomis. Be kita ko, Konvencijos dalyvėms suteikta diskrecija atsisakyti pažodžiui įgyvendinti šias nuostatas (22 punktas)[116]. Tokia kompiuterinės sistemos apibrėžtimi yra grindžiama ir Direktyvos 2013/40/ES 1 straipsnio a punkte pateikta informacinės sistemos sąvoka[117]. Pagal direktyvą, informacinė sistema – tai „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą atlieka automatinį kompiuterinių duomenų tvarkymą, taip pat kompiuteriniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugos ir priežiūros tikslais“.

Vis dėlto iš pirmo žvilgsnio gana pažangi idėja informacinių technologijų aiškinimą sieti su jų atliekamomis funkcijomis, o ne konkrečiomis technologijomis, baudžiamosios teisės srityje galėtų sulaukti ir kritikos. Esant tokioms abstrakčioms sąvokoms sudėtinga nustatyti baudžiamosios teisės veikimo ribas, todėl aiškiai neapibrėžto turinio požymiai gali kelti abejonių dėl jų atitikties legalumo ir teisinio tikrumo principų reikalavimams. Vienas iš legalumo principo aspektų yra siejamas su maksimaliu nusikalstamos veikos požymių aprašymo tikslumu ir aiškumu[118]. Išsamaus, tikslaus ir aiškaus nusi-

[114] Europos Tarybos konvencija dėl elektroninių nusikaltimų. *Valstybės žinios*, 2004, Nr. 36-1188.

[115] The Explanatory Report to the Convention on Cybercrime [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: *<http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>*.

[116] *Ibid*.

[117] Informacinės sistemos dalimi laikomi ir kompiuteriniai duomenys.

[118] Fedosiuk, O. Baudžiamoji atsakomybė kaip kraštutinė priemonė *(ultima ratio)*: teorija ir realybė. *Jurisprudencija*, 2012, 19(2): 726.

kalstamos veikos teisinio apibūdinimo reikalavimai, be kita ko, kyla ir iš teisinės valstybės principo[119], kurio įvairūs turinio aspektai ir iš jo išvedamo teisinio saugumo imperatyvai yra suformuluoti Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje: *įstatymuose ir kituose teisės aktuose nustatytas teisinis reguliavimas turi būti aiškus, suprantamas, neprieštaringas, teisės aktų formuluotės turi būti tikslios, turi būti užtikrinami teisės sistemos nuoseklumas ir vidinė darna <...>; <...> teisės pažeidimai, už kuriuos teisės aktuose yra nustatyta atsakomybė, turi būti aiškiai apibrėžti; nustatant teisinius apribojimus bei atsakomybę už teisės pažeidimus privalu paisyti protingumo reikalavimo, taip pat proporcingumo principo* <...> (Konstitucinio Teismo 2004 m. gruodžio 13 d., 2004 m. gruodžio 29 d., 2005 m. rugsėjo 29 d., 2006 m. sausio 16 d. ir kiti nutarimai).

Jau minėta, kad Konvencijoje dėl elektroninių nusikaltimų ir Direktyvoje 2013/40/ES yra pateiktas gana abstraktus ir į sistemos funkcijas (automatinį duomenų apdorojimą) orientuotas informacinės (kompiuterinės) sistemos apibrėžimas. Dėl tokio suvokimo ji turi labai daug bendro su visomis informacinėmis technologijomis, nes visos jos yra skirtos duomenims ar informacijai apdoroti – „kelyje nuo pradinių duomenų iki reikiamų rezultatų gavimo visos atliekamos procedūros vienaip ar kitaip apdoroja jiems pateiktus duomenis“[120]. Būtent dėl tokio dviprasmiškumo nusikalstamų veikų elektroninėje erdvėje požymių ribos ir apskritai jų suvokimas, neatsižvelgiant į įstatymo leidėjo tikslus formuluojant vieną ar kitą nusikalstamų veikų sudėtį, gali būti kaskart skirtingas. Minėtąjį technologijų ir terminologijos problemos aspektą galima įžvelgti ir doktrinoje – technologijoms neutralios nuostatos „padeda išvengti pernelyg siauro reguliavimo, leisdamos pernelyg platų“[121]. Iš tiesų nėra paprasta pateikti apibrėžimą, kuris, pavyzdžiui, leistų kalbėti ne apie kišeninį skaičiuotuvą, o būtent apie kompiuterį[122]. Dėl to remiantis technologijoms

[119] Švedas, G. Veikos kriminalizavimo kriterijai: teorija ir praktika. *Teisė*, 2012, 82: 21.

[120] Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008, p. 166.

[121] Ohm, P. The Arguments against Technology–Neutral Surveillance Laws. *Texas Law Review*, 2010, 88(7): 1686.

[122] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 54.

neutraliu reguliavimu nustatomos neaiškios ribos – „*pusšešėlis*, kur interpretacija yra sunkiausia, nes neaišku, ar teisės norma turėtų būti išvis taikoma“[123].

Susiklosto įdomi padėtis, kai didėjant informacines technologijas taikančių asmenų skaičiui ir prietaisų, kuriais naudojantis galima atlikti įvesties, išvesties ir duomenų apdorojimo funkcijas, įvairovei, kyla sunkumų nustatant, ką iš tikrųjų galima laikyti informacine sistema (kompiuteriu). Šiuo požiūriu būtina pabrėžti, kad kiekviena nauja informacinių technologijų karta neišvengiamai keičia minėtųjų technologijų sampratą ir jų taikymo galimybes bei atitinkamai verčia naujai pažvelgti į nusikalstamų veikų elektroninėje erdvėje sudėties požymius ir jų turinį. Pavyzdžiui, dėl mobiliųjų technologijų, galinčių atlikti minėtąsias funkcijas ir būti tinklo dalimi (susiejus dvi – mobiliojo ryšio ir tinklo – technologijas), pripažinimo informacine sistema neturėtų kilti abejonių[124]. Informacinių technologijų poreikis lėmė informacinių sistemų integravimą į gaminius, kurie iki tol galėjo būti panaudojami ir be jų. „Skaitmeninis kontekstas, kuris funkcionuoja *daiktuose*, yra visur: automobiliuose, šaldytuvuose, gyvūnuose ir net žmogaus kūne kaip dalis implantuojamų medicininių prietaisų.“[125] Tokių prietaisų, galinčių atlikti minėtąsias funkcijas, kaip informacinės sistemos pripažinimo irgi nereikėtų ginčyti. Sparti informacinių technologijų raida, įvairių prietaisų kompiuterizavimo tendencijos lėmė, kad tam tikros ateities įžvalgos[126] jau yra tapusios realybe – sukūrus namų apyvokos prietaisus su įmontuojamomis sistemomis ir prieiga prie interneto, suteikiančia išplėstinių jų nuotolinio valdymo galimybių, atsirado visiškai naujų nusikalstamo elgesio formų. Dėl šios priežasties klausimas, kas yra, ir priešingai – kas nėra informacinė sistema, neturėtų būti sprendžiamas paskubomis, neįvertinus sistemos atliekamų funkcijų sudėtingumo ir paskirties, jos pritaikymo galimybių, poveikio jai pavojingumo bei kitų svarbių aplinkybių.

---

[123] Linford, J. Improving Technology Neutrality through Compulsory Licensing. *Minnesota Law Review*, 2016, 100(126): 129.

[124] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 16.

[125] Madison, M. J. Authority and Authors and Codes. *The George Washington Law Review*, 2016, 84: 1619.

[126] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 16.

Remiantis technologinio neutralumo principu galima teigti, kad teisinis reguliavimas yra ne tik abstraktus teisėkūros metu esančių technologijų atžvilgiu, bet ir susijęs su galimomis jų ateities perspektyvomis. Technologinis neutralumas skatina kurti normas, „kurios yra pernelyg viską apimančios ir mažai pasakančios apie nenumatytas technologijas“[127]. Kadangi toks teisinis reguliavimas yra susijęs ir su tomis technologijomis, kurių išradimas ar raida iš anksto negali būti numatyta, vadinasi, ribiniais minėtųjų technologijų taikymo atvejais gali kilti klausimų dėl jo atitikties legalumo ir teisinio tikrumo principams. Beje, ši technologinio neutralumo problema yra aktuali ne tik tais atvejais, kai įstatymų leidėjas nenumato autentiško su technologijomis susijusių sąvokų išaiškinimo (kaip tai padaryta Lietuvos BK), bet ir tada, kai toks aiškinimas yra pateikiamas įstatymuose. Juose numatytos sąvokos dėl technologinio neutralumo principo taikymo vis dar išlieka gana abstrakčios ir neįmanoma tiksliai nustatyti jų ribų. Kaip tokios problemos ir jos sprendimo pavyzdį galima pateikti Jungtinių Amerikos Valstijų apeliacinio teismo (7-osios apygardos) 2005 m. balandžio 18 d. sprendimą byloje *Jungtinės Amerikos Valstijos prieš Mitrą (US v. Mitra)*[128], kuriuo kaltininkas buvo nuteistas pagal Jungtinių Amerikos Valstijų įstatymų sąvado 18 dalies (Nusikaltimai ir baudžiamasis procesas) 1030 paragrafo a dalies 5 punktą (18 U.S.C. § 1030 (a) (5)[129] už tyčinį įsikišimą į kompiuterinės sistemos darbą:

Kaltininkas neteisėtam Smartnet II sistemos valdymui, jos veikimo analizei ir signalo, kuris perėmė sistemos kontrolę, siuntimui naudojo aparatinę ir programinę įrangą sudarantį prietaisą. Smartnet II kompiuterinė radijo sistema (žinoma kaip „radialinė sistema“ (angl. trunking system) naudota policijai, gaisrinei, greitajai pagalbai ir kitiems kritiniams atvejams. Laikotarpiu tarp 2003 metų sausio–rugpjūčio mėnesių Smartnet II sistema tapo neprieinama jos naudotojams dėl stipraus visus

---

[127] Greenberg, B. A. Rethinking Technology Neutrality. *Minnesota Law Review*, 2016, 100(1495): 1562.

[128] *United States v. Mitra*, no. 04-2328, April 18, 2005-US 7th Cir. [interaktyvus. Žiūrėta 2018-04-14]. Prieiga per internetą: <*http://caselaw.findlaw.com/us-7th-circuit/1031818.html*>.

[129] The Code of the United States [interaktyvus. Žiūrėta 2018-04-14]. Prieiga per internetą: <*http://www.law.cornell.edu/uscode/text/18/1030*>.

miesto ryšių bokštus „perdengusio“ signalo. Vėliau vietoj sistemos blokavimo kaltininkas kiekvieną pasibaigusį jos naudotojų pokalbį papildydavo erotine moters dejone.

Nesutikdamas su prokuroro nuomone, jog Smartnet II yra kompiuteris[130]*, kaltininkas teigė, kad jo veiksmais buvo sutrikdyta tik radijo sistema. Anot jo, jei radijo sistema yra kompiuteris, tuomet kiekvienas telefonas ar „iPod'as“, kiekviena bevielio ryšio stotis kavinėse ir daugelis kitų prietaisų turėtų būti laikoma kompiuteriu. Toks aiškinimas būtų pernelyg platus, taip pat jo tokio nebuvo įmanoma numatyti priimant minėtąsias nuostatas.*

Vis dėlto teismas, akcentuodamas itin spartų technologijų vystymąsi, atmetė tokius kaltininko argumentus. Teismo manymu, nors įstatymų leidėjas galėjo ir nežinoti apie radialinę sistemą, jis, suvokdamas moderniame pasaulyje vykstančius pokyčius, nustatė bendrojo pobūdžio normas, o ne konkrečių uždraustų veikų sąrašą. Kuo daugiau prietaisų, teismo nuomone, turės dirbtinį intelektą, tuo labiau plėsis numatytų nuostatų apimtys. Nors tokia tendencija gali būti užuomina peržiūrėti reguliavimą, tačiau tai neįgalina teismo suteikti esamai nuostatai siauresnę apimtį, nei matyti pagal jos formuluotę. Teismo neįtikino kaltininko teiginiai, kad baudžiamosios normos buvo išaiškintos tokiu būdu, kurio nebuvo įmanoma tikėtis.

Šioje situacijoje komunikacinė sistema *Smartnet II* dėl savo sandaros ir atliekamų funkcijų[131] atitiko kompiuterį leidžiančius identifikuoti požymius. Vis dėlto toks atvejis rodo, kad ateityje gali kilti gana rimtų abejonių dėl informacines technologijas įvardijančių abs-

---

[130] Jungtinių Amerikos Valstijų įstatymų sąvado 18 dalies 1030 paragrafo e dalies 1 punkte kompiuteris yra apibrėžiamas kaip „elektroninis, magnetinis, optinis, elektrocheminis arba kitas greitaeigis duomenų apdorojimo prietaisas, atliekantis logines, aritmetines ar saugojimo (laikymo) funkcijas, apimantis bet kokias duomenų saugojimo (laikymo) ar komunikavimo priemones, tiesiogiai susijusias arba atliekančias veiksmus kartu su šiuo prietaisu. Kita vertus, šis terminas neapima automatinių rašomųjų mašinėlių arba rinkimo mašinų (angl. *typesetter)*, nešiojamųjų rankinių skaičiuotuvų ar kitų panašių prietaisų“. Remiantis prokuroro pateiktais argumentais, *Smartnet II* sistema turėtų būti pripažįstama kompiuteriu, nes ją, be kitų dalių, sudaro lustas (angl. *chip)*, kuris, valdymo kanalu gavęs signalą, sparčiai atlieka duomenų apdorojimo funkciją.

[131] Kompiuterio aparatinė ir programinė įranga pagal gautus signalus paskirstydavo pokalbius atviriems kanalams, taip pat susiedavo daugybinius vienetus į komunikavimo grupę, kuri leisdavo pareigūnams tarpusavyje palaikyti bendrą pokalbį.

trakčių sąvokų išaiškinimo tikslumo ir tinkamo teisės normų taikymo. Kadangi, kaip minėta, technologijoms neutralūs terminai dažniausiai yra bendrojo pobūdžio, tai ribiniais technologijų taikymo atvejais visada gali kilti abejonių dėl tinkamo neaiškios normos interpretavimo, ypač visuomenėje, kurioje informacinė sistema (kompiuteris) yra įprastas kasdienio naudojimo daiktas. Atitinkamai ši abejonė gali būti siejama su galimais legalumo ir teisinio tikrumo principų reikalavimų pažeidimais.

Dėl to, atsakant į antrąjį klausimą, šios problemos sprendimo būdai galėtų būti siejami ne tik su bandymais kuo tinkamiau apibrėžti technologijas žyminčias sąvokas. Tokiais atvejais ne mažiau svarbus yra praktinis baudžiamojo įstatymo taikymo lygmuo, t. y. teismų praktika. Kaip matyti doktrinoje, dėl technologinio neutralumo su naujosiomis technologijomis susijusių problemų sprendimas iš įstatymo leidėjo dažniausiai perduodamas teismams[132]. Būtent teismams paliekama spręsti, ar „naujoji technologija atitinka vieną ar kitą kategoriją“[133]. Dėl to galima teigti, kad tais atvejais, kai įstatymų leidėjas Lietuvos baudžiamajame įstatyme nepateikia autentiško su informacinėmis technologijomis susijusių požymių išaiškinimo, vertinimo kriterijų paieška ir sąvokos turinio bei jos ribų nustatymas paliekamas teismo diskrecijai: „apibrėždamas įstatymo tekstą tik bendromis sąvokomis, tačiau neatskleisdamas jų turinio ir nenurodydamas apibrėžties kriterijų įstatymų leidėjas neišvengiamai plačiai nubrėžia įstatymo taikymo sferą, taip tarsi išplėsdamas teismo pasirinkimo galimybes <...>.“[134] Nors kalbant apie precedentus negalima užmiršti ir teisės aiškinimo klausimus sprendžiančio teismo diskrecijos ribų, t. y. kokį turinį teismas gali suteikti su informacinėmis technologijomis susijusiems požymiams ir kokiais kriterijais vadovaudamasis jis turėtų spręsti, ar padaryta veika gali būti pripažįstama nusikalstama.

---

[132] Greenberg, B. A. Rethinking Technology Neutrality. *Minnesota Law Review*, 2016, 100(1495): 1513.

[133] Linford, J. Improving Technology Neutrality through Compulsory Licensing. *Minnesota Law Review*, 2016, 100(126): 136.

[134] Pikelis, A. Baudžiamosios teisėkūros labirintai: Lietuvos Aukščiausiojo Teismo senato nutarimas ir teismų praktika taikant Baudžiamojo kodekso 178 ir 180 straipsnius. Vilnius: Petro ofsetas, p. 46.

Dėl to, sprendžiant baudžiamosios atsakomybės už nusikalstamas veikas elektroninėje erdvėje kilimo klausimą, vienas iš kriterijų galėtų būti tos aplinkybės, kurios vertinamos kriminalizuojant nusikalstamas veikas. Jei veikos pavojingumas, baudžiamosios teisės veikimo sritis ir ribos, minėtosios teisės kaip paskutinės priemonės (lot. *ultima ratio)* ir kiti[135] pagrindai leidžia nustatyti kriminalizavimo pagrįstumą, tai jie galėtų padėti apibrėžti ir neaiškios baudžiamojo įstatymo normos taikymo ribas. Pavyzdžiui, analizuojant praktines *ultima ratio* principo taikymo galimybes, mokslinėje literatūroje pabrėžiama, kad remiantis šiuo principu būtina nustatyti tinkamą veikos pavojingumo lygį, nes abstrakčios definicijos kartu su tikrai pavojingu elgesiu gali apimti ir abejotino pavojingumo veikas[136]. Toks požiūris grindžiamas tuo, kad baudžiamasis įstatymas neturėtų būti taikomas *de minimis* pobūdžio veikoms[137].

Kitas galimas variantas – baudžiamosiose bylose, nustačius neteisėtą informacinių technologijų taikymo faktą, joms nustatyti pasitelkti specialių žinių turintį ekspertą arba specialistą. Eksperto (specialisto) technikos žinios gali padėti apibrėžti ne tik vieno ar kito su informacinėmis technologijomis susijusio termino turinį, apibūdinti pritaikytas technologijas ir jų funkcijas, atskleisti nusikalstamos veikos elektroninėje erdvėje padarymo mechanizmą, bet ir turėti įtakos kvalifikuojant nusikalstamą veiką[138]. Nors vertinant ekspertizės akte (specialisto išvadoje) pateikiamas išvadas, turėtų būti atsižvelgiama į tai, kad jos yra tik teisinės išvados prielaida, nes nustatyti nusikalstamos veikos sudėties požymius yra teismo, o ne ekspertų (specialistų), kompetencija. Kasacinėje praktikoje ne kartą buvo pabrėžta, kad *bylą nagrinėjančio teismo kompetencija nuspręsti, kurie iš byloje esančių duomenų atitinka visus įstatymo reikalavimus ir turi įrodomąją vertę bei kokios išvados jais remiantis darytinos, taip pat ar byloje surinktų įrodymų pakanka nustatyti, ar asmens, kuriam ši veika inkriminuojama,*

[135] Švedas, G. Veikos kriminalizavimo kriterijai: teorija ir praktika. *Teisė*, 2012, 82: 12–24.

[136] Fedosiuk, O. Baudžiamoji atsakomybė kaip kraštutinė priemonė *(ultima ratio)*: teorija ir realybė. *Jurisprudencija*, 2012, 19 (2): 733.

[137] Tompkins, Jr.; Mar, L. A. The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem. *Computer Law Journal*, 1986, 6(3): 463.

[138] Baudžiamasis procesas: nuo teorijos iki įrodinėjimo (prof. Eugenijaus Palskio atminimui): mokslo studija. Vilnius: Mykolo Romerio universiteto leidykla, 2011, p. 385.

veiksmai turi visus konkrečios nusikalstamos veikos sudėties požymius. Įrodymų vertinimas ir jais pagrįstų išvadų byloje sprendžiamais klausimais darymas yra teismo, priimančio baigiamąjį aktą, prerogatyva[139]. Tokia pozicija svarbi ta prasme, kad remiantis eksperto (specialisto) išvada panaudotą prietaisą priskyrus informacinėms technologijoms, to neturėtų pakakti nusprendžiant, kad nusikalstama veika padaryta elektroninėje erdvėje. Šis saugiklis yra susijęs su nusikalstamos veikos sudėties kaip baudžiamosios atsakomybės pagrindo principu (BK 2 straipsnio 4 dalis), įpareigojančiu nustatyti sudėties požymių visumą, o ne teikti prioritetą kuriam nors vienam iš jų. Be abejo, tokiais atvejais išlieka aktualūs ir minėtieji *ultima ratio* bei kiti svarbūs kriterijai, kaip tinkamai taikyti baudžiamąjį įstatymą.

Nusikalstamoms veikoms elektroninėje erdvėje kvalifikuoti ne mažiau svarbios ir šių nuostatų priėmimo aplinkybės, t. y. pagrindinės priežastys, lėmusios atitinkamo požymio įtvirtinimą normoje, taip pat svarbiausi tikslai, kurių buvo siekiama nustatant normą BK. Ne veltui mokslinėje literatūroje pabrėžiama, kad tik „tokiu būdu galima kiek įmanoma tiksliau suvokti įstatymo leidėjo ketinimus ir tikslus, įstatymo turinį ir optimaliausias jo veikimo galimybes“[140]. Dėl to nustačius visas baudžiamajai atsakomybei kilti būtinas sąlygas, „nėra priežasties veikos nelaikyti nusikalstama vien tik dėl to, kad pagal įprastą suvokimą naudojamas prietaisas nėra apibūdinamas kaip kompiuteris“[141]. Ir priešingai – praktikoje galimi atvejai, kai pritaikytoji priemonė pagal atliekamas funkcijas galėtų būti priskiriama informacinėms technologijoms, bet pati padaryta veika nelaikoma nusikalstama (nes, pavyzdžiui, baudžiamojo įstatymo taikymas neatitinka pagrindinių baudžiamosios teisės principų, nenustatyta kitų sudėties požymių)[142].

---

[139] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2018 m. vasario 6 d. nutartis baudžiamojoje byloje Nr. 2K-9-719/2018.

[140] Pikelis, A. Baudžiamosios teisėkūros labirintai: Lietuvos Aukščiausiojo Teismo senato nutarimas ir teismų praktika taikant Baudžiamojo kodekso 178 ir 180 straipsnius. Vilnius: Petro ofsetas, p. 45.

[141] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 57.

[142] Marcinauskaitė, R. Technologinio neutralumo principo taikymo problemos aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymius. *Socialinių mokslų studijos*, 2013, 5(1): 375–377.

Taigi technologinio neutralumo principas yra aktualus siekiant išvengti baudžiamojo įstatymo normų taikymo apribojimų, galinčių atsirasti dėl jose esančių su technologijomis susijusių požymių. Kita vertus, kai šis principas taikomas baudžiamojoje teisėje, jo turinys neišvengiamai susiaurėja dėl baudžiamosios teisės principų, leidžiančių išvengti pernelyg plataus ir nepagrįsto veikų kriminalizavimo, atitinkamai ir nepagrįsto baudžiamosios atsakomybės ribų išplėtimo.

Kompiuterių tinklas ar internetas gali būti suprantamas kaip daugiau ar mažiau „įsivaizduojamas“, t. y. turintis metaforiškai aiškius arba miglotus takus, pakraščius, sritis, viršūnes ir riboženklius.

Michaelis J. Madisonas

II SKYRIUS

NETEISĖTAS PRISIJUNGIMAS PRIE INFORMACINĖS SISTEMOS (BK 198[1] STRAIPSNIS)

II SKYRIAUS TURINYS

1. Bendrieji neteisėto prisijungimo prie informacinės sistemos kriminalizavimo ypatumai

Baudžiamosios atsakomybės už neteisėtą prisijungimą prie informacinės sistemos kaip atskiros veikos nustatymas gali būti siejamas su Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje nurodomomis priemonėmis, kurių turėtų būti imtasi „ankstyvajame etape", kol sistemoje dar neįvykdytos kitos nusikalstamos veikos (45 punktas). Kaip teigiama doktrinoje, ši veika – tai „baudimo už „nutolusią" žalą, kurios kilimas priklauso nuo kaltininko ar kito asmens būsimo sprendimo padaryti nusikaltimą, pavyzdys"[143]. Vadinasi, neteisėto prisijungimo prie informacinės sistemos kriminalizavimas vertinamas kaip viena iš priemonių, galinčių padėti užkirsti kelią paskesnėms sistemoje padaromoms nusikalstamoms veikoms[144]. Iš tiesų dėl neteisėto įsibrovimo į sistemą gali atsirasti galimybė gauti prieigą „prie konfidencialių duomenų (įskaitant slaptažodžius, informaciją apie sistemą) ir paslapčių, nemokamai naudotis sistema arba paskatinti programišius (angl. *hacker)* padaryti daug pavojingesnių su kompiuteriais susijusių nusikaltimų, pavyzdžiui, sukčiavimo ar klastojimo veikų" (44 punktas). Be to, tokio kriminalizavimo pagrindimas, remiantis ekvivalentinio vertinimo principu, gali būti išvedamas iš baudžiamojo įstatymo normų, kuriomis numatoma atsakomybė už „neteisėtą įėjimą į pastatą nesukeliant žalos"[145]. Nors neteisėto prisijungimo veika tam tikru požiūriu ir yra panaši, pavyzdžiui, į neteisėtą asmens būsto neliečiamumo pažeidimą, bet pastarosios veikos sudėties, kad ir kaip plačiai aiškinamos, negalima pritaikyti šiai specifinei veikai elektroninėje erdvėje kvalifikuoti. Atsižvelgiant į tai, Lietuvos BK XXX skyriuje kaip *delicta sui generis* kriminalizuotas neteisėtas prisijungimas prie informacinės sistemos (BK 198[1] straipsnis).

---

[143] Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 2011, 22: 161.

[144] Comprehensive Study on Cybercrime. UNODC, 2013, p. 83 [interaktyvus. Žiūrėta 2018-05-01]. Prieiga per internetą: <*http://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html*>.

[145] Sciglimpaglia, R. J. Computer Hacking: A Global Offense. *Pace International Law Review*, 1991, 3(199): 246.

Tiesa, įsigaliojus 2000 m. BK, iš pradžių ši veika jame nebuvo numatyta, dėl to kilo abejonių, ar informacinių sistemų konfidencialumo apsauga elektroninėje erdvėje yra pakankama. Ši baudžiamojo teisinio reguliavimo nepakankamumo problema buvo išspręsta 2004 m. Lietuvai ratifikavus Konvenciją dėl elektroninių nusikaltimų ir įgyvendinus jos nuostatas nacionalinėje teisėje – BK 198[1] straipsnyje neteisėto prisijungimo prie kompiuterio ar kompiuterių tinklo veika (tuo metu taip vadinama) buvo įtvirtinta kaip minėtosios konvencijos 2 straipsnyje aprašytos neteisėtos prieigos atitikmuo. Vėlesnius jos pakeitimus lėmė Pamatinio sprendimo 2005/222/TVR ir Direktyvos 2013/40/ES nuostatų perkėlimas į nacionalinę teisę. Atsižvelgiant į Pamatinio sprendimo 2005/222/TVR 2 straipsnį, 2007 metais BK 198[1] straipsnyje vietoj kompiuterio ar kompiuterių tinklo įvestas kur kas abstraktesnis informacinės sistemos terminas ir nurodyta šią veiką kvalifikuojanti aplinkybė, susijusi su didesne informacinės sistemos svarba, – jos strategine reikšme nacionaliniam saugumui, didele reikšme valstybės valdymui, ūkiui ar finansų sistemai. 2015 metais, įgyvendinus Direktyvos 2013/40/ES 3 straipsnio nuostatas, BK 198[1] straipsnyje buvo sukonkretinta aplinkybė, kad neteisėtas prisijungimas yra galimas ir prie informacinės sistemos, ir prie jos dalies. Be to, buvo sugriežtinta šio BK straipsnio 1 dalies sankcija (bet minėtoji veika ir toliau liko kaip nesunkus nusikaltimas). Kadangi šiai veikai atsirasti ir tolesniems jos pokyčiams baudžiamajame įstatyme įtakos turėjo minėtieji teisės aktai, ir objektyvieji, ir subjektyvieji neteisėto prisijungimo prie informacinės sistemos požymiai aiškintini turint mintyje Konvencijos dėl elektroninių nusikaltimų ir Pamatinį sprendimą 2005/222/TVR pakeitusios Direktyvos 2013/40/ES nuostatas.

Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje įpareigojama nustatyti baudžiamąją atsakomybę už sąmoningą neteisėtą prieigą prie visos kompiuterinės sistemos arba jos dalies. Šiame straipsnyje numatyta galimybė susiaurinti gana plačią tokios veikos apibrėžtį, į nusikalstamos veikos sudėtį įtraukiant vieną arba kelis alternatyvius požymius – jei veika padaryta pažeidžiant apsaugos priemones, jei ja buvo ketinta gauti kompiuterinius duomenis arba buvo nustatytas kitas nesąžiningas ketinimas ir dar, jei veika yra nukreipta prieš kompiuterinę sistemą, sujungtą su kita tokia sistema. Direktyvos 2013/40/ES 3 straipsnyje ši nusikalstama veika apibrėžiama kaip prieiga prie visos

informacinės sistemos arba kurios nors jos dalies neturint tam teisės, jei tai buvo padaryta tyčia pažeidžiant apsaugos priemonę, bent tais atvejais, kurie nevertinami kaip mažareikšmiai. Taigi įtvirtinti papildomi šios veikos sudėties požymiai, kuriais remiantis apibūdinamas, pavyzdžiui, neteisėtos prieigos gavimo būdas (apsaugos priemonių pažeidimas), nusakomi kaltininko tikslai (ketinimas gauti elektroninius duomenis ar kiti nesąžiningi tikslai) gali padėti užtikrinti baudžiamajai atsakomybei kilti būtiną šios veikos pavojingumo lygį, todėl laikytini racionaliais reikalavimais pripažįstant tokią veiką kaip nusikalstamą. Tokiu būdu nustačius „potencialų veikos plotį“[146], suteikiama galimybių formuotis įvairioms neteisėtos prieigos koncepcijoms, rodančioms skirtingą valstybių požiūrį į šią nusikalstamą veiką. Pasirinkti gana įvairūs tokios nusikalstamos veikos kriminalizavimo būdai lėmė skirtingas neteisėtos prieigos inkriminavimo problemas, taigi ir skirtingą mokslininkų požiūrį į šią veiką. Toks pastebėjimas yra svarbus analizuojant įvairias doktrinoje pateikiamas idėjas ir bandant spręsti nacionalinėje baudžiamojoje teisėje kylančias minėtosios veikos aiškinimo problemas.

Atsižvelgiant į pasirinktą neteisėtos prieigos prie informacinės sistemos koncepciją, užsienio valstybių teisėje galima rasti įvairių šios nusikalstamos veikos sudėties požymių derinimo būdų, atitinkamai ir skirtingų tokios veikos perteklinio kriminalizavimo problemos sprendimo variantų. Vienos iš dviejų svarbiausių – galutinio tikslo ar priemonės (angl. *„ends“ and „means“ approach)*[147] – koncepcijų pasirinkimą lemia požiūris, ar tolesni kaltininko veiksmai sistemoje, neteisėtai į ją įsibrovus, yra svarbūs sprendžiant dėl jo baudžiamosios atsakomybės. Vadovaujantis *galutinio tikslo* koncepcija, kaltininko neteisėtai atliekami veiksmai sistemoje yra svarbesni už būdą, kuriuo jis gavo prieigą prie jos. Dėl tokio požiūrio būtų galima iš dalies paneigti ir paties neteisėto prisijungimo kriminalizavimo poreikį, nes kaltininko baudžiamoji atsakomybė kiltų už tas nusikalstamas veikas, kurias jis padarė pačioje sistemoje, neteisėtai prie jos prisijungęs. *Priemonės* koncepcija, priešingai – yra orientuojama į patį prieigos prie sistemos gavimo faktą,

[146] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 48.

[147] Sciglimpaglia, R. J. Computer Hacking: A Global Offense. *Pace International Law Review*, 1991, 3(199): 213.

neatsižvelgiant į tai, kokių neteisėtų veiksmų kaltininkas ėmėsi jau pačioje sistemoje ar kokių galutinių tikslų jis siekė. Šis požiūris, be kita ko, itin aktualus tais atvejais, kai yra nustatomas tik neteisėtos prieigos faktas, o ne kaltininko neteisėti veiksmai sistemoje ar siekis juos atlikti.

Kai kuriose valstybėse baudžiamoji atsakomybė yra numatyta už neteisėtą prieigą ne prie informacinės sistemos, o prie, pavyzdžiui, duomenų, jeigu buvo padarytas neteisėtas poveikis apsaugos priemonėms arba pačiai sistemai. Tokiu atveju neteisėtos prieigos veika tampa kitos, pavyzdžiui, neteisėtos prieigos prie duomenų, veikos sudedamąja dalimi. Kaip antai Vokietijos baudžiamajame įstatyme su neteisėta prieiga yra susijęs 202a straipsnis, kuriame kriminalizuotas duomenų šnipinėjimas. Ši veika apibūdinama kaip duomenų, apsaugotų nuo neteisėtos prieigos, įgijimu įveikiant apsaugą. Jungtinėje Karalystėje neteisėtos prieigos veika numatyta Netinkamo naudojimosi kompiuteriais akto[148] 1 straipsnyje. Minėtoji veika aprašyta kaip kompiuterio privertimas atlikti kokią nors funkciją siekiant gauti prieigą prie programos arba jame laikomų duomenų, arba sudarant sąlygas tokią prieigą gauti. Kita vertus, įtvirtinus minėtąjį reikalavimą nustatyti ne tik informacinės sistemos konfidencialumo pažeidimą, bet ir kitas paskesnes kaltininko padarytas nusikalstamas veikas sistemoje (ar ja naudojantis), gali būti susiduriama su visų padarytų nusikalstamų veikų atribojimo problema. Tokiais atvejais gali kilti painiavos „dėl neteisėto prisijungimo ir tokių veikų kaip įsikišimas į duomenis ar duomenų šnipinėjimas ribų nustatymo“[149].

Kitose valstybėse atsakomybė tiesiogiai numatyta už neteisėtą prieigą prie informacinės sistemos, be neteisėtumo ir prieigos gavimo požymių, įtvirtinant ir kitas įvairias šios veikos pavojingumą rodančias aplinkybes. „Grynam“ arba „paprasčiausiam“[150] neteisėtam prisijungimui prie informacinės sistemos „nereikia, kad kaltininkas gautų

---

148 Computer Misuse Act [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://www.legislation.gov.uk/ukpga/1990/18/section/1*>.
Jungtinė Karalystė Konvenciją dėl elektroninių nusikaltimų ratifikavo 2011 m. gegužės 20 d.

149 Comprehensive Study on Cybercrime. UNODC, 2013, p. 83 [interaktyvus. Žiūrėta 2018-05-01]. Prieiga per internetą: <*http://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html*>.

150 *Ibidem*.

prieigą prie sistemos failų ar kitų sistemoje laikomų duomenų“[151], bet į šias aplinkybes gali būti atsižvelgiama formuojant kvalifikuotą neteisėtos prieigos prie informacinės sistemos sudėtį. Pavyzdžiui, neteisėtos prieigos veika yra kriminalizuota Prancūzijos baudžiamojo įstatymo 323-1 straipsnyje. Ji aprašyta kaip apgaulingas priėjimas prie visos ar dalies automatinės duomenų apdorojimo sistemos arba pasilikimas joje. Poveikis, daromas sistemoje esantiems duomenims arba pačios sistemos veiklai, yra laikomas šią veiką kvalifikuojančiomis aplinkybėmis. Estijos baudžiamajame įstatyme[152] neteisėtas naudojimasis kompiuterine sistema yra kriminalizuotas 217 straipsnyje. Pagal šį straipsnį, baudžiamoji atsakomybė kyla, jei nustatoma neteisėta prieiga prie kompiuterių sistemos pašalinant arba apeinant jos apsaugos priemones. Be to, šio straipsnio 2 dalyje įtvirtinta nemažai tokią veiką kvalifikuojančių aplinkybių, pavyzdžiui, didelės žalos padarymas, prieiga prie svarbaus sektoriaus kompiuterinės sistemos ir pan. Šiai valstybių grupei galėtų būti priskirta ir Lietuva, kurios BK 198[1] straipsnyje baudžiamoji atsakomybė yra numatyta už neteisėtą prisijungimą prie informacinės sistemos pažeidžiant jos apsaugos priemones. Tam tikri neteisėto prisijungimo atvejai (pavyzdžiui, naudojimasis svetimais asmens duomenimis[153]) taip pat numatyti kaip neteisėtą poveikį elektroniniams duomenims (BK 196 straipsnio 2 dalis) ir neteisėtą poveikį informacinei sistemai (BK 197 straipsnis) kvalifikuojanti aplinkybė.

Analizuojant Lietuvos BK 198[1] straipsnyje įtvirtintą neteisėto prisijungimo prie informacinės sistemos veiką matyti, kad jos apibrėžtis yra susiaurinta Konvencijoje dėl elektroninių nusikaltimų ir Direk-

---

151 *Ibidem*.

152 Penal Code of the Republic of Estonia [interaktyvus. Žiūrėta 2018-05-02]. Prieiga per internetą: <*https://www.riigiteataja.ee/en/eli/ee/522012015002/consolide/current*>.

153 Šiuo požiūriu BK 196 ir 197 straipsnių 2015 m. pakeitimus lėmė Direktyvos 2013/40/ES 9 straipsnio 5 dalis, kurioje numatyta, kad valstybės turėtų imtis „būtinų priemonių užtikrinti, kad jei 4 ir 5 straipsniuose nurodytos nusikalstamos veikos įvykdomos piktnaudžiaujant kito asmens duomenimis siekiant įgyti trečiosios šalies pasitikėjimą, tokiu būdu padarant žalą teisėtam tapatybės turėtojui, tai pagal nacionalinę teisę būtų laikoma sunkinančiomis aplinkybėmis, išskyrus atvejį, jei tos aplinkybės jau yra taikomos kitai nusikalstamai veikai, už kurią baudžiama remiantis nacionaline teise“.

tyvos 2013/40/ES 3 straipsnyje numatytu būdu. Siekiant išvengti akivaizdžiai nežalingų veikų kriminalizavimo, šiame BK straipsnyje numatytai prieigai inkriminuoti būtina įrodyti ne tik prisijungimo prie informacinės sistemos ar jos dalies neteisėtumą, bet ir tai, kad taip buvo prisijungta pažeidžiant sistemos apsaugos priemones. Atsižvelgiant į kvalifikuotą šios veikos sudėtį, prisijungimas prie strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčios informacinės sistemos laikomas aplinkybe, didinančia neteisėto prisijungimo pavojingumo laipsnį (BK 198[1] straipsnio 2 dalis). Taip BK 198[1] straipsnyje aprašyti nusikalstamos veikos požymiai rodo, kad neteisėtas prisijungimas prie informacinės sistemos yra kriminalizuotas „kaip pavojingas pats savaime“[154] ir nesusijęs su paskesnėmis kaltininko veikomis jau pačioje sistemoje.

Įvairūs požiūriai į neteisėtos prieigos nusikalstamą veiką rodo ne tik esant jos sulyginimo sunkumų, bet ir kvalifikavimo problemų, kurių, atsižvelgiant į šios veikos požymių įtvirtinimą BK, gali kilti ne visose, o tik kai kuriose valstybėse. Vienas iš tokių akivaizdesnių atvejų yra siejamas su jau aptartais bendresniais neteisėtos prieigos kriminalizavimo skirtumais. Būtent jais remiantis ir galima spręsti, kieno – sistemos ar duomenų – konfidencialumo pažeidimai yra šios nusikalstamos veikos ašis. Kaip teigiama literatūroje, toks atskyrimas ypač svarbus, nes pirmuoju atveju „pabrėžiama kaltininko sąveika su kompiuteriu, o ne su konkrečiais duomenimis“[155]. Antruoju atveju, priešingai – svarbiausia yra nustatyti prieigos prie duomenų neteisėtumą.

Lietuvoje pasirinkus veikos kriminalizavimo variantą, artimą *priemonės* koncepcijai, be kita ko, būtina tinkamai išspręsti nusikalstamų veikų daugeto klausimus – ir įžvelgiant šią veiką tarp visų kitų kaltininko padarytų nusikalstamų veikų, ir nustatant daugeto formą. Įvertinus nusikalstamų veikų elektroninėje erdvėje padarymo mechanizmą, galima teigti, kad kaltininko veiksmai dažniausiai neapsiriboja tik neteisėta prieiga prie informacinės sistemos – į ją įsibrovus neretai yra padaroma ir kitų nusikalstamų veikų (atsižvelgiant į sistemos ypatybes,

---

[154] *Baudžiamoji justicija ir verslas: recenzuotų mokslinių straipsnių rinkinys.* Švedas, G. (vyr. red.). Vilnius: Vilniaus universiteto Teisės fakultetas, 2016, p. 278.

[155] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 72.

jos teikiamas paslaugas). Siekiant aiškiau suvokti šią problemą, reikėtų saugumo grėsmes suskirstyti į dvi kategorijas: trikdymo ir neteisėtos prieigos rūšis[156]. Antrosios atveju, kad ir koks būtų kaltininko tikslas, kenkimo veiksmai visada yra „atliekami gavus prieigą prie informacinės sistemos ir įsilaužus į jos vidų“[157]. Vadinasi, galimybių atlikti paskesnes nusikalstamas veikas jau pačioje sistemoje kaltininkas įgyja būtent dėl savo pirminių neteisėto prisijungimo veiksmų – atsižvelgiant į visą veikos padarymo mechanizmą, šis etapas dažniausiai yra neišvengiamas. Taigi iš baudžiamosios teisės pozicijų vertinant kaltininko padarytas nusikalstamas veikas, neturėtų stebinti itin dažni neteisėto prisijungimo inkriminavimo atvejai.

Pavyzdžiui, vienas iš sukčiavimo elektroninėje erdvėje etapų[158] yra susijęs su informacinės sistemos konfidencialumo pažeidimais, kai prie jos neteisėtai prisijungiama naudojantis svetimais sistemos vartotojui atpažinti suteiktais autentifikavimo duomenimis[159]. Nors šis etapas sukčiavimo atveju dažniausiai yra tarpinis, jis paprastai neišvengiamas, kaltininkui paskesniais veiksmais siekiant sistemoje atlikti neteisėtas mokėjimo operacijas. Tai, kad kaltininko veiksmai neteisėtai prisijungus prie elektroninės bankininkystės sistemos, naudojantis svetimais vartotoją identifikuojančiais duomenimis, galėtų būti kvalifikuojami ir pagal BK 198[1] straipsnį, teigiama, pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kole-

---

156 Computer and Information security handbook. Vacca, J. R. (red). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 150.

157 Česnys, A.; Juknius, J. Saugumo patikros ir etiško įsilaužimo technologijos. Kaunas: Technologija, 2011, p. 21.

158 Siekiant visapusiškai baudžiamuoju požiūriu teisiškai įvertinti sukčiavimo elektroninėje erdvėje etapus, nepakanka tik BK 182 straipsnyje numatytos sukčiavimo normos. Kadangi ši nusikalstama veika yra susijusi su įvairiais elektroninių duomenų ir informacinių sistemų saugumo pažeidimais, be BK 182 straipsnio, kaltininkui taip pat inkriminuotinos BK XXX skyriuje ir (ar) BK 215 bei 214 straipsniuose numatytos nusikalstamos veikos. Toks veikos kvalifikavimas leidžia sukčiavimą laikyti dėl informacinių technologijų pakitusia tradicine nusikalstama veika.

159 Pavyzdžiui, naudodamasis interneto banku, vartotojas gali būti autentifikuojamas vienu iš būdų – pagal vartotojo ID, nuolatinį slaptažodį ir vieną iš identifikavimo kodų kortelėje nurodytą kodą arba pagal vartotojo ID ir vienkartinį identifikavimo kodą, sugeneruotą kodų generatoriumi.

gijos 2016 m. sausio 26 d. nutartyje baudžiamojoje byloje Nr. 2K-4-507/2016)[160]:

Nagrinėjamoje byloje nustatyta, kad E. J., pažeisdamas, t. y. suklaidindamas, (duomenys neskelbtini) informacinės sistemos apsaugos priemones, įvesdamas neteisėtai įgytus nukentėjusiosios D. B. vardu išduotus internetinės prieigos duomenis — elektroninės bankininkystės vartotojo identifikavimo kodą, asmeninį prisijungimo slaptažodį, prisijungimo prie elektroninės bankininkystės banko suteiktus slaptažodžius (prisijungimo teisė buvo suteikta tik D. B., autentifikuojamai sistemoje pagal banko jai išduotus elektroninės bankininkystės vartotojo identifikavimo kodą, asmeninį prisijungimo slaptažodį, prisijungimo prie elektroninės bankininkystės banko suteiktus slaptažodžius), jungėsi prie (duomenys neskelbtini) informacinės sistemos, leidžiančios naudotis banko paslaugų teikimu internetu, paskui atliko finansines operacijas, neteisėtai panaudodamas svetimos elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenis, ir apgaule savo naudai įgijo svetimą turtą. Šie nuteistojo veiksmai, be kitų, atitinka ir BK 198[1] straipsnio 1 dalyje numatytos nusikalstamos veikos požymius.

Tokio aiškinimo tendencijų taip pat matyti žemesniosios instancijos teismų sprendimuose konstatuojant neteisėto prisijungimo prie informacinės sistemos (elektroninės bankininkystės) faktą ir sprendžiant dėl nusikalstamų veikų sutapties rūšies:

Paprastai, kai nusikalstamos veikos daromos elektroninėje erdvėje <...>, iš pradžių neteisėtai įgyjami svetimos elektroninės mokėjimo priemonės ar jos naudotojo tapatybės patvirtinimo priemonių duomenys, pakankami finansinei operacijai inicijuoti (BK 214 straipsnio 1 dalis), po to jie neteisėtai panaudojami, neteisėtai prisijungiant prie informacinės sistemos, t. y. save identifikuojant kaip teisėtą duomenų naudotoją, prisijungiama prie internetinės bankininkystės sistemos (BK 198[1] straipsnio 1 dalis) ir atliekamos neteisėtos finansinės operacijos, pinigai iš nukentėjusiojo banko sąskaitos pervedami į kitas, saugias sąskaitas arba paimami grynaisiais (BK 215 straipsnio 1 dalis) ir taip apgaule įgyjamas svetimas turtas (BK 182 straipsnis). Neteisėtas svetimos elektroninės mokėjimo priemonės ar jos naudotojo tapatybės patvirtinimo priemonių duomenų

[160] Tokios nuomonės laikytasi ir Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2012 m. birželio 26 d. nutartyje baudžiamojoje byloje Nr. 2K-375/2012.

įgijimas, laikymas, perdavimas, jų neteisėtas panaudojimas inicijuojant ar atliekant finansines operacijas, kai neteisėtai prisijungiama prie informacinės sistemos, ir svetimo turto užvaldymas apgaule, kai įgyjamas didesnės nei 5 MGL dydžio vertės turtas, jeigu visi šie veiksmai atlikti įgyvendinant bendrą sumanymą sukčiavimo būdu užvaldyti svetimą turtą, sudaro BK 214 straipsnio 1 dalies, 215 straipsnio 1 dalies, 198[1] straipsnio 1 dalies, 182 straipsnio 1 dalies numatytų nusikalstamų veikų idealią sutaptį[161].

Autentifikavimo procedūra, kaip viena iš informacinės sistemos apsaugos priemonių, būdinga ne tik elektroninei bankininkystei, bet ir kitoms įvairias elektronines paslaugas teikiančioms sistemoms (elektroninėms parduotuvėms, elektroniniam paštui, socialiniams tinklams ir kt.). Vadinasi, nustačius neteisėto prisijungimo prie minėtųjų sistemų faktą, kaltininkui inkriminuotina ir BK 198[1] straipsnyje numatyta nusikalstama veika. Pavyzdžiui, teismų praktikoje pasitaiko atvejų, kai baudžiamoji atsakomybė pagal minėtąjį BK straipsnį kilo nustačius neteisėtą prisijungimą prie interneto prekybos ir aukcionų sistemos[162], socialinio tinklalapio *Facebook* paskyros[163], elektroninio pašto paskyros[164], mokėjimo sistemos *PayPal* kliento sąskaitos[165], interneto žaidimo paskyros[166] ir kt.

Tokiais atvejais yra aktualus ir padarytų nusikalstamų veikų sutapties (realiosios ar idealiosios) nustatymo klausimas. Atsižvelgiant į idealiosios nusikalstamų veikų sutapties plėtojimo tendencijas kasacinės instancijos teismo praktikoje[167], ši sutaptis nusikalstamų veikų

---

161 Alytaus rajono apylinkės teismo 2017 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-68-297/2017.

162 Klaipėdos miesto apylinkės teismo 2009 m. birželio 29 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-740-93/2009.

163 Klaipėdos apygardos teismo 2017 m. spalio 12 d. nutartis baudžiamojoje byloje Nr. 1A-279-651/2017.

164 Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2015 m. sausio 6 d. nutartis baudžiamojoje byloje Nr. 2K-138/2015.

165 Vilniaus apygardos teismo 2017 m. gegužės 15 d. nuosprendis baudžiamojoje byloje Nr. 1-101-190/2017.

166 Kėdainių rajono apylinkės teismo 2017 m. rugsėjo 28 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-308-188/2017.

167 Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2012 m. gegužės 8 d. nutartis baudžiamojoje byloje Nr. 2K-P-78/2012.

elektroninėje erdvėje baudžiamosiose bylose galėtų būti konstatuojama tada, jei neteisėtai jungdamasis prie informacinės sistemos kaltininkas yra „aiškiai suvokęs, kokius paskesnius veiksmus sistemoje jis rengiasi atlikti, ir palaipsniui šį sumanymą įgyvendina“[168]. Ir priešingai – jei tyčia padaryti kitas nusikalstamas veikas sistemoje atsirado tik gavus prieigą prie jos (dėl to ir buvo padaryta iš pradžių nenumatytų veikų), tokios veikos tarpusavyje galėtų sudaryti realiąją sutaptį.

2. Objektyvieji neteisėto prisijungimo prie informacinės sistemos sudėties požymiai

2.1. Informacinė sistema ar jos dalis kaip nusikalstamos veikos dalykas

Neteisėto prisijungimo prie informacinės sistemos dalykas BK 198[1] straipsnio dispozicijoje įvardijamas kaip informacinė sistema ar jos dalis. Kadangi šis požymis yra susijęs ne tiek su teisiniu, kiek su technologiniu šios nusikalstamos veikos aspektu, kalbant apie jo turinį yra aktualus minėtasis technologijų ir terminologijos klausimas. Šiomis aplinkybėmis jis kyla dėl to, kad nėra universalaus informacinės sistemos suvokimo, jos aiškinimas ir turinys gali skirtis atsižvelgiant į kontekstą, kuriame ši technologijas žyminti sąvoka yra vartojama. Be to, greta termino „informacinės sistemos“ dar vartojami kompiuterinės sistemos, informacinių ir komunikacijos technologijų terminai. Nusikalstamos veikos dalyko aiškinimą dar labiau komplikuoja kriminalizuojant neteisėto prisijungimo prie informacinės sistemos veiką įgyvendinti minėtieji technologinio neutralumo principo reikalavimai.

Baudžiamosios teisės požiūriu, technologijas žyminčių sąvokų problemas gali būti bandoma spręsti dviem būdais: *pirma*, technologijas žymintys terminai baudžiamajame įstatyme pateikiami kaip neapibrėžti (pavyzdžiui, Prancūzija, Estija, Rusija). Nors toks požiūris, atsižvelgiant į technologinio neutralumo principo reikalavimus, turi akivaizdžių privalumų, bet teisės taikymo lygmeniu nepadeda nustatyti aiškių kriterijų, kas galėtų būti ir kas nėra informacinė sistema ar

[168] *Baudžiamoji justicija ir verslas: recenzuotų mokslinių straipsnių rinkinys.* Švedas, G. (vyr. red.). Vilnius: Vilniaus universiteto Teisės fakultetas, 2016, p. 281.

jos komponentai; *antra*, baudžiamajame įstatyme pateikiamos įvairių su technologijomis susijusių terminų reikšmės (pavyzdžiui, Jungtinės Amerikos Valstijos, Kipras, Austrija). Iš pirmo žvilgsnio šis būdas galėtų atrodyti kaip galintis užtikrinti sudėties požymių aiškumą, bet dėl įtvirtinto gana bendro sąvokų turinio tokie apibrėžimai kelia analogiškų problemų, kaip ir tada, kai jie nėra suformuluoti.

Kadangi BK XXX skyriuje nepateikiamas autentiškas jame vartojamų sąvokų išaiškinimas, Lietuva galėtų būti priskiriama pirmajai grupei valstybių, kuriose klausimas, kaip tinkamai interpretuoti informacinės sistemos terminą, paliekamas BK 198[1] straipsnio taikytojo nuožiūrai. Vis dėlto toks požiūris, leidžiantis gana lanksčiai pažvelgti į informacinės sistemos sąvokos turinį, kelia ir nemažai jos apibrėžties problemų, ypač kai tokių išaiškinimų bandoma ieškoma įvairių mokslų srityse. Kaip antai nemažai informacinės sistemos interpretavimo variantų, atitinkamai ir požiūrių į naująsias technologijas, galima rasti komunikacijos bei informacijos moksluose. Čia informacinė sistema apibūdinama kaip „tarpusavyje susijusių komponentų visuma, kurie renka (arba atrenka), apdoroja, saugo ir skleidžia informaciją padėdami priimti sprendimus, atlikti koordinavimo, kontroliavimo ir analizės veiksmus organizacijoje“[169]. Informacinė sistema gali būti suvokiama ir kaip „sistema, paverčianti išorinius ir vidinius duomenis informacija, užtikrinanti informacijos kaupimą, saugojimą, apdorojimą ir perdavimą naudotojui reikiamu pavidalu, sudaranti galimybę priimti optimalius sprendimus“[170]. Be to, ji yra visuma komponentų, „skirtų įvairių rūšių duomenims ir informacijai rinkti, saugoti, apdoroti, laikyti bei skleisti, siekiant tam tikrų organizacijos tikslų ir taikant kompiuterines technologijas“[171]. Kaip matyti, šios sąvokos atitinka bendrosios sistemų teorijos teiginius, kad sistema yra vienetas, kuris funkcionuoja aplinkoje, padeda siekti bendrų tikslų ir yra sudarytas iš daugelio tarpusavyje sąveikaujančių dalių. Viena vertus, šios sąvokos gana nuosekliai atskleidžia informacinės sistemos esmę, kita vertus, žiūrint iš baudžiamosios teisės pozicijų, joms būdinga keletas aspektų,

[169] Laudon, K. C.; Laudon, J. P. Essentials of Management Information Systems. 3-iasis leidimas. New Jersey: Prentice-Hall, Inc., 1999, p. 7.

[170] Saulis, A.; Vasilecas, O. Informacinių sistemų projektavimo metodai: mokomoji knyga. Vilnius: Technika, 2008, p. 9.

[171] Dzemydienė, D.; Naujikienė, R. Informacinės sistemos. Duomenų struktūros ir valdymas. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2004, p. 32.

kurie kvalifikuojant neteisėto prisijungimo prie informacinės sistemos veiką gali kelti ir sumaišties. Didžiausių minėtųjų sąvokų perėmimo ir jų taikymo baudžiamojoje teisėje sunkumų gali kilti dėl jomis nurodomų informacinės sistemos sudedamųjų dalių (vadinamųjų komponentų arba posistemių)[172]. Vertinant informacinės sistemos kūrimo ir pritaikomumo įvairiose veiklos srityse galimybes, literatūroje sistemos sudedamosios dalys yra neribojamos tik informacinėmis ir komunikacijos technologijomis. Dėl to informacinės sistemos komponentais dažniausiai laikoma techninė ir programinė įranga, duomenys ir žmonės[173]. Panašus į šią nuomonę yra ir teiginys, kad „informacinė sistema jungia informacines technologijas su duomenimis, duomenų apdorojimo procedūras ir žmones, kurie renka duomenis ir jais naudojasi <...>“[174], arba kad sistemos komponentai yra „kompiuterinė sistema, žmonės, procedūros, duomenys ir informacija, ryšio priemonės (kai kompiuteris dirba tinkle)“[175]. Neatsižvelgiant į tai, ar informacinė sistema apibrėžiama gana abstrakčiai ar detalizuojant ją sudarančius komponentus, ją apibūdinant bendriausia prasme mintyje turimas technologijų, funkcijų, duomenų ir technologijas taikančių žmonių tarpusavio ryšys. Vadinasi, remiantis šiais požiūriais, informacinei sistemai, be ją sudarančių technologijų, dar priskiriama ir jos veikimo aplinka, siejama su šios sistemos paskirtimi ir jos vartotojais. Beje, tokį požiūrį į informacinės sistemos komponentus galima rasti ir ISO/IEC 2382-1:1996 *Informacijos technologija. Terminai ir apibrėžimai. 1 dalis. Pagrindiniai terminai* standarte (toliau – ISO/IEC 2382-1:1996), kur ji apibūdinama kaip „informacijai kurti ir skleisti skirta visuma, sudaryta iš informacijos apdorojimo sistemos ir organizacijos resursų (žmonių, technologijų, priemonių, lėšų ir pan.), reikalingų, kad ta visuma galėtų veikti“[176].

---

[172] Gupta, U. Information Systems. Upper Saddle River, New Jersey: Prentice-Hall Inc., 2000, p. 12–13.

[173] Saulis, A.; Vasilecas, O. Informacinių sistemų projektavimo metodai: mokomoji knyga. Vilnius: Technika, 2008, p. 9.

[174] Gordon, J. R.; Gordon, S. R. Information systems. 2-asis leidimas. The Dryden Press: Harcourt Brace College Publisher, 1999, p. 11.

[175] Jonušauskas, S.; Bilevičienė, T.; Kažemikaitis, V. Įvadas į informatiką. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002, p. 5.

[176] Informacinės sistemos turiniui atskleisti yra aktualūs Tarptautinės standartizacijos organizacijos (ISO) ir Tarptautinės elektrotechnikos komisijos (IEC) sudaryti tarptautiniai standartai. Kadangi informacinės technologijos skatina intensyvius informacijos mainus tarptautiniu lygiu, šie standartai padeda spręsti įvairiose srityse

Dėl tokių požiūrių natūraliai kyla klausimas, ar nustatant neteisėto prisijungimo prie informacinės sistemos dalyką turėtų būti vertinami ne tik technologiniai aspektai, bet ir visi minėtieji informacinę sistemą sudarantys komponentai.

Sprendžiant šią problemą, baudžiamosios teisės srityje reikėtų atkreipti dėmesį į tai, kad BK 198[1] straipsnyje nurodomos informacinės sistemos ištakų pirmiausia reikėtų ieškoti ne tiesiogiai komunikacijos ir informacijos mokslų srityje, o tarptautiniuose ir ES teisės aktuose, kur ji yra numatyta. Vadinasi, šiuo požiūriu yra aktualu nustatyti, koks turinys galėtų būti suteiktas BK 198[1] straipsnyje numatytos nusikalstamos veikos dalykui, įgyvendinant Konvencijos dėl elektroninių nusikaltimų 2 straipsnio ir Direktyvos 2013/40/ES 3 straipsnio nuostatas Lietuvos nacionalinėje teisėje. Pagal Direktyvos 2013/40/ES 2 straipsnio a punktą, informacinė sistema apibrėžiama kaip „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą atlieka automatinį kompiuterinių duomenų tvarkymą, taip pat kompiuteriniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugos ir priežiūros tikslais“. Skirtingai nei Direktyvoje 2013/40/ES, Konvencijoje dėl elektroninių nusikaltimų vartojamas ne informacinės, o kompiuterinės sistemos terminas. Jis šios konvencijos 1 straipsnio a punkte apibrėžtas kaip „įtaisas arba tarpusavyje sujungtų ar susijusių įtaisų grupė, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja duomenis“. Konvencijos aiškinamosios ataskaitos 23 punkte ši sąvoka detalizuojama kaip apimanti prietaisus, sudarytus iš aparatinės[177] ir programinės įrangos[178] bei sukurtus siekiant automatiškai apdoroti elektroninius duomenis.

---

vartojamų terminų įvairovės, sąvokų apibrėžčių nebuvimo ar jų netikslumų klausimus. Nagrinėjamuoju požiūriu vienas iš aktualesnių yra ISO/IEC 2382-1:1996. Jis priklauso tarptautinių standartų ISO (ISO/IEC) 2382 grupei, kuri susieja duomenų apdorojimo, informacijos technologijų ir informacijos apdorojimo sistemų terminų bei apibrėžimų standartus. Jais siekiama pateikti tikslias, nesudėtingas, visiems suprantamas ir bendrajai vartosenai priimtinas apibrėžtis.

[177] Pagal ISO/IEC 2382-1:1996 standartą, „techninė įranga – informacijos apdorojimo sistemos fizinių komponentų visuma arba tos visumos dalis (kompiuteriai, išoriniai įrenginiai)“.

[178] Pagal ISO/IEC 2382-1:1996 standartą, „programinė įranga – informacijos apdorojimo sistemos programų, procedūrų, taisyklių visuma arba tos visumos dalis su atitinkama dokumentacija“.

Kaip teigiama, kompiuterinei sistemai gali priklausyti įvesties, išvesties ir laikymo (saugojimo) įranga. Tai gali būti atskira kompiuterinė sistema arba sujungta tinklu su kitomis panašiomis sistemomis. Kompiuterinę sistemą dažniausiai sudaro įvairūs įrenginiai, kurie gali būti suskirstyti į procesorių (angl. *processor)*[179] arba centrinį procesorinį įrenginį (angl. *Central Processing Unit,* CPU) bei išorės įrenginius (angl. *peripherals)*. Išorės įrenginiais[180] laikomi tokie įrenginiai, kurie atlieka tam tikras specifines funkcijas sąveikaudami su apdorojimą atliekančiu vienetu (angl. *processing unit)*, pavyzdžiui, spausdintuvas, kompaktinių diskų skaitymo ar įrašymo (angl. *CD reader/writer)*, laikymo (saugojimo) funkcijas atliekantys įrenginiai.

Dėl Direktyvos 2013/40/ES 2 straipsnio a punkte pateikiamos informacinės sistemos apibrėžties gali kilti ir keletas jos taikymo klausimų. Joje (kaip ir Konvencijoje dėl elektroninių nusikaltimų) formuluojant informacinės sistemos sąvoką nurodomi tam tikri prietaisai ar tarpusavyje susijusių prietaisų grupės, kurie ir sudaro šias sistemas. Jau minėta, jog vadovaujantis bendrosios sistemų teorijos teiginiais galima tvirtinti, kad informacinė sistema veikia kaip vienetas, sudarytas iš įvairių sudedamųjų dalių derinių. Vadinasi, pats neteisėtas poveikis sistemos konfidencialumui gali būti padaromas tiesiogiai veikiant tik tam tikrus specifines funkcijas atliekančius jos komponentus (dalis). Dėl to baudžiamosios teisės srityje gali kilti abejonių, ar konstatuotinas prisijungimas prie informacinės sistemos, jei prieiga gauta tik prie kurio nors vieno jos įrenginio?[181] Kaip teigiama literatūroje, „konfidencialumo, prieinamumo ir vientisumo sąvokos taikomos ne tik informacijai (duomenims), bet ir kitiems tinklo ištekliams, pavyzdžiui, išoriniams įrenginiams arba jų priedams. Yra daugybė sisteminių išteklių, kurių „neteisėto“ panaudojimo galimybė gali sudaryti sąlygas pažeisti sistemos saugumą“[182]. Taigi šiuo požiūriu galima tvirtinti, kad

[179] Pagal ISO/IEC 2382-1:1996 standartą, procesorius – tai „kompiuterio funkcinis vienetas, kuris interpretuoja ir vykdo komandas“.

[180] Pagal ISO/IEC 2382-1:1996 standartą, išorinis įrenginys – tai „kiekvienas įrenginys, kuris yra valdomas kompiuterio ir gali su juo bendrauti (pavyzdžiui, įvesties ir išvesties įrenginiai, išorinė atmintis)“.

[181] *Baudžiamoji justicija ir verslas: recenzuotų mokslinių straipsnių rinkinys.* Švedas, G. (vyr. red.). Vilnius: Vilniaus universiteto Teisės fakultetas, 2016, p. 276.

[182] Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 9.

informacinės sistemos komponentai funkcionuoja kaip viena visuma, todėl neteisėtas prisijungimas prie jos gali būti konstatuojamas ir tais atvejais, kai pažeidus sistemos ar jos dalių apsaugos priemones buvo gauta prieiga ir prie atskirų jos dalių (pavyzdžiui, išorinių įrenginių, tinklo infrastruktūros įrenginių ir pan.). Kita vertus, siekiant išvengti galimų nesusipratimų aiškinant BK 198[1] straipsnyje numatyto dalyko požymį, jis buvo patikslintas 2015 metų šio straipsnio pakeitimais nustatant, kad neteisėtas prisijungimas yra laikomas nusikalstama veika tais atvejais, kai prieiga buvo gauta ir prie visos, ir prie dalies informacinės sistemos.

Apibendrinant teisės aktuose esančias informacinės sistemos sąvokas iš baudžiamosios teisės pozicijų, galima padaryti keletą išvadų, svarbių aiškinant BK 198[1] straipsnyje numatytą nusikalstamos veikos dalyką:

Pirma, pateikti informacinės sistemos apibrėžimai leidžia įžvelgti daug Direktyvoje 2013/40/ES minimos informacinės sistemos ir Konvencijoje dėl elektroninių nusikaltimų esančios kompiuterinės sistemos panašumų, išskyrus tai, kad į Direktyvoje pateiktą apibrėžimą yra aiškiai įtraukti patys kompiuteriniai (elektroniniai) duomenys. Apibrėžiant kompiuterinę sistemą Konvencijoje dėl elektroninių nusikaltimų ir informacinę sistemą Direktyvoje 2013/40/ES, išimtinai aptariami tik bendriausi technologiniai sistemų aspektai (aparatinė ir programinė įranga, sistemos atliekamos funkcijos). Beje, tokį požiūrį į informacinę sistemą galima įžvelgti ir nacionaliniuose teisės aktuose, kuriuose apibūdinant sistemą daugiausia dėmesio skiriama techninių ir programinių priemonių visumai, būtinai elektroniniams duomenims apdoroti. Pavyzdžiui, Lietuvos Respublikos informacinės visuomenės paslaugų įstatymo[183] 2 straipsnio 9 dalyje informacinė sistema yra apibrėžiama neatsižvelgiant į jos taikymo aplinką, kaip „techninių ir programinių priemonių visuma, naudojama informacijai kurti, siųsti, priimti, išsaugoti ar kitaip tvarkyti elektroniniu būdu“. Tuo remiantis, BK 198[1] straipsnyje įtvirtintas nusikalstamos veikos dalykas – informacinė sistema – turėtų būti suvokiama siauriau, t. y. be jos taikomojo aspekto, ir baudžiamosios teisės srityje bendriausia prasme

[183] Lietuvos Respublikos informacinės visuomenės paslaugų įstatymas. *Valstybės žinios*, 2006, Nr. 65-2380.

galėtų būti laikoma informacinių technologijų[184] (apimančių ir komunikavimo technologijas[185]) ar kompiuterinės sistemos sinonimu.

Antra, BK 198[1] straipsnyje numatyta informacinė sistema galėtų būti siejama tik su kompiuterizuotomis sistemomis, nes būtent jos taiko informacines technologijas[186] duomenų apdorojimo procesams realizuoti[187]. Kaip teigiama literatūroje, „kompiuteriu pagrįstos in-

---

[184] Informacinės technologijos (IT) įvairiuose šaltiniuose yra apibūdinamos panašiai. Žodynuose jos apibrėžiamos kaip „priemonių ir būdų visuma informacijai apdoroti. Apima įvairius metodus ir priemones (aparatinę ir programinę įrangą), skirtas duomenims apdoroti: rinkti, rikiuoti, laikyti, perduoti arba kitaip tvarkyti kompiuteriu“ (Enciklopedinis kompiuterijos žodynas. 2-asis papildytas leidimas. Vilnius: TEV, 2008, p. 161.). Kituose šaltiniuose irgi pateikiamas panašus IT apibrėžimas – „informacine technologija vadinama metodų ir būdų sistema informacijai rinkti, kaupti, saugoti, apdoroti ir pateikti vartotojui. Šiuolaikinės informacinės technologijos grindžiamos kompiuterinės technikos panaudojimu“ (Žilinskas, A.; Leonavičius, G.; Valavičius, E. Informatika. Vilnius: Aldorija, 2000, p. 24.).

[185] Analizuojant informacijos ir komunikacijos technologijas, minėtinas dvejopas požiūris į jų tarpusavio sąsają. Vienais atvejais komunikacijos technologijos laikomos informacinių technologijų (informacinės sistemos) sudedamąja dalimi. Kaip antai gali būti tiesiogiai nurodoma, kad informacinės technologijos skirstomos į informacijos apdorojimo (pvz., kompiuterinės sistemos), informacijos skleidimo ir platinimo (pvz., ryšių sistemos) technologijas (Technikos enciklopedija. II tomas. Redaktorių taryba: pirmininkas Zavadskas, E. K., *et al*. Vilnius: Mokslo ir enciklopedijų leidybos inst., 2003, p. 269). Be to, informacinių technologijų turinį galima atskleisti per jų sudedamųjų dalių raidą: kompiuterių, programinės įrangos, duomenų kaupimo ir ryšių įrangos (Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008, p. 22.). Kitais atvejais norint pabrėžti įvairius ryšio įrenginius ir informacijos perdavimo būdus, komunikacinės technologijos gali būti minimos ir šalia informacinių technologijų (informacinės sistemos) (Enciklopedinis kompiuterijos žodynas. 2-asis papildytas leidimas. Vilnius: TEV, 2008, p. 160).

[186] Informacinių technologijų terminas dažniausiai yra siejamas su kompiuterinėmis informacinėmis technologijomis, kurių materialųjį pagrindą sudaro kompiuterių technologijos. Kita vertus, reikėtų atkreipti dėmesį, kad bendroji informacinių technologijų samprata yra daug platesnė – joms galima priskirti viską, kas padeda įrašyti, perduoti ar pateikti informaciją (pavyzdžiui, net ir tradicinės popierinės technologijos: dokumentai, laiškai, spaudai ir kt.) (plačiau žr.: Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008, p. 17).

[187] Laučius, J.; Vasilecas, O. Informacinių technologijų projektų ir kokybės valdymas: mokomoji knyga. Vilnius: Technika, 2007, p. 7.

formacinės sistemos, tai sistemos, kurios naudoja kompiuterių technologijas, kad atliktų kai kurias arba visas numatytas užduotis. Dauguma informacinių sistemų yra kompiuterizuotos, bet ne visos. Dėl šių priežasčių terminas *informacinės sistemos* dažniausiai vartojamas kaip „kompiuteriais pagrįstų informacinių sistemų" sinonimas"[188]. Vadinasi, tik tokios kompiuterizuotos informacinės sistemos, kaip jos suvokiamos Direktyvoje 2013/40/ES, gali būti tapatinamos su Konvencijoje dėl elektroninių nusikaltimų minimomis kompiuterinėmis sistemomis.

Trečia, į informacinę sistemą kaip neteisėto prisijungimo dalyko požymio turinį yra įtrauktos ne tik informacinės, bet ir komunikacijos technologijos. Tokia išvada, be kita ko, darytina atsižvelgiant į tai, kad anksčiau BK 198[1] straipsnio dispozicijoje minimos kompiuterio ir kompiuterinio tinklo technologijos, padarius 2007 metų pakeitimus, buvo sujungtos ir šiame BK straipsnyje įvardytos vienu informacinės sistemos terminu. Vėliau 2015 metais nusikalstamos veikos dalykas buvo patikslintas nurodžius ne tik visą informacinę sistemą, bet ir atskirą jos dalį.

2.2. Neteisėtas prisijungimas – pavojinga veika

2.2.1. Prisijungimo samprata

Galiojančiame BK 198[1] straipsnyje pavojinga veika įvardijama kaip neteisėtas prisijungimas. Atskleidžiant šio požymio turinį reikėtų pabrėžti, kad ir prisijungimas, ir jo neteisėtumas, atsižvelgiant į tarptautinius ir ES teisės aktus, literatūroje išsakomas nuomones bei užsienio valstybių tokios veikos kriminalizavimo patirtį, gali būti interpretuojamas labai įvairiai. Kadangi neteisėtam prisijungimui įmanoma suteikti gana plačią arba ganėtinai siaurą reikšmę, aiškinant šį pavojingos veikos požymį reikėtų nustatyti, kaip plačiai įstatymų leidėjas siekė kriminalizuoti neteisėto prisijungimo prie informacinės sistemos nusikalstamą veiką.

Analizuojant šią veiką atkreiptinas dėmesys į tai, kad ir Konvencijoje dėl elektroninių nusikaltimų (2 straipsnis), ir Direktyvoje

[188] Potter, R. T., *et al*. Introduction to Information Systems: Supporting and Transforming Business. John Wiley & Sons, Inc., 2007, p. 6.

2013/40/ES (3 straipsnis) *prisijungimo* terminas neminimas. Šiuose teisės aktuose kalbama ne apie neteisėtą prisijungimą, o apie neteisėtą prieigą (angl. *access)* prie informacinės sistemos. Nors iš pirmo žvilgsnio galėtų atrodyti, kad abiem terminais apibrėžiamos analogiškos sąvokos, bet prisijungimui prie informacinės sistemos būdinga tam tikra specifika. Toks skirtumas atsiranda dėl įvairių prieigos prie sistemos interpretavimo variantų, kurie, kaip minėta, gali šiai sąvokai suteikti labai plačią reikšmę arba ją susiaurinti. Vadinasi, tam tikru požiūriu prieiga gali būti laikoma prisijungimo sinonimu, bet prieiga prie informacinės sistemos gali būti suprantama ir plačiau nei prisijungimas. Kadangi prisijungimo terminas Lietuvos BK nėra išaiškintas, siekiant nustatyti prieigos ir prisijungimo santykį bei atskleisti jų turinį, reikėtų atsižvelgti ne tik į bendrinę šių žodžių reikšmę, bet ir pasirinkti vieną iš galimų požiūrių į elektroninę erdvę – jos vertinimo perspektyvą.

Informacinių ir komunikacijos technologijų srityje prieiga prie informacinės sistemos yra suvokiama panašiai. Ji įvardijama kaip prieigos prie duomenų ar sistemos gavimas[189], galimybė įeiti į sistemą ir ja naudotis[190] arba galimybė prieiti prie sistemos išteklių[191]. Panašiai ji apibūdinama ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje – joje prieiga yra „įėjimas į visą arba dalį kompiuterinės sistemos“ (46 punktas). Iš šių aiškinimų matyti, kad bendriausia prasme prieiga suvokiama kaip įėjimas į informacinę sistemą ir priartėjimas prie jos išteklių. Kita vertus, tokia išvada leidžia pastebėti įdomų aspektą – aiškinant šią veiką nevengiama posakių, vartojamų veiksmams fizinėje erdvėje apibūdinti. Pavyzdžiui, kadangi prieiga laikoma įėjimu į informacinę sistemą, atitinkamai galimas ir išėjimas iš jos (tai laikytina įėjimo ir išėjimo iš patalpos analogu). Į tokią keblią padėtį, kai veiksmams elektroninėje erdvėje paaiškinti bandoma taikyti artimus fizinės erdvės kriterijus, atkreiptas dėmesys

[189] A Dictionary of Computing. 5-asis leidimas. Daintith, J. (gen. ed.). Oxford: Oxford University Press, 2004, p. 5.

[190] Dictionary of information science and technology. I tomas. Khosrow-Pour, M. (ed). Hershey, Pa., *et al*. Idea Group Reference, 2007, p. 2.

[191] Dagienė, V., *et al*. Enciklopedinis kompiuterijos žodynas. Vilnius: TEV, 2008, p. 369.

ir mokslinėje literatūroje[192]. Skirtingi autoriai, nagrinėdami probleminius neteisėtos prieigos aspektus, pateikė gana įdomių palyginimų ir bandymų paaiškinti, kodėl baudžiamojoje teisėje elektroninės erdvės vertinimas vis dar nenutolęs nuo fizinės erdvės suvokimo. Kaip teigiama doktrinoje, „internetas yra apibūdinamas vietos ir erdvės terminais iš dalies dėl to, kad tokiu būdu mes jį suprantame ir įgyjame apie jį patirties“[193]. Pasitaiko ir tokių nuomonių, kurios leidžia kompiuterį prilyginti „dėžei“, informacijos saugyklai, į kurią yra uždrausta patekti, todėl „įėjimo į visą ar dalį kompiuterinės sistemos“ posakis „sukelia buvimo kompiuterio „viduje“ arba „išorėje“ įsivaizdavimą“[194]. Akivaizdu, kad toks neteisėtas patekimas į informacinės sistemos vidų būtų siejamas ne su fizine, o su „virtualiąja prieiga“[195], kuri yra panaši į neteisėtą įėjimą į fizinėje erdvėje esančią vietą. Tokie samprotavimai leidžia ne tik suformuluoti elektroninės erdvės kaip vietos palyginimą, bet ir matyti tradicinės neteisėto įsibrovimo į svetimą valdą (angl. *trespass)* doktrinos raidą[196]. Būtent ši

---

192 Wong, M. W. S. Cyber-trespass and “Unauthorized Access“ as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1); Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2); Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010; Kerr, O. S. Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5).

193 Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2): 442.

194 Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 59.

195 Wong, M. W. S. Cyber-trespass and “Unauthorized Access“ as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1): 123.

196 Bendrosios teisės tradicijos valstybėse suformuluota *trespass* doktrina yra gana plati ir jai priskiriamos trys pagrindinės formos: įsibrovimas į svetimą valdą (angl. *trespass to land)*, kilnojamojo turto savininko teisės pažeidimai (angl. *trespass to goods)* ir kėsinimasis į asmenį (angl. *trespass to person)*. Sprendžiant, kuri iš jų yra tinkama kalbėti apie „virtualiąją analogiją“ vertinant neteisėtus veiksmus elektroninėje erdvėje, reikėtų atsižvelgti į neteisėtos prieigos kriminalizavimo skirtumus užsienio valstybėse. Tuo atveju, jei ši veika aprašyta kaip neteisėta prieiga prie duomenų, įveikiant jų apsaugą, teisingiau yra kalbėti apie *trespass to goods* „virtualiąją analogiją“. Jei nusikalstama veika yra tiesiogiai kriminalizuota kaip neteisėta prieiga prie informacinės sistemos, tinkamesnis terminas yra *trespass to land* „virtualioji analogija“.

doktrina mokslinėje literatūroje[197] dažniausiai laikoma logišku atspirties tašku aiškinant neteisėto prisijungimo prie informacinės sistemos veiką ir yra įvardijama elektroninio įsibrovimo į svetimą erdvę terminu (angl. *cybertrespass)*. Nors ši doktrina yra bendrosios teisės sistemos valstybių „kūrinys", vis dėlto apie įsibrovimo doktrinos raidą galima kalbėti ir analizuojant Lietuvos BK nuostatas. Jame numatyta keletas nusikalstamų veikų, į kurių sudėtį yra įtrauktas įsibrovimo elementas. Tai BK 165 straipsnyje aprašyta neteisėto asmens būsto neliečiamumo pažeidimo veika, BK 178 straipsnio 2 dalyje nurodoma vagystė įsibraunant į patalpą, saugyklą ar saugomą teritoriją ir BK 180 straipsnio 2 dalyje kriminalizuotas plėšimas įsibraunant į patalpą. Vadinasi, analizuojant „įsibrovimą" elektroninėje erdvėje, „galima būtų išsakyti idėją, kad tam tikra elektroninės erdvės kaip vietos privatumo apsauga, *mutatis mutandis* įgyvendinant žmogaus būsto neliečiamumo principą, yra užtikrinta BK 198[1] straipsnyje, kuriame numatoma baudžiamoji atsakomybė už neteisėtą prisijungimą prie IS"[198]. Kadangi BK 198[1] straipsnyje numatyta veika yra kriminalizuota *per se* (pati savaime) jos nesiejant su tolesniais nusikalstamais kaltininko veiksmais jau pačioje sistemoje (pavyzdžiui, elektroninių duomenų įgijimu, laikymu ir pan.), tai jai artimesnė yra neteisėto asmens būsto neliečiamumo pažeidimo veika (BK 165 straipsnis). Taigi baudžiamojo įstatymo normos, draudžiančios neteisėtą prieigą prie informacinės sistemos, yra panašios į tas, kurios draudžia neteisėtą įėjimą į fizinę erdvę[199]. Šis prieigos prie informacinės sistemos aiškinimo variantas rodo „virtualiąją analogiją"[200], reiškiančią ne ką kitą, kaip tradicinės neteisėto įsibrovimo sampratos perėmimą ir pritaikymą elektroninei erdvei.

---

197 Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 163; Wong, M. W. S. Cyber-trespass and "Unauthorized Access" as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1): 90–107; Reed, D. Should the English Legal System adopt the US Law of Cyber-Trespass? *SCRIPTed*, 2011, 8(1): 46–68.

198 *Baudžiamoji justicija ir verslas: recenzuotų mokslinių straipsnių rinkinys.* Švedas, G. (vyr. red.). Vilnius: Vilniaus universiteto Teisės fakultetas, 2016, p. 277.

199 Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review*, 2016, 116: 1154.

200 Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1620.

Kita vertus, laikantis tokio požiūrio, neskiriama pakankamai dėmesio įvairiems informacinės sistemos technologiniams aspektams: nuolat kintančioms įvesties, duomenų apdorojimo (taip pat ir komunikavimo), išvesties galimybėms. Informacinė sistema veikia fizinėje erdvėje, turi tam tikrus fizinius parametrus, šiai sistemai būdingi atitinkami ją sudarančių komponentų sąveikos būdai, bet kartu ji sukuria elektroninę erdvę. Ši erdvė pati savaime nėra analogiška fizinei erdvei – ji yra informacinės sistemos, veikiančios fizinėje erdvėje, veiklos rezultatas. Tokią gana keblią padėtį neblogai atspindi doktrinoje pateikiama mintis, kad „kai tu *eini* kažkur realioje erdvėje, tu išeini; kai tu *eini* elektroninėje erdvėje, tu niekur neišeini. Tu niekada nesi *tik* elektroninėje erdvėje. <...> Tu visuomet esi abiejose – realioje ir elektroninėje erdvėje – tuo pačiu metu“[201]. Būtent pastebėjus šį dualumą, mokslinėje literatūroje pradėta kalbėti apie dvi skirtingas elektroninės erdvės vertinimo pozicijas – *išorinę* ir *vidinę* perspektyvą[202]. Kadangi šios vertinimo pozicijos tarpusavyje konkuruoja, vienos iš jų pasirinkimas ir taikymas toms pačioms faktinėms aplinkybėms gali lemti visiškai skirtingą neteisėtos prieigos prie informacinės sistemos baudžiamąjį teisinį vertinimą. Kita vertus, pasirinkus kurią nors vieną iš jų – išorinę ar vidinę – jos vis vien išlieka kaip metaforos, kuriomis siekiama aiškiau suvokti vartotojo ir informacinės sistemos tarpusavio ryšį, jo patyrimą elektroninėje erdvėje.

Vidinė perspektyva leidžia į elektroninę erdvę pažvelgti kaip į „virtualiąją realybę“[203]. Tai sudaro sąlygas elektroninę erdvę suvokti ir veiksmus joje vertinti remiantis fizinėje erdvėje nustatytais kriterijais arba, kitaip tariant, kalbėti apie minėtąją „virtualiąją analogiją“. Poreikis skirstyti elektroninę erdvę į dalis ir nustatyti jų ribas atitinkamai yra pagrįstas tradiciniu fizinės erdvės skaidymu į tam tikras teritorijas, suteikiant galimybę analizuoti ir vertinti įvairius tokių erdvių konfidencialumo pažeidimus. Tai leidžia prilyginti kompiuterį „dėžei“ ir informacijos saugyklai, prieigą prie informacinės sistemos laikyti me-

---

[201] Lessig, L. Code and other Laws of Cyberspace. New York (N.Y.): Basic books, 1999, p. 21.

[202] Kerr, O. S. The Problem of Perspective in Internet Law. *Georgetown Law Journal*, 2003: 91.

[203] *Ibidem*.

taforišku patekimu į kompiuterio „vidų“ kaip įėjimu į pastatą[204], o tinklalapį vertinti kaip „atvirą viešą skverą fizinėje erdvėje“[205]. Toks vienas iš galimų požiūrių į elektroninę erdvę tiesiogiai atspinti informacinės sistemos vartotojo elektroninės erdvės įsivaizdavimą ir jos suvokimą – ieškoti pakraščių ir ribų yra būdinga ne tik fizinėje, bet ir elektroninėje erdvėje.

Klasikinis *vidinės perspektyvos* taikymo pavyzdys mokslinėje literatūroje[206] yra siejamas su vartotojo vardu ir slaptažodžiu apsaugoto kompiuterio bei užrakintos patalpos analogija. Prieigai prie kompiuterio nustačius autentifikavimo procedūrą, reikalavimas įvesti vartotojo vardą ir slaptažodį pripažįstamas kaip artimas durų užraktui, o „vartotojo vardo ir slaptažodžio įvedimas yra tarsi raktas, reikalingas užraktui atrakinti“[207]. Jei vartotojas įveda teisingus duomenis, jis gauna prieigą prie kompiuterio. Ir priešingai – jei kompiuteriui buvo pateikti klaidingi duomenys, prieiga vartotojui nesuteikiama. Žiūrint iš *vidinės perspektyvos* pozicijų – kitaip būtų vertinami neteisėti tinklų ar prievadų peržiūros veiksmai, kuriuos atliekant, pavyzdžiui, renkama įvairi su IP adresais, sistemoje veikiančiais servisais, operacine sistema, įdiegtomis programomis susijusi ar panaši informacija (duomenų srauto „pasiklausymas“ tinklo viduje[208]). Taip nustatomos silpnosios informacinės sistemos vietos, o saugumo spragomis dažniausiai pasinaudojama neteisėtai į ją įsibraunant. Žiūrint iš *vidinės perspektyvos* pozicijų, šie veiksmai nelaikomi „virtualiuoju įėjimu“ į informacinę sistemą, dėl to jiems apibūdinti yra taikomas „durų rankenų klebenimo“[209] palyginimas.

---

[204] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 59.

[205] Madison, M. J. Authority and Authors and Codes. *The George Washington Law Review*, 2016, 84(6): 1630.

[206] Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1620; Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 59.

[207] Kerr, O. S. The Problem of Perspective in Internet Law. *Georgetown Law Journal*, 2003, 91: 1620.

[208] Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 10.

[209] Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 2011, 22: 154.

Pagal *išorinės perspektyvos* variantą į elektroninę erdvę žiūrima ne kaip į „virtualiąją realybę“, bet tik kaip į informacinės sistemos veiklos rezultatą. Remiantis tokiu požiūriu, pirmenybė teikiama nebe šios erdvės vartotojo įsivaizdavimui, o atspindimas „pašaliečio“[210] suvokimas. Būdamas fizinėje erdvėje, informacinę sistemą jis mato kaip tam tikrą mechanizmą, sudarytą iš komponentų, kurie tarpusavyje komunikuoja siųsdami, gaudami ar kitaip apdorodami duomenis. Būtent dėl tokių jų atliekamų funkcijų ir vyksta pokyčiai virtualiojoje erdvėje. Taigi *išorinės perspektyvos* pasirinkimo atveju daugiausia dėmesio yra skiriama informacinės sistemos funkcijoms, jos komunikavimo būdams nustatyti ir jiems analizuoti, neatsižvelgiant į tai, kokių pokyčių jie sukelia elektroninėje erdvėje kaip „virtualiojoje realybėje“. Galima pateikti pavyzdį, kai vartotojas, naudodamasis naršyklės paslaugomis, siekia apsilankyti konkrečiame tinklalapyje. Pagal *vidinės perspektyvos* teoriją, jeigu užklausa yra sėkmingai įvykdyta, vartotojas tiesiog mato atvertą pageidaujamą tinklalapį. Kita vertus, tokia „virtualioji realybė“ tiesiogiai neparodo tų informacinės sistemos veiksmų, kurie buvo atlikti fizinėje erdvėje. Vartotojui nebuvo matomas visas pasikeitimo duomenimis procesas, atskiri duomenų perdavimo etapai, įvairių šiame procese dalyvaujančių siuntėjo ir gavėjo įrenginių atlikti veiksmai (pavyzdžiui, vartotojas nemato taikomųjų programų kreipimosi veiksmų į DNS serverius[211], jų atliktos IP adresų transliacijos (vertimo iš vienos formos į kitą), šių adresų pateikimo, tolesnių taikomųjų programų veiksmų siunčiant užklausas gautuoju adresu, atgalinių serverio, kuriame rasti užklausoje nurodyti duomenys, veiksmų ir kt.). Tokie techniniai aspektai yra „nematomi“[212] daugumai vartotojų. Dėl to tai, ką vartotojas mato būdamas virtualiojoje erdvėje, iš esmės skiriasi nuo to, kokias funkcijas atlieka informacinė sistema, sukurdama šią erdvę. Vadinasi, įvairioms informacinės siste-

---

[210] Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review,* 2003, 78(5): 1620.

[211] DNS – tai „domenų vardus skaitmeniniais interneto adresais verčiantis serveris“. (Paulauskas, K. V. Aiškinamasis kompiuterijos terminų santrumpų žodynas. Kaunas: Technologija, 2000, p. 83).

[212] Linzer, P. From the Gutenberg Bible to Net Neutrality - How Technology Makes Law and Why English Majors Need to Understand It. *McGeorge Law Review*, 2008, 39: 3.

mos funkcijoms apibūdinti šiuo atveju galėtų būti taikomas „veikimo už scenos“[213] palyginimas. Toks atskyrimas keičia ir patį požiūrį į prieigą prie informacinės sistemos, nes *išorinės perspektyvos* atveju taikomas ne virtualaus įėjimo į sistemą (nurodančio virtualiąją prieigą), o sąveikos su ja kriterijus. Daugelis prieigos problematiką nagrinėjusių autorių šį kriterijų įvardija labai įvairiai: kaip „interakciją su kompiuteriu“[214], „susisiekimą su kompiuteriu“[215], „privertimą kompiuterį atsakyti“[216] ar kt. Visais minėtaisiais atvejais mintyje turimas informacinės sistemos funkcijos inicijavimas. O. S. Kerrio nuomone, išimtinai vertinant tik tai, kaip veikia kompiuteris, prieiga galėtų būti interpretuojama kaip bet koks susisiekimas su kompiuteriu. Vadinasi, taikant *išorinės perspektyvos* teoriją prieigai konstatuoti užtektų, jei kompiuteriui buvo nusiųsta komanda atlikti funkciją ir „kompiuteris vykdo reikalavimą, kaip nustatyta“[217]. Apibūdindamas prieigos vertinimo variantus, panašią situaciją nurodo ir M. W. S. Wong. Anot jos, vienu iš atvejų, leidžiančių kalbėti apie prieigą, galėtų būti laikoma įrodyta vartotojo ir kompiuterio interakcija. Kita vertus, detalizuodama minėtąją situaciją, mokslininkė svarsto, ar tokiais atvejais pakanka tik nustatyti užklausos siuntimo faktą, ar turėtų būti reikalaujama „iš to sekančio automatizuoto ar kitokio kompiuterio atsako“[218].

Kaip pavyzdį, padedantį aiškiau suvokti *išorinės* ir *vidinės perspektyvų* skirtumus, galima pateikti aptartąjį atvejį, kai asmuo bando prisijungti prie vartotojo vardu ir slaptažodžiu apsaugoto kompiuterio. Jau minėta, kad žvelgiant iš *vidinės perspektyvos* prieiga prie kompiuterio

---

213 Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1620.

214 Wong, M. W. S. Cyber-trespass and "Unauthorized" Access as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1): 123.

215 Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1620.

216 Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 59.

217 Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1620.

218 Wong, M. W. S. Cyber-trespass and "Unauthorized Access" as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1): 123.

būtų tapatinama su „virtualiuoju įėjimu“ ir konstatuota nustačius, kad asmuo teisingai įvedė sistemai reikalingus duomenis. Priešingu atveju, jeigu autentifikuoti nepavyko (pavyzdžiui, buvo įvesti klaidingi duomenys), galima teigti, kad prieiga asmeniui nebuvo suteikta. Taikant *išorinės perspektyvos* teorijos kriterijus, tokia situacija yra vertinama šiek tiek kitaip. Išvada dėl prieigos gavimo sutaptų tais atvejais, kai asmeniui pavyksta sėkmingai prisijungti prie kompiuterio, bet esant nesėkmingam bandymui vertinimas iš esmės skirtųsi. Net ir negavęs „virtualiojo įėjimo“ jis, įvesdamas neteisingą vartotojo vardą arba slaptažodį, privertė kompiuterį atlikti funkciją ir pateikti rezultatą, kad yra įvesti neteisingi duomenys ir prieiga nesuteikiama. Remiantis *išorinės perspektyvos* teorija, šie veiksmai galėtų būti prilyginami prieigai prie kompiuterio. Be to, skirtingai nei *vidinės perspektyvos* atveju, vertinami ir jau aptarti prievadų ar tinklų peržiūros veiksmai. Vykstant peržiūros procesui tam tikru būdu keičiamasi duomenimis (bendraujama) su sistema: į asmens siunčiamus duomenis (užklausas) gaunamas sistemos atsakymas, taip sistema atlieka jai priskirtą funkciją. Vadinasi, tai, kas iš „virtualiosios realybės“ pozicijų būtų laikoma tik „durų rankenų klebenimu“, *išorinės perspektyvos* atveju yra vertinama kaip prieiga prie informacinės sistemos.

Analizuojant minėtuosius prieigos prie informacinės sistemos interpretavimo būdus gali kilti klausimas, kokios įtakos kvalifikuojant nusikalstamą veiką turės kurio nors vieno iš siūlomų variantų pasirinkimas, t. y. prieigą tapatinant su „virtualiuoju įėjimu“ arba ją laikant bet kokia interakcija su informacine sistema. Kadangi minėtosios *vidinė* ir *išorinė perspektyvos* rodo siauresnį, ir priešingai – platesnį požiūrį į prieigos prie sistemos gavimą, tai remiantis pasirinktu jos interpretavimo būdu, kaip buvo galima pastebėti, *pirma*, skirtingai nustatomas šios nusikalstamos veikos pradžios ir pabaigos momentas; *antra*, skirtingai apibrėžiamos nusikalstamos veikos ribos, atitinkamai ir jos inkriminavimo galimybės[219].

[219] Kaip vienas iš mokslinėje literatūroje pateikiamų tokios problemos pavyzdžių yra elektroninių laiškų siuntimo atvejis (Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1621). Į elektroninių laiškų siuntimo vertinimo problemą atkreiptas dėmesys ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje (46 punktas). Joje, apibrėžus prieigą kaip įėjimą į visą arba dalį kompiuterinės sistemos, išaiškinta, kad ji vis dėlto neapima paprasčiausio elektroninių laiškų ar rinkmenų siuntimo.

Ieškant minėtųjų perspektyvų ištakų matyti, kad joms susiformuoti padėjo gana įvairus užsienio valstybių požiūris į šią informacinės sistemos konfidencialumą pažeidžiančią nusikalstamą veiką. Atsižvelgiant į tai, baudžiamuosiuose įstatymuose (statutuose) pasirinkti skirtingi šios veikos aprašymo būdai ir prieigos aiškinimo variantai. Neretai plačias prieigos interpretavimo (atitinkamai jos vertinimo iš *išorinės perspektyvos)* galimybes lemia pateikiamas oficialus vartojamų sąvokų išaiškinimas arba pačios neteisėtos prieigos sudėtyje numatyti jos požymiai. Kaip pastarojo atvejo pavyzdį galima pateikti Jungtinės Karalystės 1990 metų Netinkamo naudojimosi kompiuteriais akto 1 straipsnyje nurodomą neteisėtos prieigos prie kompiuterinių duomenų sudėtį. Pagal šį straipsnį, baudžiamoji atsakomybė kyla, jeigu, be kitų požymių, yra nustatyta, kad kaltininkas privertė kompiuterį atlikti bet kokią funkciją, ketindamas užtikrinti prieigą prie programos ar jame laikomų duomenų, arba sudarydamas sąlygas, kad tokia prieiga būtų užtikrinta[220]. Kadangi šios nusikalstamos veikos sudėtyje įtvirtintas platus ir aiškių apribojimų neturintis prieigos apibūdinimas, tai mokslinėje literatūroje pateikiama paprasčiausio kompiuterio įjungimo, kenkimo programinės įrangos siuntimo ir kitų pavyzdžių, kurie šiuo atveju galėtų prilygti tokiam veiksmui[221].

Kita vertus, išvada, į kokią perspektyvą atsižvelgiama užsienio valstybėse aiškinant neteisėtą prieigą prie informacinės sistemos, turėtų priklausyti ne tik nuo tokios nusikalstamos veikos požymių aprašymo, bet ir nuo teismų praktikos, formuojamos šios kategorijos bylose. Praktinis teisės aktų taikymo lygmuo aktualus ir tais atvejais, kai prieigos išaiškinimas aktuose nepateikiamas (pavyzdžiui, Vokietijoje, Prancūzijoje, Estijoje, Lietuvoje), ir tada, kai teisės aktuose prieigos sąvoka yra atskleidžiama (pavyzdžiui, įvairių Jungtinių Amerikos Valstijų statutai). Kaip antai O. S. Kerris ir J. Cloughas[222], ana-

---

220 Computer Misuse Act [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://www.legislation.gov.uk/ukpga/1990/18/contents*>.

221 Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 63.

222 Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1625; Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 2011, 22: 155.

lizuodami įvairiose Jungtinėse Amerikos Valstijose priimtus teismų sprendimus, pabrėžė, kad vienais atvejais teismai, vadovaudamiesi *vidinės perspektyvos* kriteriais, bando susiaurinti gana plačius prieigos apibrėžimus, o kitais – priešingai – juos taiko pažodžiui. Kaip vienas iš siaurinamojo prieigos aiškinimo pavyzdžių nurodytinas Kanzaso valstijos Aukščiausiojo Teismo 1996 m. sprendimas baudžiamojoje byloje *Kanzaso valstija prieš Allen (State of Kansas v. Allen)*[223].

Šioje byloje nustatyta, kad kaltininkas naudojo savo kompiuterį (su įrengtu modemu) bandydamas apie 28 kartus interneto ryšiu susisiekti su „Southwestern Bell Telephone" bendrovės kompiuterio sistemos įrenginiais, kontroliuojančiais tarpmiestinių skambučių jungiklius. Sėkmingo sujungimo atveju jam būtų suteikta galimybė padaryti neribotą skaičių nemokamų tarpmiestinių skambučių. Pagal byloje pateiktus paaiškinimus, jungiantis prie sistemos, asmuo turėjo matyti prašymą įvesti vartotojo vartą ir slaptažodį. Tačiau tai, kad kaltininkas „peržengė" šį prisijungimo etapą ar bent bandė įvesti sistemos reikalaujamus duomenis, nebuvo nustatyta.

Teismas byloje prieigą prie kompiuterinės sistemos išaiškino pagal įprastinę ir suprantamą jos reikšmę, taip atsisakymas taikyti pakankamai plačią Kanzaso valstijos statuto 21-3755 paragrafo a dalies 1 punkte esančią jos sąvoką. Toks sprendimas buvo pagrįstas ankstesniais precedentais, kuriuose preziumuota, jog Statute vartojamiems žodžiams yra suteikta įprastinė jų reikšmė, kas ir leido teismui, vadovaujantis žodyne pateiktu prieigos išaiškinimu, t. y. kad prieiga pirmiausia rodo „laisvę ar galimybę gauti arba panaudoti". Atsižvelgiant į tai buvo konstatuota, kad tol, kol kaltininkas veikė neperžengdamas sistemos nustatytų apribojimų, negalima teigti, jog jis turėjo galimybę pasinaudoti „Southwestern Bell Telephone" kompiuteriais ar iš to ką nors gauti. Byloje prieita prie išvados, kad kaltininkas nebuvo gavęs prieigos prie šios bendrovės kompiuterinės sistemos.

Minėtosios perspektyvos aktualios aiškinantis, ir kaip plačiai Lietuvos BK 198[1] straipsnyje yra kriminalizuotas neteisėtas prisijungimas prie informacinės sistemos. Sprendžiant kokia, ar gana plačia arba siauresne, neteisėtos prieigos koncepcija buvo vadovaujamasi BK

[223] *State of Kansas v. Anthony A. Allen*, no. 74,639, Soupreme Court of Kansas, 1996 [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://files.grimmelmann.net/cases/Allen.pdf*>.

įtvirtinant neteisėto prisijungimo prie informacinės sistemos veiką, svarbu atsižvelgti ir į šios nusikalstamos veikos sudėties požymių tarpusavio ryšį. Būtent jų visuma ir padeda nustatyti neteisėto prisijungimo veikos apimtį, o tarpusavio sąsaja – apibrėžti atskirų šios veikos požymių turinį (neretai interpretuojant vieną iš jų tenka atsižvelgti į tai, kaip suprantami kiti). Apie siauresnį pavojingos veikos variantą Lietuvoje leidžia kalbėti prieigai įvardyti pasirinktas *prisijungimo* terminas ir kiti šios nusikalstamos veikos sudėties požymiai (pavyzdžiui, jos padarymo būdas, kuriam reikia nustatyti apsaugos priemonių pažeidimo prisijungiant prie informacinės sistemos faktą).

Pagal įprastinę reikšmę, prisijungimo veiksmas apibrėžiamas kaip „komanda, kuria prisijungiama prie tinklo arba sistemos ir pradedamas darbo seansas su ja“[224]. Remiantis tokiu aiškinimu, prisijungimo momentą galima laikyti darbo seanso su informacine sistema pradžia, neatsižvelgiant į priėjimo prie jos būdą (tiesiogiai arba naudojantis elektroninių ryšių tinklais). Kita vertus, tai nėra vienintelis šios pavojingos veikos interpretavimo būdas – aiškinant prisijungimą gali būti taikomas ir galimybės prieiti prie sistemos išteklių (programinės, techninės įrangos, duomenų) kriterijus. Nors BK 198[1] straipsnio dispozicijoje jis neminimas, bet apie tokį *naudos kriterijų* tarsi leistų kalbėti pati prisijungimo prie informacinės sistemos sąvoka. Dėl sėkmingo prisijungimo dažniausiai atsiranda galimybių sistemoje atlikti vienokio ar kitokio pobūdžio veiksmus (pavyzdžiui, elektroninės bankininkystės sistemoje atlikti finansines operacijas[225], pakeisti tinklalapio turinį[226], socialinio tinklalapio lankytojams priskirtus autentifikavimo duomenis[227] ar kitokius elektroninius duomenis[228] ir pan.).

---

[224] Dagienė, V., *et al*. Enciklopedinis kompiuterijos žodynas. Vilnius: TEV, 2008, p. 375.

[225] Pavyzdžiui, Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. N1-1470-88/2009; Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendis baudžiamojoje byloje Nr. 1-53-100/2009.

[226] Radviliškio rajono apylinkės teismo 2010 m. kovo 22 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-116-632/2010.

[227] Klaipėdos miesto apylinkės teismo 2009 m. liepos 1 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-770-795/2009.

[228] Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-515-487/2009.

Ne veltui teismų praktikoje prisijungimu laikomi *informacinės sistemos vartotojo ar abonento veiksmai, kuriais jis gali prieiti prie atitinkamos svetimos informacinės sistemos resursų (kompiuterio techninės įrangos, periferinių įrenginių, saugomos ar perduodamos kompiuterinės informacijos ir pan.)*[229]. Dėl to, kaip teigiama literatūroje, prisijungimo baigtumo momentas siejamas su realia kaltininko galimybe „pamatyti informacinės sistemos laikomas duomenų bylas, susipažinti su duomenų turiniu, atlikti kitus veiksmus (juos keisti, trinti, kopijuoti ir kt.)“[230]. Remiantis *naudos kriterijumi,* galima įžvelgti daug prisijungimo ir iš *vidinės perspektyvos* suvokiamos prieigos panašumų. Jau minėta, kad pagal įprastinį prieigos aiškinimą įvairiuose jos apibrėžimuose šalia įėjimo į sistemą nurodoma ir galimybė ja naudotis[231], galimybė prieiti prie sistemos išteklių[232] ar priėjimo prie duomenų ar informacinės sistemos gavimas[233]. Būtent toks siauresnis prieigos kaip „įėjimo į visą arba dalį sistemos“ aiškinimas pateikiamas ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje (46 punktas). Taigi, neatsižvelgiant į tai, ar prisijungimas yra laikomas komanda, kuria pradedamas darbo seansas su sistema, ar jam apibūdinti taikomas *naudos kriterijus* – abiem atvejais jis metaforiškai gali būti prilyginamas „virtualiajam įėjimui“ į informacinę sistemą. Paprasčiausios sąveikos ir prisijungimo atskyrimas irgi gali būti nustatomas analizuojant kokybinius „naudojimosi“ kompiuteriu, t. y. nusprendžiant, kokiu lygiu kaltininkas gali naudotis kompiuteriu[234], skirtumus. Dėl to veiksmai,

[229] Pavyzdžiui, Tauragės rajono apylinkės teismo 2017 m. birželio 15 d. nuosprendis baudžiamojoje byloje Nr. 1-70-607/2017; Panevėžio apygardos teismo 2015 m. sausio 29 d. nuosprendis baudžiamojoje byloje Nr. 1A-23-366/2015; Šiaulių apygardos teismo 2014 m. gegužės 7 d. nuosprendis baudžiamojoje byloje Nr. 1A-388-309/2014; Šilutės rajono apylinkės teismo 2015 m. sausio 9 d. nuosprendis baudžiamojoje byloje Nr. 1-20-351/2015.

[230] Abramavičius, A., *et al.* Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 436–437.

[231] Dictionary of Information Science and Technology. I tomas. Khosrow-Pour, M. (ed.). Hershey, Pa., *et al.* Idea Group Reference, 2007, p. 2.

[232] Dagienė, V., *et al*. Enciklopedinis kompiuterijos žodynas. Vilnius: TEV, 2008, p. 369.

[233] A Dictionary of Computing. 5-asis leidimas. Daintith, J. (gen. ed.). Oxford: Oxford University Press, 2004, p. 5.

[234] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 68.

kuriuos atlikus nepavyko prisijungti prie informacinės sistemos, galėtų būti vertinami tik kaip parengtinė nusikalstama veika, nes jais nėra pasiekiamas toks naudojimosi kompiuteriu lygis, kokį įgyja asmuo, sėkmingai prisijungęs prie informacinės sistemos. Be to, išvadą, kad šiai nusikalstamai veikai konstatuoti nepakanka tik sąveikos su sistema, leidžia daryti ir reikalavimas nustatyti jos apsaugos priemonių pažeidimą.

Kita vertus, tokiam prisijungimo prie informacinės sistemos aiškinimui reikia ir tam tikro patikslinimo. *Naudos kriterijus* iš tiesų padeda geriau suvokti prisijungimo prie informacinės sistemos esmę, bet šią veiką kriminalizavus *per se*, jos inkriminavimo neturėtų riboti tai, ar kaltininkas atliko tolesnius veiksmus sistemoje (pavyzdžiui, sistemoje galėjo būti nerasti norėti peržiūrėti duomenys arba jie apsaugoti slaptažodžiu, sistema veikė testuojamoje aplinkoje), ar prieš pažeisdamas informacinės sistemos konfidencialumą jis turėjo tyčią jau pačioje sistemoje atlikti kitas nusikalstamas veikas. Kadangi neteisėto prisijungimo prie informacinės sistemos nusikalstamos veikos sudėtis yra formali, jos baigtumo momentas turėtų būti siejamas su sėkmingo prisijungimo prie sistemos veiksmu, o ne kaltininko realiai atliktais tolesniais veiksmais sistemoje.

Apibendrinant galima teigti, kad Lietuvos BK kriminalizuotam prisijungimo veikos aiškinimui artimesnė yra *vidinės perspektyvos* pozicija, todėl šį veiksmą galima metaforiškai lyginti su „virtualiuoju įėjimu“ į informacinę sistemą. Patekimas į vidų sudaro sąlygas prieiti ir prie sistemos išteklių: techninės, programinės įrangos, duomenų ir kt., bet sprendžiant dėl šios veikos baigtumo momento neturėtų būti svarbūs tolesni kaltininko veiksmai sistemoje. Pačioje sistemoje padarytos kitos nusikalstamos veikos kvalifikuotinos pagal kitus BK straipsnius (pavyzdžiui, BK 182, 196, 198 straipsniai).

2.2.2. Prisijungimo neteisėtumo vertinimas

Didžiausia teisėto ir neteisėto prisijungimo prie informacinės sistemos atribojimo problema yra susijusi su privačių ir viešųjų erdvių, sukurtų elektroninėje erdvėje, atskyrimu ir tokių ribų nustatymo galimybėmis. Akivaizdu, kad šiuo atveju taikant privačios ir viešosios sferos koncepcijas, kurios suformuluotos veiksmams fizinėje erdvėje vertinti, dėl unikalių elektroninės erdvės savybių susiduriama su

tam tikrais sunkumais. Itin paplitęs interneto kaip „tam tikro serviso, prieinamo per „tinklų tinklą“ ir dažniausiai funkcionuojančio kaip viešoji vieta, reguliuojama tik numanomais leidimais, kuriais remiantis yra keičiamasi informacija“[235], suvokimas. Kiekvienas gali ne tik laisvai skelbti, bet ir naudodamasis paieškos priemonėmis gana lengvai gauti prieigą prie informacijos[236]. Tokia išvada yra pagrįsta pagrindine komunikavimo elektroninėje erdvėje filosofija, kad „ištekliai, kurių URL[237] yra žinomas, turėtų būti prieinami iš bet kurio į tinklą sujungto kompiuterio, nebent buvo imtasi techninių žingsnių padaryti juos neprieinamus“[238]. Toks požiūris į viešųjų ir privačių erdvių atskyrimą rodo esant ne tik teisinių, bet ir tam tikrų techninių kliūčių, iš dalies apibrėžiančių privačios elektroninės erdvės ribas. Šių ribų nustatymo būdas skiriasi nuo taikomo fizinėje erdvėje – elektroninėje erdvėje galimų veiksmų apribojimus nustato šios erdvės architektūra, pagrįsta kompiuterio kodu. Būtent „programinė ir techninė įranga, kuri sukuria elektroninę erdvę, nustato elgesio apribojimų rinkinį“[239]. Panašios technologijos, į kurias yra sąmoningai įmontuotas įtaką asmens elgesiui galintis daryti mechanizmas, apibrėžiamos „norminių technologijų“[240] terminu. Tokių technologijomis nustatytų suvaržymų turinys gali kaskart skirtis, bet būtent jos padeda numatyti prieigos prie elektroninės erdvės sąlygas. Pavyzdžiui, vienais atvejais informacinės sistemos konfidencialumas gali būti užtikrina-

---

235 Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 163.

236 Linzer, P. From the Gutenberg Bible to Net Neutrality - How Technology Makes Law and Why English Majors Need to Understand It. *McGeorge Law Review*, 2008, 39: 21.

237 URL (angl. *Uniform Resource Locator, Universal Resource Locator)* – ištekliaus unifikuotas (universalusis) rodmuo. Tai „standartizuotas adresų sistemos rodmuo, vartojamas multiterpinio elemento laikymo vietai pasaulinėje hipertekstinėje WWW sistemoje nustatyti“. (Paulauskas, K. V. Aiškinamasis kompiuterijos terminų santrumpų žodynas. Kaunas: Technologija, 2000, p. 301).

238 Reed, C. Internet: law text and materials. Cambridge: Cambridge University Press, 2004, p. 66.

239 Lessig, L. Code and other Laws of Cyberspace. New York (N.Y.): Basic books, 1999, p. 89.

240 Regulating Technologies. Brownsword, R.; Yeung, K. (eds). Oxford; Portland (Or.): Hart Publishing, 2008, p. 158.

mas įdiegus programinę prieigos kontrolės įrangą, o kitais – prieigai prie sistemos nebus nustatyta apskritai jokių ribojimų.

Šis aspektas itin svarbus analizuojant vertybių (ne išimtis ir informacinės sistemos konfidencialumo) apsaugos galimybes elektroninėje erdvėje. Atsižvelgiant į sukurtą kodą, vertybėms gali būti nustatoma didesnė arba mažesnė apsauga. Būtent tai ir leido L. Lessigui kelti klausimą, kokios vertybės turėtų būti „įmontuotos į erdvę“[241], kad joje paskatintų įvairias gyvenimo formas? Kalbėdamas apie elgesio suvaržymus elektroninėje erdvėje, jis atkreipė dėmesį į tai, kad „nėra pasirinkimo, kuris nebūtų susijęs su tam tikra *statyba*. Kodas niekada nėra randamas; jis visada yra sukuriamas <...>“[242]. Remiantis tokia autoriaus nuomone, galima daryti išvadą, kad prieigai prie informacinės sistemos nustatyti įvairūs apribojimai rodo priemones, kurių buvo imtasi šios sistemos konfidencialumui užtikrinti, ir atskleidžia jos savininko ar teisėto valdytojo požiūrį į prieigos prie sistemos galimybes bei sąlygas. Pabrėžtina, kad įvairių prieigos prie informacinės sistemos apribojimų taikymas dažniausiai yra nulemtas dėl saugumo politikos nustatytų sistemos saugos reikalavimų (pavyzdžiui, kam ir kokiomis sąlygomis suteikiama prisijungimo prie sistemos teisė). Atitinkamai spręstina, kokių apribojimų nepaisymas rodo prieigos prie informacinės sistemos neteisėtumą, taigi ir šios sistemos konfidencialumo pažeidimus.

BK 198[1] straipsnyje numatytas prisijungimo neteisėtumo nustatymo reikalavimas yra susijęs su Konvencijos dėl elektroninių nusikaltimų ir Direktyvos 2013/40/ES nuostatomis, kuriose numatyta pareiga kriminalizuoti ne bet kokią, o neteisėtą prieigą prie informacinės sistemos. Būtent prieigos neteisėtumas parodo įvairius informacinės sistemos konfidencialumo pažeidimus. Ir Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje, ir Direktyvos 2013/40/ES 3 straipsnyje nurodoma „neteisėta prieiga“, arba „prieiga neturint tam teisės“, prie visos informacinės sistemos ar jos dalies. Vadinasi, akivaizdu, kad šiais teisės aktais nereikalaujama kriminalizuoti tokių veiksmų, kai prieiga prie informacinės sistemos arba jos dalies gaunama turint sistemos

[241] Lessig, L. Code and other Laws of Cyberspace. New York (N.Y.): Basic books, 1999, p. 6.

[242] *Ibid*.

(arba jos dalies) savininko ar teisėto valdytojo leidimą[243]. Į tokio leidimo turėjimą, sprendžiant prieigos prie informacinės sistemos teisėtumo klausimą, atkreiptas dėmesys ir Konvencijos dėl elektroninių nusikaltimų aiškinamosios ataskaitos 47 punkte. Dėl to neteisėta prieiga prie informacinės sistemos nelaikytini jungimosi veiksmai prie atvirų ir viešai prieinamų sistemų (ar jų dalių).

Analizuojant teismų praktiką matyti, kad teismų sprendimuose pats prieigos neteisėtumo turinys atskleidžiamas gana retai. Šią tendenciją iš esmės lemia minėtoji glaudi prisijungimo, jo neteisėtumo ir saugumo priemonių pažeidimų sąsaja, todėl neteisėtumas dažniausiai konstatuojamas, pavyzdžiui, nurodžius konkrečius informacinės sistemos apsaugos priemonių pažeidimo veiksmus[244]. Jei teismų sprendimuose neteisėtumo turinys yra detalizuotas, matyti, kad jo suvokimas yra artimas minėtuosiuose tarptautiniuose ir ES teisės aktuose pateikiamam prisijungimo neteisėtumo aiškinimui. Kaip antai, pagal teismų praktiką, neteisėtumas reiškia, kad *asmuo neturi informacinės sistemos savininko ar teisėto valdytojo leidimo jungtis prie šios informacinės sistemos*[245]. Tais atvejais, kai informacinės sistemos savi-

[243] Šis aspektas yra aktualus kalbant apie saugumo patikras ir etiško įsibrovimo technologijas. Jos dažniausiai tapatinamos su įsiskverbimo testavimu, kuris, jei laikomasi visų tokiems testavimams keliamų reikalavimų, neturėtų būti vertinamas kaip nusikalstama veika, numatyta BK 198[1] straipsnyje. Būtent į neteisėto prisijungimo prie informacinės sistemos sudėtį įtraukiami neteisėtumo bei tyčios požymiai susiaurina šios veikos taikymo galimybes ir leidžia minėtųjų etiškų įsibrovimo veiksmų nelaikyti nusikalstamais. Be to, Direktyvos 2013/40/ES preambulės 17 punkte nurodoma, kad „šia direktyva nesiekiama nustatyti baudžiamosios atsakomybės tais atvejais, kai yra šioje direktyvoje numatytų objektyvių nusikalstamų veikų sudėties požymių, bet veiksmai padaromi <...> siekiant atlikti informacinių sistemų tikrinimą arba saugumo užtikrinimą turint tam leidimą, pavyzdžiui, kai įmonė arba pardavėjas paskiria asmenį patikrinti apsaugos sistemos patikimumą".

[244] Pavyzdžiui, Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendis baudžiamojoje byloje Nr. 1-53-100/2009; Radviliškio rajono apylinkės teismo 2010 m. kovo 22 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-116-632/2010.

[245] Pavyzdžiui, Tauragės rajono apylinkės teismo 2017 m. birželio 15 d. nuosprendis baudžiamojoje byloje Nr. 1-70-607/2017; Panevėžio apygardos teismo 2015 m. sausio 29 d. nuosprendis baudžiamojoje byloje Nr. 1A-23-366-2015; Kauno apygardos teismo 2015 m. gegužės 7 d. nutartis baudžiamojoje byloje Nr. 1A-432-594/2015; Šiaulių apygardos teismo 2014 m. gegužės 7 d. nuosprendis baudžiamojoje byloje Nr. 1A-388-309/2014; Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje Nr. 1-1430-276/2011.

ninkas ar teisėtas valdytojas „pasidalija slaptažodžiu“[246] su trečiąja šalimi, prieiga prie informacinės sistemos paprastai laikoma teisėta (tik turėtų būti nustatoma, kad šis asmuo veikė kaip savininko ar teisėto valdytojo atstovas, t. y. kaip jo *alter ego* arba „kitas aš“[247]). Pavyzdžiui, vienoje iš baudžiamųjų bylų konstatuota, kad kaltininkas pagal BK 198[1] straipsnį buvo išteisintas pagrįstai, nes nenustatytas prisijungimo prie informacinės sistemos neteisėtumas (bet pritarta nuteisimui pagal BK 182 straipsnio 1 dalį ir 215 straipsnio 1 dalį):

Prisijungimas prie informacinės sistemos turi būti neteisėtas. Neteisėtumas teismų praktikoje reiškia, kad asmuo neturi informacinės sistemos savininko ar teisėto valdytojo leidimo jungtis prie šios informacinės sistemos. Nustatyta, kad teisėtos elektroninės bankininkystės sistemos naudotojos nuteistosios motinos M. B. leidimu nuteistoji nuo 16 metų amžiaus naudojosi M. B. autentifikavimo kodais ir suteiktais kintamais slaptažodžių kortelės slaptažodžiais. Tai ji darė su motinos žinia, motina šiais duomenimis nesinaudojo, o tik jos dukra nuteistoji K. B. Už duomenų išsaugojimą yra atsakinga šių duomenų teisėta naudotoja M. B., kuri savo teises perleido dukrai K. B. Pirmosios instancijos teismas išsamiai pasisakė dėl nuteistosios veikos kvalifikavimo pagal BK 198[1] straipsnio 1 dalį ir pagrįstai K. B. pagal BK 198[1] straipsnio 1 dalį išteisino, nes nepadaryta veika, turinti šio nusikaltimo požymių[248].

Analizuojant neteisėtumo požymį matyti, kad vadovaujantis Konvencijos dėl elektroninių nusikaltimų ir Direktyvos 2013/40/ES nuostatomis, galima pastebėti tik vieną iš prieigos neteisėtumo interpretavimo variantų. Kiek išsamiau įvertinti šią problemą įmanoma remiantis skirtinga užsienio valstybių praktika aprašant neteisėtos prieigos prie informacinės sistemos veiką. Apibendrinus įvairius požiūrius į informacinės sistemos konfidencialumo pažeidimus, galima nurodyti dvi problemas: *pirma*, neteisėtumo turinio ir jo ribų nustatymo; *antra*, neteisėtumo konstatavimo, atsižvelgiant į prieigos prie sistemos apribojimus ir jų pažeidimo būdus.

Pirmasis klausimas parodo vieną iš mokslinėje literatūroje kylančių diskusijų, susijusių su dviem prieigos teisėtumo pažeidimo as-

---

246 Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review*, 2016, 116: 1178.

247 *Ibid*., p. 1179.

248 Vilniaus apygardos teismo 2014 m. birželio 5 d. nutartis baudžiamojoje byloje Nr. 1A-459-209/2014.

pektais, – neteisėta prieiga (angl. *unauthorized access)* ir prieiga, kuria peržengiamos teisėtumo ribos (angl. *exceeding authorized access)*, bei jų tarpusavio santykiu. Vadinasi, svarbu nustatyti, koks turinys yra suteikiamas neteisėtos prieigos požymiui, arba kitaip – „kaip nustatyti, kaip toli „prieiga turint tam teisę“ išsitęsia“[249]. Nagrinėjant minėtuosius prieigos prie informacinės sistemos būdus, daugelio mokslininkų[250] darbuose keliamas klausimas, ar gali būti nustatyti nusikalstamos veikos požymiai, jei teisėta prieiga prie informacinės sistemos buvo pasinaudota neteisėtiems tikslams. Tokia padėtis susiklosto tada, kai vartotojas, turintis teisę prieiti prie informacinės sistemos ir jos išteklių, viršija vidaus arba kitais teisės aktais nustatytas tokio leidimo ribas[251]. Dėl to svarbiausia spręstina problema yra ta, ar „teisėta prieiga, panaudota neteisėtiems tikslams, išlieka teisėta prieiga?“[252] Atsakymo į šį klausimą paieškas pasunkina įvairios neteisėtumo, prisijungiant prie informacinės sistemos, interpretavimo galimybės – nuo gana plataus požiūrio į šį požymį iki ganėtinai siauro. Aiškinimų įvairovę lemia ir minėtieji šios nusikalstamos veikos aprašymo skirtumai užsienio valstybių baudžiamuosiuose įstatymuose. Atsižvelgiant į pasirinktą tokios nusikalstamos veikos konstrukciją, vienose valstybėse yra tiesiogiai kriminalizuota neteisėta ir teisėtumo ribas peržengianti prieiga prie informacinės sistemos[253], kitose – numačius tik neteisėtos prieigos požymį, paliekamas atviras klausimas dėl jo turinio.

---

[249] Tompkins, Jr.; Mar, L. A. The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem. *Computer Law Journal*, 1986, 6: 464.

[250] Computer and Information security handbook. Vacca, J. R. (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 293; Bainbridge, D. Introduction to Computer Law. 5-asis leidimas, Harlow: Pearson: Longman, 2004, p. 385; Cybercrime: Digital Cops in a Networked Environment. Balkin, J., *et al*. (ed.). New York (N.Y.): New York University Press, 2007, p. 90–93; Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 164; Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1630. Computer Law: The Law and Regulation of Information Technology. 6-asis leidimas. Reed, C.; Angel, J. (eds.). Oxford: Oxford University Press, 2007.

[251] Computer Law: The Law and Regulation of Information Technology. 6-asis leidimas. Reed, C.; Angel, J. (eds.). Oxford: Oxford University Press, 2007, p. 569.

[252] Bainbridge, D. Introduction to Computer Law. 5-asis leidimas, Harlow: Pearson: Longman, 2004, p. 385.

[253] Pavyzdžiui, Jungtinių Amerijos Valstijų įstatymų sąvado 18 dalies (Nusikaltimai ir baudžiamasis procesas) 1030 paragrafas (18 U.S.C. § 1030).

Siekiant aiškiau suvokti neteisėtos prieigos ir tos, kuria peržengiamos teisėtumo ribos, santykį, galima remtis pašalinio asmens (angl. *outsider)* ir informacinės sistemos teisėto vartotojo (angl. *insider)* kriterijais bei atitinkamai vertinti išorinius ir vidinius prisijungimus prie informacinės sistemos. Būtent pašalinio asmens (kartais įvardijamo „svetimšalio" terminu)[254] ir teisėto vartotojo skirtumais yra pagrįstas neteisėtos ir teisėtumo ribas peržengiančios prieigos atskyrimas. Mokslinėje literatūroje[255] prieinama prie išvados, kad svarbiausia aplinkybė, leidžianti apibūdinti pašalinį asmenį, yra jo prieigos teisių prie informacinės sistemos nebuvimas, o tai rodo neteisėtą prisijungimą prie sistemos „iš išorės". Tokio pobūdžio veiksmai yra atliekami asmens, kuris neturi prieigos prie informacinės sistemos teisės, bet neteisėtai (pavyzdžiui, pažeisdamas sistemos saugumo priemones) siekia gauti tam tikro lygio prieigą prie jos. Dėl to tokiai prieigai apibūdinti dažniausiai taikoma „įsilaužimo ir įėjimo"[256] analogija. Kiek kitaip prieigos prie informacinės sistemos situacija atrodo, kai vertinami vartotojo, nustatytomis sąlygomis turinčio teisėtą prieigą prie sistemos, veiksmai. Kaip matyti literatūroje, tai yra asmenys, „kurie, atsižvelgiant į jų funkciją organizacijoje, turi tam tikro lygio autorizuotą prieigą prie informacinės sistemos ir jos terpės. Prieigos lygis gali kisti nuo paprasto vartotojo iki sistemos administratoriaus, turinčio beveik neribotas teises"[257]. Klausimas dėl šio asmens atsakomybės kyla tada, kai jis prisijungia prie informacinės sistemos turėdamas tikslą, kuriam įgyvendinti prieigos teisė nebuvo suteikta. Kadangi tai skirtingi nei įsibrovimo „iš išorės" atvejai, jiems apibūdinti dažniausiai taikomas kitas – teisėtumo ribas peržengiančios prieigos – požymis. Juo remiantis galima įžvelgti tokios veikos aiškinimų ir *ultra vires* doktrinos panašumų.

---

254 Štitilis, D. Elektroniniai nusikaltimai. Vilnius: Mykolo Romerio universitetas, 2011, p. 21.

255 Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1630; Cybercrime: Digital Cops in a Networked Environment. Balkin, J., *et al*. (ed.). New York (N.Y.): New York University Press, 2007, p. 90.

256 Cybercrime: Digital Cops in a Networked Environment. Balkin, J., *et al*. (ed.). New York (N.Y.): New York University Press, 2007, p. 90.

257 Computer and Information security handbook. Vacca, J. R. (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 293.

Taigi, vadovaujantis neteisėtos ir teisėtumo ribas peržengiančios prieigos požymiais, galima atskleisti dvi skirtingas prieigos prie informacinės sistemos puses. Juos abu įtraukus į nusikalstamos veikos sudėtį, šios veikos apibrėžtis neišvengiamai būtų išplėsta – tokiu atveju baudžiamoji atsakomybė kiltų ne tik už prieigą prie sistemos neturint tam teisės, bet ir už leistinos prieigos ribų peržengimą. Kaip pavyzdį galima pateikti Jungtinių Amerikos Valstijų įstatymų sąvado 18 U.S.C. § 1030 (a) (1)–(5) punktus[258], kuriuose *expressis verbis* numatyti neteisėtos ir teisėtumo ribas peržengiančios prieigos požymiai. Be to, galimi atvejai, kai sudėtyje nurodomas tik vienas – neteisėtos prieigos požymis, bet jo turinys išplečiamas teismų praktikoje. Kaip teigia W. S. Wong, Jungtinėje Karalystėje neteisėtos prieigos požymis priskiriamas abiem variantams, todėl tai, „kuris aspektas pabrėžiamas konkrečioje byloje, yra tik fakto klausimas ir priklauso nuo kiekvienos bylos aplinkybių“[259]. Pabrėžtina, kad šiose valstybėse plačias neteisėtumo interpretavimo galimybes suteikia pati jų teisės aktuose įtvirtinta neteisėtos prieigos nusikalstamos veikos konstrukcija. Vienas iš būdų, padedantis išvengti tokios veikos perteklinio kriminalizavimo, yra minėtojo patekimo į sistemą etapo susiejimas su tolesniais jau sistemoje atliekamais kaltininko veiksmais. Pasirinkus tokį veikos kriminalizavimo būdą, galima plačiau aiškinti ir patį neteisėtumo požymį bei atitinkamai sudaryti sąlygas formuotis lankstesniam požiūriui į jį.

Manytina, kad neteisėtumas kiek kitaip aiškinamas tais atvejais, kai neteisėta prieiga prie informacinės sistemos yra kriminalizuojama kaip pavojinga *per se*, t. y. jos nesiejant su tolesniais kaltininko veiksmais sistemoje ar jo nusikalstamais ketinimais. Tokiais atvejais galimybės kalbėti apie teisėtumo ribas peržengiančią prieigą yra gana ribotos – stengiantis išvengti baudžiamajai atsakomybei kilti būtino pavojingumo lygio nesiekiančių veiksmų kriminalizavimo, turėtų būti taikomas kur kas siauresnis neteisėtos prieigos aiškinimo būdas. Priešingu atveju į baudžiamosios teisės reguliavimo sritį patektų įvairūs civiliniai ar

[258] Išskyrus 18 U.S.C. § 1030(a) 3 punkte kriminalizuotą neteisėtą prieigą prie Jungtinių Amerikos Valstijų Vyriausybės kompiuterio, jei ši veika padarė poveikį tokiam kompiuterio naudojimui.

[259] Wong, M. W. S. Cyber-trespass and “Unauthorized Access“ as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1): 126.

drausminiai teisiniai santykiai[260]. Tokia aiškinimo tendencija matyti ir Direktyvoje 2013/40/ES. Jos Preambulės 17 punkte teigiama, kad „darbo ginčai dėl prieigos prie darbdavio informacinių sistemų ir jų naudojimo asmeniniais tikslais neturėtų užtraukti baudžiamosios atsakomybės, kai prieiga tokiomis aplinkybėmis būtų laikoma neteisėta ir todėl sudarytų pagrindą baudžiamajai atsakomybei". Tiesa, šioje direktyvoje pabrėžiama, kad palankesnės sąlygos nusikalstamoms veikoms elektroninėje erdvėje padaryti gali atsirasti tada, kai kaltininkas dėl einamų pareigų gauna prieigą prie informacinės sistemos, kuriai gali kilti grėsmė, todėl nacionalinėje teisėje turėtų būti atsižvelgiama ir į tokias aplinkybes (18 punktas).

Kaip bandymo nustatyti neteisėtos prieigos turinio ribas ir pakankamai siauro šio požymio aiškinimo pavyzdys minėtinas Merilando apeliacinio teismo 1998 m. sprendimas baudžiamojoje byloje *Briggs prieš Merilando valstiją (Briggs v. State of Maryland)*[261]:

Šioje byloje nustatyta, kad kompiuterių specialistas, bendrovėje prižiūrintis kompiuterinės sistemos veiklą, porą dienų prieš pokalbį dėl jo tolesnio darbo bendrovėje kai kurias kompiuterines rinkmenas įkėlė į katalogą pavadinimu „ha-ha he-he" ir prieigą prie jų apribojo tik jam žinomu slaptažodžiu. Kaltininkui, be kitų nusikalstamų veikų, taip pat buvo inkriminuota neteisėtos prieigos veika, numatyta tuo metu galiojusio Merilando kodekso §146 (c) (2) (i) 27 straipsnyje[262]*. Pirmosios instancijos teismas pripažino, kad bendrovės darbuotojas, nors ir turėjo prieigos teisę prie sistemos, tačiau jam nebuvo suteikta teisė prieiti prie jos tokiu būdu, kad būtų sutrikdytos kompiuterinės sistemos teikiamos paslaugos. Su tokia išvada nesutikdamas kaltininkas teigė, kad ši veika, numatyta minėtajame straipsnyje, yra susijusi tik su veiksmais, kurie atliekami neturint prieigos teisės prie sistemos (pavyzdžiui, kalbant apie programišių*

[260] Pavyzdžiui, informacinės sistemos saugumui užtikrinti gali būti imtasi įvairių administracinių priemonių, kurioms priskiriamos ir darbuotojų darbo taisyklės, pareiginės instrukcijos ir pan.

[261] *Briggs v. State of Maryland*, no. 24, Court of Appeals of Maryland, 1997 [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://law.justia.com/cases/maryland/court-of-appeals/1998/24a97-2.html*>.

[262] Vėlesniais pakeitimais Merilando kodekso 7-302 paragrafe numatyta ne tik neteisėta prieiga prie kompiuterio ar duomenų, bet ir tokia, kuria peržengiamos teisėtumo ribos (The Code of Maryland [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://law.justia.com/codes/maryland/2010/criminal-law/title-7/subtitle-3/7-302*>).

(angl. hacker), įsibraunančių į sistemą, veiksmus). Šis straipsnis, anot jo, neapima teisėtumo ribas peržengiančios prieigos, kai suteikta prieiga yra tiesiog naudojama netinkamu būdu. Apeliacinės instancijos teismas pritarė tokiems argumentams ir konstatavo, kad šiam darbuotojui iš tiesų buvo suteikta prieigos teisė. Taip pat teismas atkreipė dėmesį į tai, kad pačioje normoje nėra tiesioginių nuorodų į sistemos vartotojų veiksmus, kurie viršija jiems suteiktų leidimų ribas. Teismas akcentavo, kad jei teisės aktų leidėjas būtų siekęs kriminalizuoti tokius veiksmus, jis tą būtų aiškiai nurodęs normos tekste. Todėl šioje byloje prieita prie išvados, kad minėtąja norma siekta kriminalizuoti tik tuos netinkamo naudojimosi kompiuteriu ar kompiuteriniais tinklais atvejus, kai pati prieiga yra neteisėta.

Prieigos neteisėtumo požymis yra numatytas ir Lietuvos BK 198[1] straipsnyje. Nustatant jo turinio ribas, turėtų būti atsižvelgiama ne tik į tai, kad ši nusikalstama veika, kaip minėta, yra kriminalizuota *per se*, bet ir į kitus neteisėtumą padedančius suvokti sudėties požymius. Pavyzdžiui, šios veikos padarymo būdas, įtvirtintas BK 198[1] straipsnyje atsižvelgiant į Konvencijos dėl elektroninių nusikaltimų ir Direktyvos 2013/40/ES nuostatas, apibūdinamas kaip informacinės sistemos apsaugos priemonių pažeidimas. Apsaugos priemonių tikslas – užtikrinti prisijungimo prie sistemos galimybę tik prieigos teisę turintiems vartotojams, todėl manytina, kad dėl tokio požymio atsiranda sąlygos kalbėti apie siauresnį neteisėtos prieigos turinį, į šią veiką neįtraukiant teisėtumo ribas peržengiančios prieigos. Dėl to nustačius, kad asmuo, turintis prieigos teisę prie informacinės sistemos, tuo pasinaudojo įgyvendindamas tikslus, kuriems įgyvendinti nebuvo suteikta prieigos teisė, BK 198[1] straipsnis netaikytinas. Ši išvada neužkerta kelio kaltininkui inkriminuoti kitas jo padarytas nusikalstamas veikas, nes prisijungimas prie informacinės sistemos turint tam teisę savaime nereiškia, kad ir kiti kaltininko veiksmai sistemoje yra teisėti. Kadangi atskirai yra vertinami informacinės sistemos konfidencialumo pažeidimai, tai atskirai vertintini ir kiti, pavyzdžiui, elektroninių duomenų konfidencialumo, integralumo, prieinamumo ar kitų teisinių vertybių pažeidimai. Dar svarstytina, ar į šią aplinkybę negalėtų būti atsižvelgiama kaltininkui individualizuojant bausmę už informacinėje sistemoje padarytas kitas nusikalstamas veikas (jų didesnį pavojingumą rodytų tai, kad kaltininkas turėjo teisėtą prieigą prie sistemos ir ja piktnaudžiavo). Be to, neatmestina galimybė kvalifikuojant

padarytas veikas taikyti BK 228 straipsnį, jei yra nustatyta specialaus subjekto, didelės žalos ir kitų piktnaudžiavimo veikai inkriminuoti reikšmingų požymių. Pavyzdžiui, BK 228 straipsnio taikymo atveju yra aktuali Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2018 m. gegužės 31 d. nutartis baudžiamojoje byloje Nr. 2K-7-84-489/2018, kurioje valstybės tarnautojo (vartotojo, dirbančio su registrais ir informacinėmis sistemomis) veiksmai prisijungiant prie policijos informacinės sistemos registrų, surenkant bei vėliau perduodant informaciją apie privatų asmenų gyvenimą, pripažinti piktnaudžiavimu (BK 228 straipsnis).

Tokį požiūrį į neteisėtą prieigą galima įžvelgti šiuo klausimu analizuojant žemesniosios instancijos teismų praktiką, nors ir negausią. Pavyzdžiui, vienoje iš baudžiamųjų bylų kaltininkas buvo atleistas nuo baudžiamosios atsakomybės pagal BK 40 straipsnį už BK 198 straipsnio 1 dalyje, 198[1] straipsnio 1 dalyje ir 210 straipsnyje numatytų nusikalstamų veikų padarymą. Šis nuosprendis aktualus tuo požiūriu, kad jame buvo sprendžiamas buvusio darbuotojo prisijungimo prie informacinės sistemos teisėtumo klausimas. Nustačius, kad kaltinamasis prie informacinės banko sistemos prisijungė tada, kai jam buvo panaikinta prieigos prie visų banko sistemų teisė, tokie veiksmai pripažinti neteisėtais ir kvalifikuoti pagal BK 198[1] straipsnio 1 dalį. Teismas šioje byloje nustatė, kad T. Č. *laikotarpiu nuo 2010 m. spalio 13 d. iki 2010 m. gruodžio 8 d., (duomenys neskelbtini) banko patalpose (duomenys neskelbtini), per jo darbo vietoje esantį kompiuterį <...>, nenustatyta programine įranga nustatęs ir vėliau (ikiteisminio tyrimo nenustatytu laiku) savavališkai pakeitęs prisijungimo prie (duomenys neskelbtini) banko tarnybinėse stotyse administruojamos neviešos informacinės sistemos administratoriaus slaptažodį, 2011 m. balandžio 13 d. 12 val. 01 min., neteisėtai, t. y. neturėdamas šios informacinės sistemos savininko ar teisėto valdytojo leidimo jungtis prie šios informacinės sistemos, tyčia, pažeisdamas šios sistemos apsaugos priemones, prisijungdamas prie šios banko informacinės sistemos kaip neribotą prieigos teisę turintis vartotojas, būdamas pasirašytinai susipažinęs su (duomenys neskelbtini) banko informacijos klasifikavimo reikalavimais, neteisėtai nukopijavo į savo išorinį duomenų kaupiklį <...>, šioje sistemoje saugomus neviešus elektroninius duomenis <...> ir tokiu būdu įgijo minėtuosius neviešus elektroninius duomenis, kurie yra komercinę paslaptį sudaranti informacija, po to laikė*

juos savo kontroliuojamose informacijos laikmenose – išoriniame duomenų kaupiklyje <...>, iki 2011 m. balandžio 29 d. apie 19 val., taip pat – išoriniuose duomenų kaupikliuose <...>, ir patalpose (duomenys neskelbtini) buvusiame asmeniniame nešiojamajame kompiuteryje <...> iki 2011 m. gegužės 5 d. 13 val. 45 min.“ Įvertinęs byloje esančius įrodymus, teismas konstatavo, jog *„<...> visiškai įrodyta, kad T. Č. padarė nusikalstamas veikas, numatytas LR BK 198 straipsnio 1 dalyje, 198[1] straipsnio 1 dalyje, 210 straipsnyje“*[263].

Nustačius, kad darbuotojas, turėdamas teisę prisijungti prie informacinės sistemos, ja pasinaudojo kitoms nusikalstamoms veikoms padaryti, BK 198[1] straipsnyje numatyta neteisėto prisijungimo veika teismų praktikoje paprastai neinkriminuojama. Pavyzdžiui, vienoje iš baudžiamųjų bylų buvo sprendžiamas notaro biure dirbančio asmens baudžiamosios atsakomybės klausimas. Nuosprendyje nurodyta, kad *Ž. Š. neteisėtai perėmė ir panaudojo neviešus elektroninius duomenis, o būtent: jis, laikotarpiu nuo 2006-07-01 iki 2007-01-30, pasinaudojęs (duomenys neskelbtini) notaro biurui suteiktu prisijungimo vardu (duomenys neskelbtini) ir slaptažodžiu (duomenys neskelbtini), ikiteisminio tyrimo metu tiksliai nenustatytu laiku ir vietoje, iš kompiuterių su kintamais IP adresais (duomenys neskelbtini) 386 kartus neteisėtai prisijungė prie Registro centro duomenų bazės bei stebėjo ir fiksavo neviešus elektroninius duomenis apie privačių asmenų turimą kilnojamąjį ir nekilnojamąjį turtą, tokiu būdu padarė (duomenys neskelbtini) notarų biurui 5 606 Lt turtinę žalą.* Iš Ž. Š. parodymų nustatyta, kad jis *dirbdamas (duomenys neskelbtini) notaro biure nuo 2002 m. iki 2006 m. birželio mėnesio padėjėju, <...> turėjo teisę prisijungti prie Registro centro duomenų bazės. Jis žinojo, kad asmeniškai, savo reikmėms prisijunti prie Registro centro duomenų bazės negalima. Kai išėjo iš darbo, jis savo reikmėms prisijungdavo prie Registro centro duomenų bazės iš skirtingų kompiuterių, kurie priklausė jam, draugams, interneto kavinėms. Prisijungdavo tikslu gauti duomenis apie asmenų nekilnojamąjį turtą*[264]. Esant tokioms aplinkybėms, Ž. Š. prisijungimo prie informacinės sistemos veiksmai pagal BK 198[1] straipsnį nebuvo vertinami[265]. Panašią praktiką galima matyti

[263] Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje Nr. 1-1430-276/2011.

[264] Vilniaus rajono apylinkės teismo 2009 m. rugsėjo 8 d. nuosprendis baudžiamojoje byloje Nr.1-278-298/2009.

[265] Ž. Š. veika kvalifikuota pagal BK 228 straipsnio 1 dalį ir 198 straipsnio 1 dalį.

analizuojant ir kitų teismų praktiką elektroninių nusikalstamų veikų baudžiamosiose bylose[266].

Antrasis prisijungimo neteisėtumui interpretuoti svarbus aspektas yra susijęs su prieigos prie informacinės sistemos apribojimo būdais ir atitinkamai pagal juos suskirstytais prieigos neteisėtumo pasireiškimo variantais. Šiai analizei yra svarbios informacinės sistemos savininko ar teisėto valdytojo taikomos priemonės, kurios padeda nustatyti prisijungimo prie sistemos sąlygas ir atitinkamas teises sistemos vartotojams. Vadinasi, sprendžiant dėl galimybės taikyti BK 198[1] straipsnį bendriausia prasme vertintini trys aspektai: elektroninės erdvės pobūdis (viešoji, neviešoji ir pan.), būdai, kuriais leidžiama teisėta prieiga prie šios erdvės, ir prieigos prie informacinės sistemos aplinkybės[267]. Kaip teigia O. S. Kerris, nors apie leidimą prieiti prie informacinės sistemos yra kalbama kaip apie „monolitinę sąvoką“[268], iš tiesų ji parodo du pagrįstai vieną nuo kito atskirtus prieigos apribojimo būdus. Vienas iš jų yra pagrįstas *kompiuterio kodu*, kitas – *sutartimi*. Toks atskyrimas matyti ir kitų mokslininkų darbuose analizuojant bene analogiškus *kodu* ir *sutartimi* nustatytus apribojimus, kuriais apibrėžiamos prieigos prie kompiuterio sąlygos arba tokia prieiga draudžiama[269]. Būtent toks skirstymas mokslinėje literatūroje leido nustatyti du atskirus neteisėtos prieigos prie informacinės sistemos gavimo būdus – prieigą apeinant *kodu* apibrėžtas ribas ir prieigą pažeidžiant *sutartimi*[270] pagrįstus apribojimus. Analizuojant teismų praktiką, gali-

---

[266] Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-617-885/2011.

[267] Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review*, 2016, 116: 1146–1147.

[268] Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1644.

[269] Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 2011, 22: 166; Wong, M. W. S. Cyber-trespass and "Unauthorized Access" as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1): 124.

[270] Susitarimu pagrįsti prieigos prie informacinės sistemos apribojimai siejami su nuostatomis ir sąlygomis, kurių turi laikytis asmuo, gaudamas prieigą prie informacinės sistemos (toks būdas gali būti įvardijamas ir kaip prieiga prie informacinės sistemos *per spustelėjimą* (angl. *click-through agreement)*. Šie apribojimai peržengiami, kai asmuo, gaudamas prieigą prie sistemos, nesilaiko nustatytų susitarimo sąlygų.

ma matyti, kad būtent dėl reguliavimo *kodu* pažeidimų vertinimo iš tiesų kyla nemažai problemų.

Elektroninės erdvės ribų ir galimybių joje klausimas pirmiausia gali būti sprendžiamas taikant *kompiuterio kodą*, kuris, anot L. Lessigo, ir padeda sukurti elektroninę erdvę tokią, kokia ji yra – nustatant tam tikrus suvaržymus ir suteikiant leidimus. Atitinkamai informacinės sistemos konfidencialumo apsauga užtikrinama būtent per jį[271]. *Reguliavimą kodu* savo darbuose analizavo ir O. S. Kerris, kuris tokį terminą pasiūlė, atsižvelgdamas į tai, kad prieigos kontrolė tiesiogiai priklauso nuo *kompiuterio kodo*, sudarančio kliūtį įgaliojimų ribas viršijančių vartotojų veiksmams[272]. Taigi toks veiksmų elektroninėje erdvėje reguliavimas siejamas su „technine kliūtimi“[273] – tam tikrais techninės ar programinės įrangos konfigūravimais, leidžiančiais nustatyti atitinkamo lygio apribojimus, taikomus prieigai prie informacinės sistemos ar jos išteklių. Bendriausia prasme teigtina, kad prieigos kontrolės mechanizmas apsaugo sistemą nuo galimų taikomos saugumo politikos pažeidimų, kai prie sistemos jungiamasi „iš išorės“ arba joje tam tikrus veiksmus atlieka prieigos teisę prie jos turintys vartotojai. Kita vertus, kalbant apie *kodu* nustatytus apribojimus, būtina atpažinti tuos „techninius barjerus“, kurių nepaisymas laikomas neteisėta prieiga prie sistemos baudžiamąja teisine prasme. Vadinasi, O. S. Kerrio teigimu, „kai dėl prieigos ribų ir suvaržymų nereikalaujama vartotojo autentiškumo patvirtinimo, prieiga prie informacinės sistemos išlieka atvira visiems“[274]. Tokie atvejai galėtų būti, pavyzdžiui, prieigos prie informacinės sistemos ribojimas tik sistemos naudojimosi sąlygomis (angl. *terms of use)*, su kuriomis turi sutikti potencialus sistemos vartotojas. Tokia išvada doktrinoje yra daroma atsižvelgiant į tai, kad

Tokius atvejus mokslinėje literatūroje siūloma priskirti ne baudžiamosios, o civilinės teisės reguliavimo sričiai (plačiau žr. Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1649–1660).

[271] Lessig, L. Code and other Laws of Cyberspace. New York (N.Y.): Basic books, 1999, p. 12.

[272] Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1644.

[273] Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 2011, 22: 166.

[274] Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review*, 2016, 116: 1143.

„prieiga, reguliuojama tik rašytinėmis naudojimosi sąlygomis, nėra prieiga, reikalaujanti autentiškumo patvirtinimo“[275]. Tokių aiškinimo galimybių suteikia ir Direktyvos 2013/40/ES preambulės 17 punktas, kuriame teigiama, kad „sutartiniai įsipareigojimai arba susitarimai apriboti prieigą prie informacinių sistemų taikant naudojimo politiką arba veiklos sąlygas, <...> neturėtų užtraukti baudžiamosios atsakomybės, kai prieiga tokiomis aplinkybėmis būtų laikytina neteisėta ir todėl sudarytų pagrindą baudžiamajai bylai“. Šie pastebėjimai svarbūs ir dėl to, kad leidžia pabrėžti, jog iš baudžiamosios teisės pozicijų svarbu įvertinti ne tik prieigos veiksmų teisėtumą (ar neteisėtumą), bet ir nuspręsti, ar neteisėti veiksmai yra būtent nusikalstami.

Reguliavimo kodu apėjimo sąvoka irgi nėra vientisa – ji parodo dvi alternatyvias prieigos kontrolės nustatytų apribojimų pažeidimo rūšis: *pirma*, autentifikavimo procedūros pažeidimus; *antra*, pasinaudojimą informacinės sistemos saugumo silpnosiomis vietomis[276], siekiant paveikti jos atliekamas funkcijas[277]. Beje, panašų skirstymą įmanoma rasti ne tik mokslinėje literatūroje, bet ir užsienio valstybių baudžiamuosiuose įstatymuose. Pavyzdžiui, Estijos baudžiamojo įstatymo 217 paragrafe, kuriame numatoma atsakomybė už neteisėtą naudojimąsi kompiuterine sistema, nurodoma neteisėta prieiga prie kompiuterinės sistemos pašalinant arba apeinant jos kodą, slaptažodį arba kitas apsaugos priemones.

Pirmieji – autentifikavimo procedūros[278] pažeidimo atvejai yra gana akivaizdūs ir neturėtų kelti didesnių tokio pobūdžio veiksmų

---

[275] Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review*, 2016, 116: 1165.

[276] Nurodant programinės įrangos saugumo problemas, vartojami įvairūs terminai: defektas, programavimo klaida, yda, apsirikimas ir pan. (plačiau žr. Plėštys, R., *et al*. Tinklų sauga. Kaunas: Vitae Litera, 2008, p. 50). Nors kiekvienas iš jų turi tam tikrą specifinę reikšmę, toliau siekiant išvengti terminų painiavos vartojamas bendrasis *informacinės sistemos saugumo silpnųjų vietų* terminas.

[277] Computer and Information security handbook. Vacca, J. R. (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 94; Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1644–1645.

[278] Identifikavimas, autentifikavimas ir autorizacija yra skirtingo turinio sąvokos. Autentifikuojant identifikavimo duomenys yra susiejami su autentifikavimo duomenimis ir atitikimo atveju teigiama, kad vartotojo tapatybė yra nustatyta. Autorizuojant autentifikuotam vartotojui suteikiama įvairių jam numatytų galimybių atlikti

neteisėtumo konstatavimo problemų. Pačią galimybę gauti neteisėtą prieigą prie informacinės sistemos, naudojantis svetimais vartotojo tapatybę patvirtinančiais duomenimis, lemia asmens identifikavimo elektroninėje erdvėje specifika. Ir fizinėje, ir elektroninėje erdvėje asmenims, siekiantiems atlikti tam tikrus veiksmus, dažniausiai prireikia patvirtinti savo tapatybę. Kita vertus, skirtingai nei fizinėje, elektroninėje erdvėje toks identifikavimas vyksta asmeniui tiesiogiai nedalyvaujant, t. y. „norint identifikuoti, nereikia fiziškai būti atitinkamoje geografinėje vietoje“[279]. Kaip minėta, elektroninė erdvė yra informacinės sistemos veiklos rezultatas, vadinasi, autentifikavimas joje vyksta atsižvelgiant į komunikavimo elektroninėje erdvėje ypatumus. Būtent jie leidžia tapatybę analizuoti grynai techniniu požiūriu ir ją laikyti tiesiog „skaitmeniniu pseudonimu“[280], kuris reprezentuoja asmenį. Atitinkamai technologijos turėtų padėti užtikrinti ne tik tai, kad asmuo, identifikuodamas save, galėtų nevaržomai naudotis tokiu pseudonimu, bet ir tai, kad kitiems asmenims nebūtų suteikta galimybė pasinaudoti šiuo pseudonimu. Akivaizdu, kad tokia asmens tapatybės nustatymo procedūra yra kur kas sudėtingesnė, nes tarp asmenų įsiterpia tarpinė – informacinių technologijų – grandis. Būtent tokia komunikavimo elektroninėje erdvėje specifika rodo ne tik asmenų ir technologijų ar pačių technologijų sąveiką, bet neretai ir *automatizuotą* tam tikrų veiksmų pobūdį. Vadinasi, klaidinimo dėl asmens tapatybės veiksmai elektroninėje erdvėje tiesiogiai nukreipiami ne prieš konkretų autentifikavimo procedūrą atliekantį asmenį, o prieš technologijas, taikomas autentifikavimo procedūrai palengvinti (įvykdyti), kai minėtasis asmuo tiesiogiai šioje procedūroje gali ir nedalyvauti. Į informacinės sistemos suklaidinimo galimybę, kaltininkui save pateikiant kaip teisėtą šios sistemos vartotoją, atkreiptas dėmesys ir teismų praktikoje: prie tokios išvados pirmą kartą buvo prieita minėtojoje Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus

veiksmus sistemoje (Plėštys, R., *et al*. Tinklų sauga. Kaunas: Vitae Litera, 2008, p. 35). Monografijoje šios sąvokos vartojamos taip, kaip ir analizuojamųjų autorių darbuose, be to, parenkamos atsižvelgiant į kontekstą.

279 Štitilis, D., *et al*. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai. Vilnius: Mykolo Romerio universitetas, 2011, p. 22.

280 *Ibid*, p. 31.

teisėjų kolegijos 2001 m. spalio 9 d. nutartyje baudžiamojoje byloje Nr. 2K-682/2001. Nors šiuo Lietuvos Aukščiausiojo Teismo išaiškinimu siekta pagrįsti apgaulės kaip objektyvaus sukčiavimo sudėties požymio buvimą kaltininko veikoje, jis aktualus ir tuo, kad jame pripažįstama ne tik asmens, bet ir informacinės sistemos suklaidinimo galimybė. Dėl to šis sistemos suklaidinimo aspektas svarbus analizuojant ne tik finansinės operacijos inicijavimą, bet ir nustatant kitų kaltininko veiksmų neteisėtumą, panaudojus ne jam priklausančias autentifikavimo elektroninėje erdvėje priemones.

Neteisėtam prisijungimui būtinus duomenis kaltininkas galėjo gauti įvairiai: naudodamasis socialinės inžinerijos (pavyzdžiui, prisijungimo prie informacinės sistemos duomenų „žvejyba“ (angl. *phishing)* ar apgaulinga IP taktika (angl. *pharming)*, kenkimo programine įranga ir daugeliu kitų galimų būdų[281]. Baudžiamosios atsakomybės neturėtų padėti išvengti ir ta aplinkybė, kad kaltininkui prisijungimo duomenys tapo prieinami dėl to, kad interneto naršyklė ar kitos teisėto vartotojo anksčiau naudotos programos, kurioms reikia tapatybės patvirtinimo, suteikė galimybę išsaugoti jo prisijungimo duomenis. Nors tokiais atvejais prie informacinės sistemos prisijungiama automatiškai, kai kaltininkui nereikia iš naujo įvesti prisijungimo duomenų, toks prisijungimas neturėtų būti laikomas teisėtu. Prisijungimo veiksmų teisėtumo tokiais atvejais nepagrindžia ir tai, kad kaltininkas netaikė specialių slaptažodžių sužinojimo priemonių ir tyčia neieškojo prisijungimo duomenų, o tokia prieigos galimybė jam pasitaikė atsitiktinai[282]. Kaip fizinėje erdvėje pamestas raktas nelaikomas atviru kvietimu užeiti į tam tikrą privačią erdvę, taip ir palikti prisijungimui prie informacinės sistemos ar jos dalies būtini duomenys nerodo jos savininko ar teisėto valdytojo viešo leidimo naudotis šia sistema (ar jos dalimi).

Remiantis teismų praktika matyti, kad autentifikavimo procedūrų pažeidimai nėra reti ir, kaltininkui inkriminuojant BK 198[1] straipsnyje numatytą nusikalstamą veiką, jie leidžia konstatuoti prisijungimo

[281] Plačiau žr. Kalpokas, V.; Marcinauskaitė, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos*, 2012, Nr. 3(77): 33–39.

[282] Šiaulių apylinkės teismo 2017 m. gruodžio 7 d. baudžiamasis įsakymas byloje Nr. 1-995-899/2017.

veiksmų prie informacinės sistemos neteisėtumą[283]. Iš to galima daryti išvadą, kad siekiant neteisėtai prisijungti pakanka panaudoti teisėtam sistemos vartotojui suteiktus ir jam autentifikuoti skirtus duomenis. Galimi ir tokie atvejai, kai neteisėta prieiga prie informacinės sistemos gaunama ir kitu būdu – pasinaudojant silpnosiomis informacinės sistemos saugumo vietomis.

Analizuojant antrąją *reguliavimo kodu* apėjimo rūšį, atkreiptinas dėmesys į tai, kad tokiu neteisėtu būdu prie informacinės sistemos gali būti prisijungiama „per pažeidžiamas vietas saugumo sistemoje, panaudojus nedokumentuotas operacinės sistemos galimybes“[284]. Tokių galimybių nustatymas ir pasinaudojimas jomis leidžia išvengti standartinės procedūros, kontroliuojančios prieigą prie informacinės sistemos. Sėkmingai pasinaudojusiam tokiu pažeidžiamumu asmeniui sistemoje gali būti suteikiamos administratoriaus ar jam prilyginamos teisės. Kai tik „pašalietis“ gauna tokio lygio prieigą, jis gali valdyti sistemą, įgyti joje esančius duomenis arba ją panaudoti kitų sistemų atakoms[285]. Pabrėžtina, kad įvairių galimybių apeiti kodu nustatytą reguliavimą gali atsirasti ir dėl jau esamų informacinės sistemos saugumo silpnųjų vietų, ir dėl kaltininko tikslingų veiksmų jas sukuriant (pavyzdžiui, pasinaudojus kenkimo programine įranga).

Aptariant tokį neteisėto prisijungimo prie informacinės sistemos būdą pabrėžtina, kad programą sudaro sudėtingi taisyklių rinkiniai ir tam tikra jų vykdymo seka, kuri nurodo sistemai, ką ši turėtų daryti. Kaip teigiama literatūroje, „programa gali atlikti tik tai, kas joje užpro-

---

[283] Pavyzdžiui, Kauno apylinkės teismo 2018 m. vasario 28 d. baudžiamasis įsakymas byloje Nr. 1-1154-825/2018; Klaipėdos apygardos teismo 2017 m. spalio 12 d. nutartis baudžiamojoje byloje Nr. 1A-279-651/2017; Klaipėdos apygardos teismo 2015 m. vasario 19 d. nuosprendis baudžiamojoje byloje Nr. 1A-38-255/2015; Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. baudžiamasis įsakymas byloje Nr. N1-1470-88/2009; Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje Nr. 1-1430-276/2011; Klaipėdos miesto apylinkės teismo 2009 m. birželio 29 d. baudžiamasis įsakymas byloje Nr. 1-740-93/2009.

[284] Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 10.

[285] Computer and Information security handbook. Vacca, J. R. (red). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 294.

gramuota, skrupulingai iki paskutinio simbolio“[286]. Kadangi programa iš tiesų atlieka tik tas funkcijas, kurioms ji buvo sukurta, tai kitokias jos funkcijas lemia pačios programos ar jos vykdymo aplinkos defektai arba tiesiog klaidos. Pasinaudojus tokiomis sistemos saugumo silpnosiomis vietomis galima priversti programą veikti jai nenumatytu būdu. Informacinė sistema, kuri yra netinkamai sukonfigūruota arba jos programinė įranga turi žinomų saugumo spragų, gali suteikti prieigos teisę neautorizuotiems vartotojams. Pavyzdžiui, galima paminėti „buferio perpildymo“[287] (angl. *buffer overruns)* saugumo spragą, kuri leidžia suaktyvinti pasirinktą kodą ar komandas ir tokiu būdu gauti prieigą prie informacinės sistemos. Ši galimybė atsiranda tada, kai perpildytos programos darbas tampa neprognozuojamas ar net priešingas jos paskirčiai. Dėl to prieigos teisė prie informacinės sistemos kaltininkui suteikiama neįvedus tinkamo slaptažodžio. Pasinaudojus šia spraga, atsiranda galimybė gauti „pagrindinio vartotojo statusą ir neribotą prieigą prie visų kompiuteryje esančių duomenų“[288]. Tokiems būdams gali būti priskirta ir „SQL komandos įterpimo“[289] (angl. *SQL command injection)* ataka, kuri leidžia prisijungti prie informacinės sistemos nežinant teisėto jos vartotojo slaptažodžio, ir daugelis kitų būdų. Dėl to akivaizdu, kad dėl esamų ar sukurtų sistemos silpnųjų saugumo vietų gauta prieiga prie jos, kaip ir minėtaisiais autentifikavimo procedūros pažeidimo atvejais, turėtų būti pripažįstama kaip neteisėta.

Mokslinėje literatūroje, aptariant įvairius prieigos neteisėtumo nustatymo aspektus, tokiai išvadai pagrindą suteikė Jungtinių Amerikos Valstijų apeliacinio teismo (2-osios apygardos) 1991 m. kovo 7 d. sprendime byloje *Jungtinės Amerikos Valstijos prieš R. T. Morris (US*

---

[286] Plačiau žr. Erickson, J. Hakingas. Programų kodo narstymo menas. 2-asis pataisytas ir papildytas leidimas. Kaunas: Smaltija, 2010, p. 117.

[287] Plačiau žr. Whitman, M. E., *et al*. Principles of information security. 3-ioji laida. Boston: Thomson: Course Technology, 2009, p. 75; McClure, S., *et al*. Apsauga nuo hakerių: tinklo saugumo palaikymo paslaptys ir sprendimai. Kaunas: Smaltija, 2006, p. 216–220.

[288] Plačiau žr. Erickson, J. Hakingas. Programų kodo narstymo menas. 2-asis pataisytas ir papildytas leidimas. Kaunas: Smaltija, 2010, p. 124.

[289] Plačiau žr. Kazanavičius, E., *et al*. Programų sauga [elektroninis išteklius]: mokomoji knyga. Kaunas: TEV, 2011, p. 98; Whitman, M. E., *et al*. Principles of information security. 3-ioji laida. Boston: Thomson: Course Technology, 2009, p. 75.

v. Morris)[290] suformuluotas precedentas. Šioje byloje kaltininkas buvo nuteistas pagal Kompiuterinio sukčiavimo ir piktnaudžiavimo panaudojant kompiuterius akto 2 (d) skyrių ir tuo metu galiojusio Jungtinių Amerikos Valstijų įstatymų sąvado 1030 paragrafo a dalies 5 (A) punktą (18 U.S.C. § 1030 (a) (5) (A)) už tyčinį įsikišimą į kompiuterių sistemos darbą. Teismas, priimdamas tokį sprendimą, kartu suformulavo naują neteisėtos prieigos nustatymo kriterijų, kuris mokslinėje literatūroje vėliau buvo pavadintas „numatytų funkcijų“[291] kriterijumi.

Šioje byloje nustatyta, kad kaltininkas sukūrė programą, žinomą „interneto kirmino“ pavadinimu. Šios programos tikslas buvo išnaudoti kompiuterinio tinklo saugumui užtikrinti naudotų priemonių silpnąsias vietas, kurias kaltininkas buvo nustatęs. Programa taip pat galėjo plisti kompiuterių tinklais po to, kai buvo įterpta į kompiuterį, prijungtą prie tinklo. Šioje byloje, be kitų klausimų, spręstos ir neteisėtos prieigos prie kompiuterio (18 U.S.C. § 1030(a) (5) (A) inkriminavimo galimybės. Joje konstatuota, kad kaltininko prieiga prie kompiuterių buvo neteisėta, nes jis išnaudojo programų silpnąsias vietas, todėl programa nenumatytu būdu jam suteikdavo prieigą prie kompiuterių. Kaip nurodė teismas, kaltininkas nenaudojo nė vienos iš programų ypatybių taip, kaip leisdavo numatytos jų funkcijos. Priešingai – jis rasdavo programose spragas, kurias išnaudojęs gaudavo specialų ir neteisėtą prieigos kelią prie kito kompiuterio. Būtent tai teismui sudarė galimybes konstatuoti prieigos neteisėtumo faktą.

Nors teismas ir nedetalizavo naujai suformuluoto programos „numatytų funkcijų“ kriterijaus, mokslinėje literatūroje jam interpretuoti buvo skiriama nemažai dėmesio. Kaip teigiama, šis kriterijus gali būti kildinamas iš „socialinių normų, susiformavusių kompiuterių naudotojų bendruomenėje, prasmės“[292]. Jos atspindi paprastą logiką – programinė įranga kuriama tam tikriems tikslams pasiekti, o programa, kai sudaromos sąlygos ja naudotis, turėtų būti naudojama tik pagal savo paskirtį, neiškreipiant jos atliekamų funkcijų. Galimybė naudotis programa nesuteikia vartotojams leidimo neteisėtai pasinau-

[290] *United States v. Morris*, no. 774, United States Court of Appeals, 2nd Circuit, 1991 [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://www.loundy.com/CASES/US_v_Morris2.html*>.

[291] Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1632.

[292] *Ibidem*.

doti jos silpnosiomis vietomis ir priversti programą atlikti jai nenumatytų (nebūdingų) funkcijų. Vadinasi, kaltininkui gavus prieigą prie informacinės sistemos nenumatytu būdu, t. y. pasinaudojus programoje esančiomis saugumo spragomis, tokia prieiga turėtų būti laikoma neteisėta. Jei prieiga prie informacinės sistemos yra uždrausta, toks draudimas „uždaro abejas – priekines ir užpakalines – duris“[293], be to, uždraudžiami ir bet kokie kiti būdai, kuriais gali būti sudarytos sąlygos neteisėtai prisijungti prie sistemos. Čia kaip ir fizinėje erdvėje – paprastai įėjimas į patalpą yra galimas pro priekines duris, o jeigu jos uždarytos, tai „atviras langas nėra kvietimas pro jį įšokti ir patekti į vidų“[294]. Beje, minėtasis aiškinimas taikomas ir tada, kai kaltininkas pasinaudojo jau esamomis silpnosiomis informacinės sistemos saugumo vietomis, ir tada, kai jis tikslingais veiksmais pats jas sukūrė.

Analizuojant Lietuvos teismų praktiką matyti, kad nedažnai pasitaiko tokių prisijungimų neteisėtumo vertinimo atvejų. Kita vertus, pavieniai teismų sprendimai leidžia daryti išvadą, kad prieigos prie informacinės sistemos gavimas, pasinaudojus programinės įrangos saugumo silpnosiomis vietomis, vis dėlto pripažįstamas kaip neteisėtas. Pavyzdžiui, galima paminėti jau aptartą Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendį baudžiamojoje byloje Nr. 1-53-100/2009, kuriame dėl banko programoje buvusių spragų gauta prieiga pripažinta neteisėta, ir J. V., be kitų, inkriminuota ir BK 198[1] straipsnyje nurodyta nusikalstama veika.

Taigi apibendrinant galima teigti, kad prisijungimo prie informacinės sistemos neteisėtumas konstatuotinas nustačius, jog šiam veiksmui atlikti nebuvo gautas sistemos savininko ar teisėto valdytojo leidimas. Nors patiės prisijungimo neteisėtumą galima aiškinti iš įvairių pozicijų, BK 198[1] straipsnyje jis turėtų būti siejamas tik su neteisėtu, o ne su teisėtumo ribas peržengiančiu prisijungimu. Tokiu atveju prisijungimo prie informacinės sistemos neteisėtumas turėtų būti nustatomas atsižvelgiant ir į autentifikavimo procedūros pažeidimus, ir į sistemos saugumo silpnųjų vietų panaudojimą.

---

293 Madison, M. J. Authority and Authors and Codes. *The George Washington Law Review*, 2016, 84(6): 1631.

294 Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review*, 2016, 116: 1143.

2.3. Informacinės sistemos apsaugos priemonių pažeidimas – nusikalstamos veikos padarymo būdas

Neteisėto prisijungimo prie informacinės sistemos būdas – šios sistemos apsaugos priemonių pažeidimas yra vienas iš kriterijų, kuriais remiantis nustatomos neteisėto prisijungimo inkriminavimo ribos ir, kaip minėta, nusprendžiama, kokia neteisėto prisijungimo koncepcija gali būti pasirinkta kriminalizuojant tokią veiką Lietuvos BK 198[1] straipsnyje. Šio straipsnio sudėtyje esančio objektyviojo požymio ištakos yra siejamos su Konvencijos dėl elektroninių nusikaltimų 2 straipsnio ir Direktyvos 2013/40/ES 3 straipsnio nuostatomis. Jose tiesiogiai numatyta galimybė neteisėto prisijungimo prie informacinės sistemos veiką susiaurinti iki prisijungimo būdų, kuriais pažeidžiamos informacinės sistemos apsaugos priemonės.

Nors dėl reikalavimo nustatyti apsaugos priemonių pažeidimą turėtų būti užtikrinamas pakankamas neteisėto prisijungimo prie informacinės sistemos pavojingumo lygis (būtinas baudžiamajai atsakomybei kilti), vis dėlto atsižvelgiant į technologinį nusikalstamos veikos aspektą kyla tam tikrų analizuojamojo požymio interpretavimo problemų. Jų priežastys, kaip ir jau aptartų objektyviųjų požymių atveju, yra susijusios su technologinio neutralumo principo taikymu aprašant neteisėto prisijungimo veiką. Be to, apsaugos priemonių pažeidimo aiškinimo sunkumų kyla ir dėl nuolat sprendžiamo minėtojo technologijų bei terminologijos klausimo. Siekiant detaliau analizuoti šias problemas, reikėtų rasti atsakymą į keletą klausimų: *pirma*, kaip turėtų būti suvokiamos informacinės sistemos apsaugos priemonės; *antra*, kaip reikėtų interpretuoti tokių priemonių pažeidimus; *trečia*, ar apsaugos priemonių pažeidimo nustatymas visais atvejais leistų išspręsti šios veikos perteklinio kriminalizavimo problemą. Kadangi, kaip minėta, BK 198[1] straipsnyje numatytos veikos pagrindas yra informacinės sistemos, o ne elektroninių duomenų konfidencialumo pažeidimas, todėl pirmiausia analizuotinos pačios informacinės sistemos, o ne jose esančios elektroninių duomenų apsaugos priemonės.

Taigi, ieškant tokių priemonių sampratos, reikėtų atkreipti dėmesį į tai, kad atsižvelgiant į požiūrį joms gali būti suteikta ir plati, ir gana siaura prasmė. Pirmasis atvejis yra siejamas su kompleksiniu saugumo užtikrinimo požiūriu ir leidžia nustatyti pačių įvairiausių būdų prieigai prie informacinės sistemos pasunkinti – „nuo organiza-

cinių-administracinių draudimų iki specialiųjų kompiuterių įrangos priemonių“[295]. Pritarus tokiai nuomonei, svarbu suvokti ir šių būdų tarpusavio ryšį. Pavyzdžiui, organizacinės priemonės pirmiausia turėtų būti palaikomos fizinėmis ir techninėmis priemonėmis, kita vertus, „techninėms apsaugos priemonėms reikia atitinkamos organizacinės paramos“[296]. Toks gana platus požiūris[297] leidžia joms bendriausia prasme priskirti moralines ir etines[298], teisines[299], organizacines (administracines)[300], fizines[301] ir technines (aparatines ir programines) priemones. Be to, galima pabrėžti, kad dėl glaudžios informacinės sistemos ir elektroninių duomenų sąsajos šis klasifikavimas neretai taikomas aptariant ir informacinės sistemos, ir elektroninių duomenų (informacijos) kompleksinius saugumo užtikrinimo sprendimus – įvairialypius metodus ir priemones[302].

---

295 Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 12.

296 Kazanavičius, E., *et al*. Informacijos saugos vadyba. Kaunas: Vitae Litera, 2008, p. 24.

297 Kazanavičius, E. *et al*. Programų sauga [elektroninis išteklius]: mokomoji knyga. Kaunas: TEV, 2011, p. 23; Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 11.

298 Tai „elgesio normos, kurios tradiciškai susiklostė arba formuojasi šalyje ir visuomenėje didėjant kompiuterių paplitimo lygiui“. (Kazanavičius, E., *et al*. Informacijos saugos vadyba: mokomoji knyga. Kaunas: Kauno technologijos universitetas, 2008, p. 23). Šios normos paprastai nėra privalomos kaip norminiai teisės aktai.

299 Literatūroje vadinamos ir įstatymų leidybos apsaugos priemonėmis. Joms priskiriami „įstatymai, norminiai aktai ir standartai, kuriais reglamentuojamos ribotos prieigos informacijos naudojimo ir apdorojimo taisyklės, taip pat apibrėžiamos atsakomybės už šių taisyklių pažeidimą priemonės“. (Venčkauskas, A.; Toldinas, E. Kompiuterių ir operacinių sistemų sauga: mokomoji knyga. Kaunas: Vitae Litera, 2008, p. 11).

300 Tai priemonės, „reglamentuojančios duomenų apdorojimo sistemos funkcionavimo procesus, jos išteklių naudojimą, personalo veiklą, taip pat vartotojų sąveikos su sistema tvarką, siekiant pasunkinti ir užkirsti saugumo grėsmių realizavimo galimybę“ (Kazanavičius, E., *et al*. Informacijos saugos vadyba: mokomoji knyga. Kaunas: Kauno technologijos universitetas, 2008, p. 23–24).

301 Literatūroje techninės priemonės dažniausiai yra siejamos su įvairiais mechaniniais, elektriniais įrenginiais, skirtais sudaryti fizines kliūtis prieiti prie sistemos komponentų. Joms dar priklauso ryšio, apsaugos signalizacijos ir vizualaus stebėjimo techninės priemonės (Kazanavičius, E., *et al*. Informacijos saugos vadyba: mokomoji knyga. Kaunas: Kauno technologijos universitetas, 2008, p. 24).

302 Pavyzdžiui, minint informacijos apsaugą literatūroje nurodomos bene analogiškos techninės ir organizacinės saugumo užtikrinimo priemonės (plačiau žr. Budnikas, A., *et al*. Elektroninės valdžios sauga. Kaunas: Vitae Litera, 2008, p. 52).

Siauresnis neteisėto prisijungimo būdo aiškinimas yra paremtas išimtinai technologiniu požiūriu ir leidžia vadovautis technologine apsaugos priemonių koncepcija. Šiuo atveju apsaugos priemonės siejamos tik su minėtąja aparatine ir programine įranga, „skirta apsaugoti informacinę sistemą nuo įvairaus pobūdžio pažeidimų ir duomenų praradimo dėl techninių priežasčių ar neteisėtų veiksmų“[303]. Kadangi šios priemonės atlieka apsaugos funkciją, literatūroje jos neretai yra įvardijamos kaip „kompiuterių saugumo servisai“[304]. Jos padeda spręsti įvairius sistemos apsaugos uždavinius: „pavyzdžiui, prieigos kontrolė, apimanti autentifikavimo ir autorizacijos procedūras; auditas; informacijos šifravimas; antivirusinė apsauga; tinklo duomenų srauto kontrolė ir daug kitų uždavinių“[305]. Kadangi apsaugos priemonių esama gana įvairių (pavyzdžiui, ugniasienės, prieigos kontrolės mechanizmai ir kt.), bendriausia prasme būtų galima teigti, kad neteisėtam prisijungimui prie informacinės sistemos turėtų būti būdingi aparatinės arba programinės įrangos nustatytų apribojimų pažeidimai. Atsakyti į klausimą, kokiu požiūriu į apsaugos priemones vadovavosi įstatymų leidėjas, numatydamas baudžiamąją atsakomybę už neteisėtą prisijungimą prie informacinės sistemos, kol kas yra sudėtinga. Kadangi BK 198[1] straipsnyje numatytos nusikalstamos veikos sudėties požymiai suformuluoti pagal Konvencijos dėl elektroninių nusikaltimų ir Direktyvos 2013/40/ES nuostatas, viena vertus, galima kalbėti apie siauresnę apsaugos priemonių sampratą. Pavyzdžiui, Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje minimi įvairūs tik technologiniai informacinės sistemos apsaugos priemonių aspektai (49 punkte). Technologine apsaugos priemonių koncepcija vadovavosi ir BK 198[1] straipsnį komentavę autoriai[306]. Kita vertus, dėl tokio siauresnio nusikalstamos veikos padarymo būdo interpretavimo kyla ir diskusinių klausimų.

---

303 Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 436.

304 Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008, p. 12.

305 *Ibidem*.

306 Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 436.

Vienas iš tokių momentų yra susijęs su informacinių sistemų, kuriose nėra jokių saugumo užtikrinimo mechanizmų, konfidencialumo apsauga. Neteisėto prisijungimo veikai suteikus gana siaurą apibrėžtį tampa akivaizdu, kad prieiga prie apsaugos priemonių neturinčios sistemos negalės būti kvalifikuojama pagal BK 198[1] straipsnį[307]. Esant tokioms situacijoms tiesiog nebūtų įmanoma kaltininko veikoje nustatyti informacinės sistemos apsaugos priemonių buvimo ir jų pažeidimo fakto, taigi atitinkamai ir šios veikos padarymo būdo. Tokia neteisėto prisijungimo koncepcija iš dalies galėtų būti pateisinama tuo, kad BK 198[1] straipsnyje esanti veika yra kriminalizuota *per se*, nenurodant ryšio su kitomis jau sistemoje padaromomis nusikalstamomis veikomis. BK kiekvienas nusikalstamų veikų elektroninėje erdvėje padarymo mechanizmo etapas yra suskirstytas į atskiras, t. y. viena su kita nesusijusias, veikas. Būtent dėl tokio atsakomybės už neteisėtą prisijungimą nustatymo būdo atsiranda gana ribotų plataus ir laisvo jos požymių interpretavimo galimybių. Kaip minėta, tokios problemos yra susijusios su neteisėto prisijungimo veikos perteklinio kriminalizavimo rizika. Kita vertus, dėl tokio neteisėto prisijungimo suvokimo neužkertamas kelias kaltininko veikoje įžvelgti ir kitų nusikalstamų veikų, padarytų jau pačios informacinės sistemos viduje (pavyzdžiui, jei kaltininkas, prisijungęs prie sistemos, neteisėtai įgijo, laikė, pašalino, pakeitė ar darė kitokį poveikį elektroniniams duomenims, sutrikdė ar nutraukė informacinės sistemos darbą ir pan.).

Kitas diskutuotinas technologinės koncepcijos aspektas yra susijęs su sudėtingomis situacijomis, kai gali tekti vertinti pačių apsaugos priemonių (aparatinės ir programinės įrangos) pakankamumą. Kaip teigia I. Waldenas, „įvedus saugumo priemonių ribą, tikėtina, kad dėl to gali būti sukurtas didesnis teisinis netikrumas <...>“[308]. Pirmiausia dėl to, kad sudėtyje numačius apsaugos priemonių pažeidimo požymį

---

[307] Tai kelia klausimų dėl informacinės sistemos, kurioje nėra jokių saugumo užtikrinimo mechanizmų, pakankamos konfidencialumo apsaugos. Analogišką pastebėjimą, analizuodamas ne informacines sistemas, o elektroninius duomenis, pateikė ir J. Cloughas, kuris minėtuosius reikalavimus pavadino *nesąžiningai diskriminuojančiais* (Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 2011, 22: 169).

[308] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 162.

lieka neaišku, ar būtina įvertinti ir tokių priemonių „tinkamumą arba protingumą“[309]. Tokių abejonių gali kilti ir dėl Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje pateiktų pastebėjimų (49 punktas). Joje teigiama, kad bendru susitarimu neteisėtos prieigos prie informacinės sistemos veika turėtų būti kriminalizuota, bet tam tikrų dvejonių valstybėse kyla tais atvejais, kai šia veika nepadaroma žalos, arba net tada, kai aptinkamos silpnosios sistemos saugumo vietos. Nors reikėtų pripažinti, kad nesant aiškių kriterijų, kaip turėtų būti vertinamas priemonių pakankamumas, tokio kriterijaus taikymas dar labiau apribotų neteisėto prisijungimo veikos inkriminavimo galimybes ir keltų bereikalingų diskusijų konstatuojant šio požymio buvimą kaltininko veikoje. Vadinasi, galima teigti, kad dėl įvairių saugumo priemonių trūkumų nereikėtų paneigti pačių apsaugos priemonių buvimo fakto. Be to, toks reikalavimas galėtų būti laikomas nepagrįstu ir jį vertinant iš nukentėjusiojo pozicijos. Rūpestingumui nustatyti šiuo atveju turėtų pakakti fakto, kad jis ėmėsi atitinkamų saugumo priemonių, siekdamas pašaliniam asmeniui parodyti, kad prisijungimas prie informacinės sistemos yra ribotas, o ne reikalauti, kad jis apsaugos priemones padarytų kone neįveikiamas. Prie tokios išvados leidžia prieiti ir lygiavertis veiksmų fizinėje bei elektroninėje erdvėje vertinimas – norint konstatuoti įsibrovimą fizinėje erdvėje, nebūtina nustatyti, kad buvo imtasi priemonių, dėl kurių kaltininkui kilo itin sunkiai įveikiamų kliūčių[310]. Atitinkamai ir elektroninėje erdvėje, jei nukentėjusysis, pavyzdžiui, nepakeitė gamintojo nustatytų pirmi-

---

309 *Ibidem*.

310 Įsibrovimo doktrinoje daugiausia dėmesio skiriama įvairių neteisėto patekimo į patalpą, saugyklą, saugomą teritoriją ar kt. būdų analizei. Pavyzdžiui, aptariamas neteisėtas patekimas įsilaužiant, naudojantis apgaule ar kitais būdais (plačiau žr.: Piesliakas, V. Grobimas įsibraunant į butą, patalpą ar kitokią saugyklą. *Socialistinė teisė*, 1984, Nr. 1; Drakšienė, A. Baudžiamoji atsakomybė už vagystę. *Teisė*, 2000, Nr. 37, taip pat Lietuvos Aukščiausiojo Teismo senato 2005 m. birželio 23 d. nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“. *Teismų praktika*, 2005, Nr. 23). Pačių apsaugos priemonių nustatymas dažniausiai yra aktualus kalbant apie saugyklos, saugomos teritorijos sąvokas ir įsibrovimą į jas, tačiau bet kuriuo iš šių atvejų diskusija galėtų kilti dėl būtinumo nustatyti tokių priemonių buvimą (pavyzdžiui, automobilį pripažįstant saugykla), bet ne dėl esamų priemonių efektyvumo. Jei kaltininkas suvokia nustatytas ribas fizinėje erdvėje, tai, ar apsaugos priemonės galėjo jį sulaikyti nuo nusikalstamos veikos padarymo, kvalifikuojant jo veiką įtakos neturėtų daryti.

nių prisijungimo duomenų, neatnaujino programinės įrangos ar jo įdiegta programinė įranga turi žinomų saugumo spragų ir daugeliu kitų atvejų, neturėtų paneigti pačių apsaugos priemonių pažeidimo fakto. Juo labiau kad apie tokias išimtis nesudaro sąlygų kalbėti ir pats BK 198[1] straipsnis.

Kitas jau minėtas klausimas yra susijęs su technologijų ir terminologijos problema, t. y. pačių informacinės sistemos apsaugos priemonių pažeidimo interpretavimu. Kadangi BK 198[1] straipsnio dispozicijoje nusikalstama veika aprašyta kaip neteisėtas prisijungimas prie informacinės sistemos pažeidžiant jos apsaugos priemones, natūraliai gali kilti klausimas, ar apsaugos priemonių pažeidimas turėtų būti siejamas su joms padaroma žala. Ar vis dėlto tokią nusikalstamos veikos padarymo būdo formuluotę galima interpretuoti ir kitaip – kaip apsaugos priemonėmis nustatytų apribojimų (reikalavimų) pažeidimą. Būtent pastarasis aiškinimas galėtų būti išvedamas, nors ir iš negausios, dar tik besiformuojančios, bet šiuo požiūriu aiškios kasacinės instancijos teismų praktikos neteisėto prisijungimo prie informacinės sistemos baudžiamosiose bylose. Bene akivaizdžiausi žalos nepadarymo pačioms informacinės sistemos apsaugos priemonėms atvejai yra tie, kai kaltininko veiksmais pažeidžiami autentifikavimo mechanizmais nustatyti prisijungimo prie sistemos apribojimai. Šiais atvejais žalą sukeliantis poveikis sistemos apsaugai nebūtinas, nes prieigai prie jos gauti pakanka apgaulės atliekant autentifikavimo procedūrą (sistemai neteisėtai pateikiant jos teisėto vartotojo duomenis). Toks būdas leidžia suklaidinti informacinę sistemą, kuri kaltininkui suteikia prieigą nepadarius jokio neigiamo ar žalą sukeliančio poveikio pačioms sistemos apsaugos priemonėms. Taigi informacinės sistemos apsaugos priemonių pažeidimas turėtų būti konstatuotas ir tada, kai apsaugos priemonėms padaroma žalos (pavyzdžiui, sukuriamos silpnosios saugumo vietos arba apskritai pašalinamos saugumo priemonės), ir tada, kai pažeidžiami jų nustatyti apribojimai nesukeliant žalos pačioms apsaugos priemonėms (pavyzdžiui, pasinaudojimas silpnosiomis saugumo vietomis, autentifikavimo procedūros pažeidimai).

Jau minėta, kad vartotoją elektroninių paslaugų sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo užtikrinimo priemonių. Analizuojant kasacinės instancijos teismo praktiką matyti, kad tokių priemonių

pažeidimai nesiejami išimtinai tik su pačioms elektroninių paslaugų sistemos apsaugos priemonėms padaroma žala. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2016 m. sausio 26 d. nutartyje baudžiamojoje byloje Nr. 2K-4-507/2016 atkreiptas dėmesys į tai, kad aiškinant *informacinės sistemos apsaugos priemonių pažeidimo požymį, kasacinėse nutartyse pabrėžta, jog: 1) vartotoją informacinėje sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo (taip pat ir konfidencialumo) užtikrinimo priemonių, 2) teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir 3) neteisėtas prisijungimas prie informacinės sistemos (internetinės bankininkystės sistemos) pažeidžiant autentifikavimo priemonėmis nustatytų prisijungimo prie informacinės sistemos apribojimus (reikalavimus) paprastai negali būti laikomas nereikšmingu, vertinant jį iš baudžiamosios teisės pozicijų, ypač jei tai leido padaryti kitus neteisėtus veiksmus sistemoje* (kasacinės nutartys baudžiamosiose bylose Nr. 2K-375/2012, 2K-138/2015, 2K-555-788/2015). Požiūris, kad informacinės sistemos apsaugos priemonių pažeidimas konstatuotinas ir tada, kai šios įdiegtos priemonės yra suklaidinamos neteisėtai įvedus teisėto vartotojo duomenis, palengva įsitvirtina ir žemesniosios instancijos teismų praktikoje[311]. Tai sudaro sąlygas kalbėti apie vis labiau plėtojamą apgaulės, kuria pripažįstama ne tik asmens, bet ir informacinės sistemos suklaidinimo galimybė, doktriną. Analizuojant žemesniosios instancijos teismų praktiką galima matyti, kad informacinės sistemos apsaugos priemonių pažeidimai šių teismų sprendimuose yra aprašomi įvairiai (ir pažeidimas, ir apėjimas ar suklaidinimas)[312], bet jie nesiejami išimtinai tik su žalos pačioms minėtosioms priemonėms padarymu:

[311] Kauno apygardos teismo 2017 m. gruodžio 4 d. nuosprendis baudžiamojoje byloje Nr. 1-284-594/2017; Alytaus rajono apylinkės teismo 2017 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-68-297/2017; Šiaulių apylinkės teismo 2016 m. gruodžio 21 d. nuosprendis baudžiamojoje byloje Nr. 1-957-771/2016; Vilniaus miesto apylinkės teismo 2018 m. kovo 15 d. nuosprendis baudžiamojoje byloje Nr. 1-782-506/2018.

[312] Pavyzdžiui, Raseinių rajono apylinkės teismo 2017 m. kovo 22 d. nuosprendis baudžiamojoje byloje Nr. 1-9-237/2017; Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendis baudžiamojoje byloje Nr. 1-53-100/2009; Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. baudžiamasis įsakymas byloje Nr. N1-724-276/2010;

Prisijungimu pažeidžiant informacinės sistemos apsaugos priemones laikoma, jei priėjimas prie informacinės sistemos resursų yra gaunamas apeinant informacinės sistemos saugumo politikos nustatytas procedūras ir procesus. Toks pažeidimas gali būti ir procedūrinio, ir techninio pobūdžio: prisistatant kitu vartotoju, įvedant ne savo slaptažodį, panaudojant nusikaltimams daryti tiesiogiai skirtus ar pritaikytus įrenginius ar kompiuterines programas, išvengiant identifikacijos, apeinant užkardas (ugniasienes) ir pan., taip pat panaudojant silpnąsias vietas sistemos apsaugoje[313].

Siekiant tikslumo reikėtų pabrėžti, kad ankstesnėje teismų praktikoje pasitaikydavo siauresnės apimties, todėl diskutuotinų, apsaugos priemonių pažeidimo interpretavimo atvejų, dėl kurių apsaugos priemonių pažeidimo požymiui buvo suteiktas itin siauras turinys. Vadovaujantis tokiais išaiškinimais, informacinės sistemos apsaugos priemonių pažeidimą buvo galima konstatuoti tik tuo atveju, jei kaltininkas būtų jas sugadinęs, pakenkęs jų funkcionavimo režimui arba sutrikdęs informacinės sistemos darbą ir pan.[314] Pavyzdžiui, vienoje iš baudžiamųjų bylų kaltininkas pagal BK 198[1] straipsnio 1 dalį buvo išteisintas, nes nepadaryta veika, turinti nusikaltimo ar baudžiamojo nusižengimo požymių: *Nagrinėjamuoju atveju iš byloje nustatytų aplinkybių visumos matyti, kad kaltinamasis A. R., atlikdamas neteisėtus veiksmus, tik siekė pasisavinti svetimus pinigus. Byloje nebuvo nustatyta, kad kaltinamasis būtų siekęs pamatyti informacinėje sistemoje laikomas duomenų bylas, susipažinti su duomenų turiniu, atlikti kitus veiksmus (juos keisti, trinti, kopijuoti ir t. t.), kad jo veiksmai būtų buvę nukreipti prieš elektroninių duomenų ir informacinių sistemų saugumą, kad jis prie informacinės sistemos prisijungė pažeisdamas apsaugos priemones, t. y. jas sugadindamas ar pakenkdamas apsaugos priemonių režimui, todėl nėra pagrindo daryti išvados, kad kaltinamasis A. R. padarė nusikaltimą,*

Klaipėdos miesto apylinkės teismo 2009 m. liepos 1 d. baudžiamasis įsakymas byloje Nr. 1-770-795/2009.

313 Tauragės rajono apylinkės teismo 2017 m. birželio 15 d. nuosprendis baudžiamojoje byloje Nr. 1-70-607/2017.

314 Pavyzdžiui, Vilniaus miesto apylinkės teismo 2013 m. sausio 25 d. nuosprendis baudžiamojoje byloje Nr. 1-258-716/2013; Šakių rajono apylinkės teismo 2015 m. birželio 18 d. nuosprendis baudžiamojoje byloje Nr. 1-21-829/2015; Panevėžio apygardos teismo 2015 m. sausio 29 d. nuosprendis baudžiamojoje byloje Nr. 1A-23-366/2015; Kauno apygardos teismo 2015 m. gegužės 7 d. nutartis baudžiamojoje byloje Nr. 1A-432-594/2015.

numatytą Lietuvos Respublikos BK 198[1] straipsnio 1 dalyje, ir dėl šio kaltinimo jis turi būti išteisintas kaip nepadaręs veikos, turinčios nusikaltimo ar baudžiamojo nusižengimo požymių (Lietuvos Respublikos BPK 3 str. 1 d. 1 p.) <...>[315].

Tokie informacinės sistemos apsaugos priemonių pažeidimą siauriau aiškinantys požiūriai iš dalies yra probleminiai, nes dėl kaltininko prisijungimo prie informacinės sistemos neteisėtai gautais sistemos naudotojo tapatybės patvirtinimo duomenimis poveikis apsaugos priemonėms vis dėlto yra padaromas – tokiais atvejais dėl apgaulės konstatuotinas nustatytų autentifikavimo procedūrų pažeidimas. Pripažinus, kad bene tiksliausias neteisėto prisijungimo prie informacinės sistemos atitikmuo fizinėje erdvėje yra randamas įsibrovimo į svetimą valdą doktrinoje, pabrėžtina, kad įsibrovimas fizinėje erdvėje nėra siejamas tik su įsilaužimu (padarant žalos). Neteisėti patekimo į vidų veiksmai konstatuojami ir tuo atveju, kai tai padaroma, pavyzdžiui, pasinaudojus apgaule[316]. Dėl to svarstytina, ar iš tiesų „virtualiajam įsibrovimui" į sistemą turėtų būti keliami aukštesni reikalavimai, palyginti su jo fizinėje erdvėje egzistuojančiu atitikmeniu, ypač atsižvelgiant į ekvivalentinio vertinimo principo svarbą kriminalizuojant nusikalstamas veikas elektroninėje erdvėje.

Dėl tokios išvados kyla ir BK 198[1] straipsnyje numatytos nusikalstamos veikos perteklinio kriminalizavimo klausimas, susijęs su neteisėto prisijungimo prie informacinės sistemos pavojingumą pagrindžiančių aplinkybių paieška. Jau minėta, kad Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje atkreipiamas dėmesys į tai, kad yra neginčijamas baudžiamosios atsakomybės poreikis už neteisėtą prieigą, bet tam tikrų prieštaravimų gali kilti tais atvejais, kai paprasčiausiu įsibrovimu nebuvo sukeltas pavojus, arba net tada, kai tokiais neteisėtais veiksmais buvo aptikta saugumo spragų (49 punktas). Nusikalstamos veikos pavojingumo nustatymo svarbą

---

315 Šakių rajono apylinkės teismo 2015 m. birželio 18 d. nuosprendis baudžiamojoje byloje Nr. 1-21-829/2015.

316 Pavyzdžiui, aptariamas neteisėtas patekimas įsilaužiant, pasinaudojant apgaule ar kitais būdais (plačiau žr.: Piesliakas, V. Grobimas įsibraunant į butą, patalpą ar kitokią saugyklą. *Socialistinė teisė*, 1984, Nr. 1; Drakšienė, A. Baudžiamoji atsakomybė už vagystę. *Teisė*, 2000, Nr. 37, taip pat Lietuvos Aukščiausiojo Teismo senato 2005 m. birželio 23 d. nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose". *Teismų praktika*, 2005, Nr. 23).

galima būtų pagrįsti ir Direktyvos 2013/40/ES 3 straipsnio nuostatomis, kuriomis remiantis ne tik įpareigojama kriminalizuoti neteisėtą prieigą prie informacinės sistemos, bet ir tiesiogiai nurodoma, kad sankcijų taikymas yra galimas bent tais atvejais, kurie nelaikomi mažareikšmiais. Pačioje Direktyvoje mažareikšmiškumo klausimas paliekamas spręsti valstybių nacionalinei teisei ir praktikai. Joje tik abstrakčiai užsimenama, kad atvejis „gali būti laikomas mažareikšmiu, pavyzdžiui, kai nusikalstama veika padaryta žala ir (arba) dėl jos kylanti grėsmė viešiesiems arba privatiems interesams, pavyzdžiui, kompiuterių sistemos arba kompiuterinių duomenų vientisumui arba asmens neliečiamumui, teisėms ir kitiems interesams, yra menka arba tokio pobūdžio, kad nėra būtina skirti baudžiamąją sankciją laikantis teisės aktuose nustatytų ribų arba nustatyti baudžiamąją atsakomybę“ (Preambulės 11 punktas). Tokie aiškinimai gali būti tiesiogiai siejami su baudžiamosios atsakomybės kaip kraštutinės priemonės (lot. *ultima ratio)* principu ir iš jo kylančiais racionaliais reikalavimais, taikomais įstatymų leidėjui ir teisės taikytojui pripažįstant tam tikras veikas kaip nusikalstamas. Pavyzdžiui, konstitucinėje jurisprudencijoje pabrėžiama, kad *pagal Konstituciją įstatymų leidėjas baudžiamajame įstatyme nusikalstamomis gali įvardyti tik tas veikas, kurios yra iš tikrųjų pavojingos ir kuriomis iš tikrųjų daroma didelė žala asmens, visuomenės ir valstybės interesams arba dėl šių veikų kyla grėsmė, kad tokia žala bus padaryta* (Lietuvos Respublikos Konstitucinio Teismo 2003 m. birželio 10 d. nutarimas).

Nustačius neteisėtą prisijungimą prie informacinės sistemos, abejonių dėl tokios veikos pavojingumo dažniausiai nekyla, kai sistemos apsaugos priemonėms yra padaroma žalos, bet iš jau pateiktų interpretacijų matyti, kad toks prisijungimo būdas nėra vienintelis. *Kodu* nustatyti apribojimai gali būti įveikiami juos apeinant, pavyzdžiui, naudojantis apgaule ar aptiktomis sistemos saugumo spragomis. Kadangi BK 198[1] straipsnyje numatytos nusikalstamos veikos baigtumo momentas yra siejamas su neteisėto prisijungimo prie informacinės sistemos veiksmu, minėtaisiais atvejais gali kilti abejonių dėl nustatytos veikos pavojingumo, taigi ir baudžiamosios atsakomybės taikymo pagrįstumo. Taikant *ultima ratio* principą, tokiais atvejais siūlytina atsižvelgti ir į kitas baudžiamojoje byloje nustatytas aplinkybes, kuriomis apibūdinama paties prisijungimo specifika, kaltininko veiksmai,

pritaikytos priemonės (įrankiai), paties prisijungimo aplinkybės ir kt. Dėl to didesnį neteisėto prisijungimo prie informacinės sistemos pavojingumą gali rodyti šie aspektai: *pirma*, tokie veiksmai suteikė realių galimybių sistemoje atlikti kitus neteisėtus veiksmus ir ja pasinaudoti siekiant neteisėtų tikslų; *antra*, prisijungiant buvo taikomos papildomos priemonės; *trečia*, pasinaudota informacinės sistemos saugumo spragomis, kurias sukūrė pats asmuo; *ketvirta*, duomenys, reikalingi prisijungti prie informacinės sistemos, buvo įgyti juos nusiperkant arba gauti panaudojus kenkimo programinę įrangą ir kt. Vienas iš šių kriterijų – sąlygų padaryti kitas nusikalstamas veikas sistemoje sudarymas yra suformuluotas ir pradėtas taikyti kasacinės instancijos teismo praktikoje. Minėtojoje Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2016 m. sausio 26 d. nutartyje baudžiamojoje byloje Nr. 2K-4-507/2016 išaiškinta, kad neteisėti prisijungimo prie sistemos veiksmai paprastai negali būti laikomi nereikšmingais, juos vertinant iš baudžiamosios teisės pozicijų, jei tai leido atlikti kitus neteisėtus veiksmus sistemoje. Būtent tolesni neteisėti veiksmai rodo ir didesnį nukentėjusio asmens teisėtų interesų pažeidimo lygį, taigi ir baudžiamosios atsakomybės taikymo būtinumą. Taigi minėtieji ir panašūs kriterijai leistų paneigti baudžiamosios atsakomybės taikymo būtinumą tais atvejais, jeigu byloje yra nustatytas tik pavienis prisijungimo atvejis, kai nebuvo padaryta realios žalos sistemos apsaugos priemonėms, ir remiantis bylos duomenimis akivaizdu, kad asmuo neketino atlikti kokių nors kitų neteisėtų veiksmų sistemoje. Teiginio „pažink savo priešą“[317] kontekste svarbu pabrėžti, kad tokie veiksmai gali būti atlikti tiesiog iš smalsumo ar altruistinių paskatų siekiant nustatyti pažeidžiamas sistemos vietas ir apie jas pranešti sistemos savininkui ar teisėtam valdytojui.

Apibendrinant galima teigti, kad informacinės sistemos apsaugos priemonės gali būti aiškinamos plačiai, arba priešingai – jų techninę koncepciją taikant gana siaurai. Siekiant nuspręsti, kuri pozicija geriausiai atspindėtų įstatymo leidėjo valią, reikėtų atsižvelgti į aplinkybę, kad šios nusikalstamos veikos ištakos yra tiesiogiai siejamos su tarptautiniais ir ES teisės aktais. Nors juose apsaugos priemonių turinys neatskleidžiamas, bet aiškinant įvairius neteisėtos prieigos aspek-

[317] Computer and Information security handbook. Vacca, J. R. (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009, p. 40.

tus jos dažniausiai aptariamos tik technologiniu požiūriu. Kita vertus, toks požiūris nėra imperatyvus – apsaugos priemonių pažeidimas gali būti atviras įvairioms interpretacijoms, tik prieš tai būtina įvertinti neteisėto prisijungimo prie informacinės sistemos perteklinio kriminalizavimo grėsmę.

2.4. Nusikalstamą veiką kvalifikuojančios aplinkybės

Informacinės sistemos (ar jos dalies) strateginė ar didelė reikšmė valstybės valdymui, ūkiui ar finansų sistemai yra požymis, taikomas BK 198[1] straipsnio 2 dalyje formuluojant kvalifikuotą neteisėto prisijungimo prie informacinės sistemos sudėtį. Patys neteisėti prisijungimai prie tokio pobūdžio informacinės sistemos kaip *modus operandi*, be kita ko, gali būti laikomi „informacinio karo“ elementu, kuris yra asimetrinis ta prasme, kad „leidžia silpnesniajam priešininkui nusverti stipresnės šalies <...> strateginį pranašumą, palyginti žema kaina taikant kibernetinę ataką prieš pažeidžiamą kritinę informacinę infrastruktūrą“[318]. Minėtojo požymio įtraukimas į kvalifikuotą neteisėto prisijungimo prie informacinės sistemos sudėtį gali būti paaiškinamas tuo, kad neteisėtai prisijungus prie didesnę reikšmę turinčios sistemos atsirastų sąlygos sukelti didesnių neigiamų padarinių (konfidencialumo, integralumo, prieinamumo ar kitų baudžiamojo įstatymo saugomų vertybių pažeidimo prasme).

Aiškinant BK 198[1] straipsnio 2 dalyje didesnę informacinės sistemos (ar jos dalies) reikšmę nurodančius strateginės reikšmės ir didelės reikšmės minėtosioms sritims (valstybės valdymui, ūkiui ar finansų sistemai) požymius, svarbu pabrėžti, kad ir teisės aktuose, ir literatūroje jie yra taikomi apibūdinant ne tiek informacinę sistemą (ar jos dalį), kiek pačią infrastruktūrą, informacinę infrastruktūrą arba objektą. Be to, šalia st*rateginės reikšmės* ir *didelės reikšmės* neretai vartojami ir kiti terminai, nusakantys didesnę infrastruktūros, informacinės infrastruktūros ar objekto svarbą. Dėl to atskleidžiant, kaip galėtų būti suvokiama informacinė sistema (ar jos dalis), minima BK 198[1] straipsnio 2 dalyje, yra tikslinga: *pirma*, nustatyti kriterijus, kuriais vadovaujantis yra konstatuojama infrastruktūros, informacinės infrastruktūros ar objekto

[318] None-State Actors as Standard Setters. Peters, A.; Koechlin, L., *et al*. (eds). Cambridge: Cambridge University Press, 2009, p. 62.

ypatinga svarba; *antra*, parodyti tokio pobūdžio infrastruktūros, informacinės infrastruktūros ir informacinės sistemos (ar jos dalies) tarpusavio ryšį.

Teisės aktuose ir mokslinėje literatūroje, atsižvelgiant į sukurtą teisinį reguliavimą, vartojami gana įvairūs, bet tarpusavyje glaudžiai susiję terminai, kuriais nurodoma papildomų infrastruktūrai (informacinei infrastruktūrai) ar objektui būdingų bei didesnę jų reikšmę rodančių požymių. Pavyzdžiui, be strateginės reikšmės nacionaliniam saugumui turinčių įmonių, teisės aktuose yra minimi ir *kitų nacionaliniam saugumui užtikrinti svarbių* įmonių[319] ar *valstybinės reikšmės objektų* terminai[320]. Be to, ne tik nacionaliniuose[321], bet ir ES teisės aktuose[322] bei itin dažnai mokslinėje literatūroje[323] yra vartojamas *ypatingos svarbos* infrastruktūros (informacinės infrastruktūros) arba *kritinės infrastruktūros* (informacinės infrastruktūros, angl. *critical infrastructure)* terminas. Nors iš pirmo žvilgsnio tokia terminų gausa tarsi leistų kelti strateginės reikšmės ar didelės reikšmės požymių turinio nustatymo klausimą, bet palyginus minėtųjų terminų apibrėžtis galima įžvelgti daug jų tarpusavio panašumų. Šių terminų sąsaja atsiranda nustatant svarbiausius kriterijus, pagal kuriuos infrastruktūra (informacinė infrastruktūra) ar objektas galėtų būti pripažįstami kaip ypatingos svarbos, o dėl jų veiklos sutrikdymo būtų padarytas

[319] Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas. *Valstybės žinios*, 2002, Nr. 103-4604.

[320] Lietuvos Respublikos civilinės saugos įstatymas. *Valstybės žinios*, 1998, Nr. 115-3230; Lietuvos Respublikos Vyriausybės 2010 m. birželio 7 d. nutarimas Nr. 717 „Dėl Objektų pripažinimo valstybinės reikšmės objektais tvarkos aprašo patvirtinimo“. *Valstybės žinios*, 2010, Nr. 69-3442.

[321] Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. *Valstybės žinios*, 2011, Nr. 83-4033.

[322] Europos Sąjungos Tarybos 2008 m. gruodžio 8 d. Direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo. [2008] OL L 345/76.

[323] None-State Actors as Standard Setters. Peters, A., *et al*. (eds). Cambridge: Cambridge University Press, 2009; Seeds of Disaster, Roots of Response: How Private Actions Can Reduce Public Vulnerability. Auerswald, P. E., *et al* (eds). Cambridge: Cambridge University Press, 2006; Cybercrimes: A Multidisciplinary Analysis. Ghosh, S.; Turrini, E. (eds). Berlin: Springer, 2010, p. 173.

globalus neigiamas poveikis įvairiems svarbiems sektoriams. Net ir pakitus situacijai, patys vertinimo kriterijai leidžia įvertinti tam tikrų objektų svarbą ir motyvuotai juos priskirti prie ypatingos svarbos infrastruktūros objektų. Be to, toks nustatymas yra aktualus sprendžiant, ar pagal minėtuosius kriterijus gali būti apibrėžiama ir strateginės reikšmės arba didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai turinti informacinė sistema (ar jos dalis).

Ar infrastruktūra yra ypatingos svarbos (kritinė), priklauso nuo jos interpretavimo, be to, pats sąvokos formulavimas, pavyzdžiui, ją apribojant tam tikrais konkrečiais objektais, yra komplikuotas, nes sąvoka „kritinis“ visada yra susijusi su perspektyvos klausimu[324]. Ypatingos svarbos suvokimas laikui bėgant gali keistis, tai priklauso nuo visuomenės raidos, informacinės infrastruktūros plėtros ir tam tikrų jos sektorių susiejimo su informacinėmis technologijomis bei kt. Nustatant, kokia infrastruktūra gali būti pripažįstama kritine, kaip minėta, svarbi bendrųjų kriterijų paieška, kurios buvo imtasi ES lygiu priėmus Europos Sąjungos Tarybos 2008 m. gruodžio 8 d. Direktyvą 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (toliau – Direktyva 2008/114/EB)[325]. Jos 2 straipsnio a punkte ypatingos svarbos infrastruktūros objektas apibūdinamas kaip „turtas, sistema ar jų dalis, esantys valstybėse narėse, kurie yra ypač svarbūs esminėms visuomeninėms funkcijoms, žmonių sveikatai, saugai, saugumui, ekonominei ar socialinei gerovei palaikyti, ir kurių veikimo sutrikdymas ar sunaikinimas dėl šių funkcijų nepalaikymo turėtų didelį poveikį valstybei narei“. Bent dviem valstybėms narėms daromas poveikis leistų tokio pobūdžio objektą pripažinti Europos ypatingos infrastruktūros objektu (2 straipsnio b punktas). Be to, šioje direktyvoje pateikiami bendrieji kriterijai, kuriais vadovaujantis atliekamas objektų vertinimas, – tai *nukentėjusiųjų kriterijus* (įvertinama atsižvelgiant į numanomą žuvusiųjų ar sužeistųjų skaičių), *ekonominio poveikio kriterijus* (įvertinama atsižvelgiant į ekonominio nuostolio ir (arba)

[324] Cybercrimes: A Multidisciplinary Analysis. Ghosh, S.; Turrini, E. (eds). Berlin: Springer, 2010, p. 175.

[325] Europos Sąjungos Tarybos 2008 m. gruodžio 8 d. Direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo. [2008] OL L 345/76.

produktų ar paslaugų suprastėjimo lygį; įskaitant ir galimą poveikį aplinkai), ir *poveikio visuomenei kriterijus* (įvertinama atsižvelgiant į poveikį visuomenės pasitikėjimui, fizines kančias ir kasdienio gyvenimo sutrikdymą, įskaitant būtinųjų paslaugų netekimą) (3 straipsnio 2 dalis).

Įgyvendinant šią direktyvą, Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimu Nr. 943 patvirtintas Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašas[326] (toliau – Nutarimas Nr. 943). Jame Europos ypatingos svarbos infrastruktūros objektas apibrėžiamas kaip „Europos Sąjungos valstybėse narėse <...> esantis valstybinės reikšmės objektas[327], kurio sunaikinimas ar jo veiklos sutrikdymas turėtų didelį poveikį bent dviem valstybėms narėms. Poveikio mastas vertinamas remiantis bendraisiais kriterijais, įvertinant kitų rūšių infrastruktūros objektų sukeltą poveikį“ (2 punktas). Beje, šiuo Nutarimu Nr. 943 patvirtintame apraše nurodomi ir analogiški nukentėjusiųjų, ekonominio poveikio ir poveikio visuomenei kriterijai (12 punktas).

Šiek tiek detalesnį kriterijų, į kuriuos atsižvelgiama infrastruktūros objektą pripažįstant kaip ypatingos svarbos, sąrašą galima rasti Lietuvos Respublikos Vyriausybės 2016 m. liepos 20 d. nutarime Nr. 742 „Dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo“ (toliau – ir Nutarimas Nr. 742). Juo patvirtintoje metodikoje infrastruktūros objektų svarba nustatoma įvertinus potencialią žalą, kurią patirtų valstybė, jeigu infrastruktūros objektas būtų sunaikintas, sugadintas ar sutriktų jo veikla (7 punktas). Nors metodikoje pateikiama gana įvairių vertinimo kriterijų, bendriausia prasme jie vis dar gali būti priskiriami vienam iš minėtųjų – nukentėjusiųjų, ekonominio poveikio ir poveikio visuomenei – kriterijų. Vadinasi, pripažįstant ypatingą infrastruktūros objekto svarbą, remiamasi tokiais žalos nustatymo kriterijais: įtaka ypatingos svarbos paslaugos

[326] Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimas Nr. 943 „Dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašo patvirtinimo“. *Valstybės žinios*, 2011, Nr. 105-4950.

[327] Valstybinės reikšmės objekto termino išaiškinimas gali būti randamas Lietuvos Respublikos civilinės saugos įstatyme (*Valstybės žinios*, 1998, Nr. 115-3230).

teikimo sutrikdymui; gyventojų gyvybei ir sveikatai keliamas pavojus; ekonominė žala valstybei; žala aplinkai; įtaka gyventojų pasitikėjimui valstybe; infrastruktūros objekto įtaka kito infrastruktūros objekto, užtikrinančio tos pačios ypatingos svarbos paslaugos teikimą, nepertraukiamam funkcionavimui; infrastruktūros objekto įtaka kito infrastruktūros objekto, užtikrinančio kitų ypatingos svarbos paslaugų teikimą, nepertraukiamam funkcionavimui; įtaka viešojo saugumo užtikrinimui; žala kitoms Europos Sąjungos valstybėms narėms; įtaka valstybės integracijos į europines ir transatlantines institucijas stiprinimui ir tarptautinių saugumo garantijų užsitikrinimui (7 punktas).

Apibendrinant galima teigti, kad nustatant ypatingos svarbos (valstybinės reikšmės) infrastruktūros objektą, svarbiausia atsižvelgti į šio objekto veiklos pobūdį ir (ar) paskirtį, kuria remiantis daroma prielaida, kad dėl neigiamo poveikio jam gali būti sukeliamas pavojus ar padaroma didelė žala įvairiems sektoriams. Vertinant sukeltų padarinių apimtį arba kilusios grėsmės lygį, taikytini minėtieji nukentėjusiųjų skaičiaus, poveikio ekonomikai ir visuomenei kriterijai, kurių detalesnė išraiška pateikiama, pavyzdžiui, Nutarime Nr. 742. Ypatingos svarbos infrastruktūros objektu gali tapti objektas, atitinkantis tam tikrus vertinimo kriterijus, ir visai nesvarbi jo nuosavybės forma (gali priklausyti ir privačiam, ir viešajam sektoriui).

Mokslinėje literatūroje apibrėžiant ypatingos svarbos infrastruktūrą irgi orientuojamasi į šios infrastruktūros svarbą bei neigiamų padarinių, kurių gali kilti dėl jai daromo neteisėto poveikio, apimtį. Pavyzdžiui, B. Lopezas, kalbėdamas apie kritinę infrastruktūrą, atkreipė dėmesį į tai, kad ji „yra tiek gyvybiškai svarbi, kad jos negebėjimas veikti turės neigiamą poveikį saugumui arba ekonominiam saugumui“[328]. E. M. Brunneris ir M. Suter taip pat pabrėžė, kad atskiras komponentas arba visa infrastruktūra dažniausiai apibrėžiama kaip „kritinė“ dėl jos strateginės pozicijos visoje infrastruktūros sistemoje. Kartu šie autoriai nurodė keletą tokio pobūdžio infrastruktūros suvokimo būdų, o tai leido į ypatingą infrastruktūros svarbą pažvelgti *sisteminiu* ir *simboliniu* požiūriu. *Sisteminis požiūris* reikštų, kad infrastruktūra arba jos komponentai yra ypatingos svarbos (kritiniai) dėl

[328] Seeds of Disaster, Roots of Response: How Private Actions Can Reduce Public Vulnerability. Auerswald, P. E., *et al.* (eds). Cambridge: Cambridge University Press, 2006, p. 39.

savo struktūrinės pozicijos visoje sistemoje, ypač jei jie padeda užtikrinti kitų infrastruktūrų tarpusavio ryšį. Kaip teigia patys autoriai, dėl tokio požiūrio kyla tam tikrų problemų nustatant, kokia infrastruktūra ar jos komponentai yra kritiniai – iš esmės viskas yra susiję su komunikacinėmis technologijomis ir net pavienis nelabai reikšmingas atvejis gali sukelti nenumatytą pakopinį efektą, turėsiantį įtakos daugeliui sektorių. Taigi, jei ypatinga svarba aiškinama remiantis infrastruktūrų tarpusavio sąsają, visos jos tampa potencialiai kritinės. Taikant *simbolinę sampratą,* infrastruktūra arba infrastruktūros komponentai patys savaime pripažįstami kritiniais dėl savo paskirties ar funkcijos visuomenėje. Tokiais atvejais probleminiai infrastruktūrų tarpusavio ryšio klausimai yra antraeiliai. Ypatingos svarbos infrastruktūrai nustatyti netaikomas *tarpusavio sąsajos kriterijus*, nes pati infrastruktūros simbolinė reikšmė yra pakankama, kad taptų susidomėjimą keliančiu objektu. Vadovaujantis simboliniu požiūriu, skirtingai nei sisteminiu, kritinę infrastruktūrą apibrėžti yra kur kas paprasčiau – šiuo atveju svarbiausiu akcentu tampa jos atliekama funkcija, svarba ir simbolinė reikšmė. Kita vertus, toks požiūris dažniausiai verčia orientuotis į pavienes infrastruktūras, didesnės reikšmės neteikiant infrastruktūrų tarpusavio sąsajai[329].

Sprendžiant, ar minėtieji nukentėjusiųjų, ekonominio poveikio ir poveikio visuomenei kriterijai gali būti taikomi apibūdinant ir informacinę sistemą (ar jos dalį), būtina nustatyti infrastruktūros, informacinės infrastruktūros ir informacinės sistemos (ar jos dalies) ryšį.

Pati infrastruktūra suvokiama kaip „pagrindinė sistemos struktūra, ypač viešosios paslaugos ir įrenginiai (magistralės, mokyklos, tiltai ir vandens sistemos), reikalingi prekybai palaikyti bei ekonomikos ir gyvenamųjų rajonų plėtrai skatinti“[330]. Vykstant informacinių technologijų raidai, infrastruktūros plėtrai ir tinkamai jos veiklai užtikrinti svarbi tampa informacinė infrastruktūra – vienas iš visą infrastruktūrą sudarančių elementų. Taigi analizuojant ypatingos svarbos infrastruktūros ir ypatingos svarbos informacinės infrastruktūros sąsają atkreip-

[329] Brunner, E. M.; Suter, M. International CIIP Handbook 2008/2009, p. 530–532 [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf*>.

[330] Black‘s Law Dictionary. 9-asis leidimas. Garner, B. A. (ed. in chief). St. Paul (Minn.): West: Thomson Reuters business, 2009, p. 851.

tinas dėmesys į tai, kad abu šie terminai nėra sinonimai, tik sąveikauja tarpusavyje kaip visuma ir jos dalis. Kadangi dauguma strategiškai svarbių sektorių yra priklausomi nuo technologijų, neišvengiamai tenka atskirti *fizinį* ir *virtualųjį* ypatingos svarbos infrastruktūros apsaugos lygmenis. Toks požiūris yra susijęs su mokslinėje literatūroje pateikiamu gana taikliu pastebėjimu, kad „elektroninė erdvė turi sąlytį beveik su viskuo ir su kiekvienu“[331]. Būtent virtualusis apsaugos lygmuo yra aiškiausiai siejamas su informacinės infrastruktūros kaip infrastruktūros dalies apsauga. Kaip teigia D. Assafas, ypatingos svarbos (kritinė) informacinė infrastruktūra apima du terminus: *ypatingos svarbos infrastruktūra* ir *informacinė infrastruktūra*. Analizuodamas jų tarpusavio ryšį, autorius priėjo prie išvados, kad ypatingos svarbos informacinė infrastruktūra yra ta informacinės infrastruktūros dalis, kuri yra esminė užtikrinant ypatingos svarbos infrastruktūros paslaugų nenutrūkstamumą. Kitaip tariant, tai yra „ryšių ir informacijos tinklai, sistemos, programinė įranga ir įrenginiai (įskaitant priežiūros ir kontrolės įrangą), sudarantys ypatingos svarbos infrastruktūros pagrindą“[332]. Panaši nuomonė, kaip turėtų būti suprantama ypatingos svarbos informacinė infrastruktūra, suformuota ir nacionaliniu lygiu priimtuose teisės aktuose, numatant ypatingos svarbos informacinės infrastruktūros apibrėžtį. Pavyzdžiui, Lietuvos Respublikos kibernetinio saugumo įstatyme ypatingos svarbos informacinė infrastruktūra apibrėžiama kaip „elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams“ (2 straipsnio 2 dalis).

Kaip matyti, pati ypatingos svarbos informacinė infrastruktūra apibūdinama ir *technologiniu* aspektu, kaip informacinė sistema (jos dalis), informacinių sistemų grupės bei komunikacinės technologijos, ir *teisiniu*, rodančiu didesnę informacinės infrastruktūros reikšmę visuomenėje – joje įvykęs incidentas gali padaryti arba padaro didelę

[331] Cybercrimes: A Multidisciplinary Analysis. Ghosh, S.; Turrini, E. (eds). Berlin: Springer, 2010, p. 175.

[332] None-State Actors as Standard Setters. Peters, A.; Koechlin, L., *et al.* (eds). Cambridge: Cambridge University Press, 2009, p. 62.

žalą nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės gerovei. Be abejo, tokių padarinių dažniausiai sukelia neteisėtas poveikis informacinei sistemai (jos daliai), kuri yra svarbiausia užtikrinant nenutrūkstamą ypatingos svarbos infrastruktūros veiklą. Apibendrinant galima daryti tokias išvadas:

pirma, strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinčioms informacinėms sistemoms apibūdinti kaip sinonimai gali būti taikomi bendrieji ypatingos svarbos, valstybinės reikšmės informacinės sistemos terminai;

antra, informacinė infrastruktūra yra infrastruktūros dalis, rodanti jos sąsają su informacinėmis ir komunikacijos technologijomis. Atsižvelgiant į informacinės infrastruktūros sandarą, ją gali sudaryti ir viena informacinė sistema, ir keletas jų;

trečia, strateginės reikšmės nacionaliniam saugumui arba didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai informacinės sistemos (jos dalies) požymiams kaltininko veikoje nustatyti ir jiems pagrįsti taikytini minėtieji didesnę svarbą leidžiantys nustatyti nukentėjusiųjų skaičiaus, poveikio ekonomikai ar visuomenei kriterijai. Tokiu atveju informacinės sistemos (jos dalies) reikšmė atitinkamiems sektoriams būtų vertinama atsižvelgiant ne tik į konkretaus sektoriaus, kuriame ji funkcionuoja, svarbą, bet ir taikant minėtuosius neigiamų padarinių apimtį leidžiančius nustatyti kriterijus. Dėl to BK 198^1 straipsnio 2 dalyje numatytas neteisėtą prisijungimą prie informacinės sistemos (jos dalies) kvalifikuojantis ir nusikalstamos veikos dalyką apibūdinantis požymis būtų vertinamas kaskart atsižvelgiant į tai, ar neteisėtu prisijungimu buvo padaryta didelė žala ar kilo tokios žalos grėsmė nacionaliniam saugumui, valstybės valdymui, ūkiui ar finansų sistemai. Šie kriterijai suteikia galimybę informacinės sistemos (jos dalies) ypatingą svarbą vertinti vadovaujantis ir *sisteminiu*, ir *simboliniu* požiūriu;

ketvirta, kadangi ypatingos svarbos informacinę sistemą (jos dalį) nurodantis požymis didesnę šios sistemos svarbą apibūdina pačia bendriausia prasme, tai BK 198^1 straipsnio 2 dalyje nurodomos konkrečios nacionalinio saugumo, valstybės valdymo, ūkio ir finansų sritys. Konstatuojant, kad neteisėtai buvo prisijungta prie informacinės sistemos (jos dalies), turinčios strateginės reikšmės nacionaliniam

saugumui ar didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai, turėtų būti nurodoma viena (ar kelios) iš dispozicijoje nurodytų sričių. Pats neigiamų padarinių apimties kriterijus taikomas atsižvelgiant į konkrečios srities ir joje galinčios kilti didelės žalos ar jos grėsmės specifiką (pavyzdžiui, ekonominio poveikio kriterijus gali būti taikomas konstatuojant, kad informacinė sistema (jos dalis) yra didelės reikšmės finansų sistemai).

3. Subjektyvieji neteisėto prisijungimo prie informacinės sistemos sudėties požymiai

Neteisėto prisijungimo prie informacinės sistemos inkriminavimo apribojimai nustatomi remiantis ne tik jau aptartais objektyviaisiais, bet ir šios nusikalstamos veikos subjektyviaisiais požymiais. Vienas iš svarbiausių požymių, dėl kurio, analizuojant informacinės sistemos (jos dalies) konfidencialumo pažeidimus, gali kilti nemažai įrodinėjimo problemų, yra kaltės požymis. Jo nustatymo kiekvienoje byloje reikalavimas grindžiamas dviem tarpusavyje susijusiais – nusikalstamos veikos sudėties kaip baudžiamosios atsakomybės pagrindo (BK 2 straipsnio 4 dalis) ir nėra nusikaltimo be kaltės (BK 2 straipsnio 3 dalis) – baudžiamosios atsakomybės principais. Baudžiamosios atsakomybės nuostata, kad asmuo pagal baudžiamąjį įstatymą atsako tik tuo atveju, jeigu yra kaltas padaręs nusikalstamą veiką, reiškia ne ką kitą, kaip baudžiamosios atsakomybės kilimą tik tada, jei asmens psichinis santykis su objektyviaisiais požymiais atitinka vieną iš BK nustatytų kaltės formų. Principas, kad nėra nusikaltimo be kaltės, „išreiškia vieną svarbiausių šiuolaikinės baudžiamosios atsakomybės nuostatų – atsakomybę tik už kaltai padarytą veiką“[333]. Šis aspektas yra aktualus ir analizuojant neteisėtą prisijungimą prie informacinės sistemos, nes šios nusikalstamos veikos padarymo mechanizmas visada yra susijęs su informacinių technologijų galimybėmis ir jų atliekamomis funkcijomis. Akivaizdu, kad taikant technologijas įmanomos situacijos, kai gaunami asmens nenumatyti jų veiklos rezultatai. Iš tiesų vienais atvejais gali nekilti klausimų, ar asmens kompiuteriu atlikti veiksmai yra nusikalstami, vis

[333] Švedas, G. Baudžiamosios politikos pagrindai ir tendencijos Lietuvos Respublikoje. Vilnius: Teisinės informacijos centras, 2006, p. 109.

dėlto „technologijos sukuria problemą, ar nusikaltimas yra padarytas kompiuterio vartotojo, ar kompiuterio programos“[334]. Pavyzdžiui, dėl prieigos kontrolę užtikrinančios programinės įrangos spragų asmeniui gali būti suteikta galimybė prisijungti prie informacinės sistemos. Kita vertus, dėl netinkamo programinės įrangos veikimo prieigą gavęs asmuo gali nesuvokti, kad pažeidė nustatytus apribojimus[335]. Būtent kaltės principas tokiais atvejais leidžia eliminuoti objektyvų pakaltinimą, taigi neleidžia kilti baudžiamajai atsakomybei, jei žala vertybėms buvo padaryta nesant kaltės.

Aiškinant kaltės požymį, būtina atkreipti dėmesį į tai, kad neteisėto prisijungimo prie informacinės sistemos nusikalstama veika yra tyčinė. Kadangi šios veikos sudėtis yra formali, tai pagal šiuo metu galiojančio BK 15 straipsnio nuostatas ji gali būti padaroma tik tiesiogine tyčia. Neatsargios kaltės forma BK 198[1] straipsnyje tiesiogiai nenumatoma, atitinkamai baudžiamoji atsakomybė už dėl neatsargumo padarytą tokią veiką yra negalima (BK 16 straipsnio 4 dalis). Tokia kaltės formų apribojimo galimybė numatyta ir Direktyvos 2013/40/ES 3 straipsnyje, kuriame tiesiogiai minima tyčinė prieiga prie visos informacinės sistemos ar jos dalies, ir Konvencijos dėl elektroninių nusikaltimų 2 straipsnyje, nustatančiame pareigą kriminalizuoti sąmoningą prieigą prie visos kompiuterinės sistemos arba jos dalies. Būtent tyčinės kaltės reikalavimas leidžia išvengti šios nusikalstamos veikos kaip „viską sugaunančios“[336] – nuo iš tikrųjų pavojingų veikų iki bet kokio netinkamo elgesio naudojantis kompiuteriu – konstrukcijos. Kaip teigiama mokslinėje literatūroje, kitokie nei tyčiniai veiksmai gali rodyti tiesiog „nerūpestingumą, kvailumą, neatidumą“[337], bet jų padarymas neturėtų būti vertinamas iš baudžiamosios teisės pozicijų. Dėl to teigtina, kad tyčinės kaltės įtraukimas į neteisėto prisijungimo

[334] Cybercrime: Digital Cops in a Networked Environment. Balkin, J., *et al*. (ed.). New York (N.Y.): New York University Press, 2007, p. 93.

[335] Tokie atvejai gali būti prilyginami kazusui ir nuo aptartųjų tyčinių *kompiuterio kodu* nustatytų apribojimų pažeidimų skiriasi tuo, kad tokios programinės įrangos silpnosios vietos nėra žinomos vartotojui ir jomis sąmoningai nesinaudojama gaunant prieigą prie informacinės sistemos.

[336] Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 2011, 22: 167.

[337] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 92.

prie informacinės sistemos sudėtį susiaurina šios nusikalstamos veikos apibrėžtį ir padeda išvengti pernelyg plataus, o vertinant iš baudžiamosios teisės pozicijų ir nepagrįsto, šios veikos taikymo.

Atskleidžiant neteisėto prisijungimo prie informacinės sistemos kaltės turinį reikėtų pabrėžti, kad šios nusikalstamos veikos sudėtis, kaip minėta, yra formali ir ji gali būti padaryta tik tiesiogine tyčia. Vadinasi, konstatuojant tyčinę kaltę turėtų būti nustatoma, kad kaltininkas suvokia, jog neteisėtai jungiasi prie informacinės sistemos, pažeidžia jos apsaugos priemones ir nori taip veikti. Kadangi neteisėto prisijungimo veika BK 198[1] straipsnyje kriminalizuota *per se* nesant sąsajos su kitomis nusikalstamomis veikomis ar kaltininko nusikalstamais ketinimais, tai remiantis tokiu kaltės turiniu nereikalaujama įrodyti, kad kaltininkas, gavęs neteisėtą prieigą prie informacinės sistemos, ketino pačioje sistemoje padaryti kitas nusikalstamas veikas (pavyzdžiui, pažeisti elektroninių duomenų konfidencialumą, sutrikdyti informacinės sistemos darbą ar kt.). Neteisėto prisijungimo prie informacinės sistemos tikslai ir motyvai gali būti įvairūs: chuliganiškos paskatos, siekis daryti kitas nusikalstamas veikas ir pan.[338] Šios veikos padarymo motyvai ir tikslai yra neįtraukti į jos sudėtį, tai kvalifikuojant minėtąją veiką pagal BK 198[1] straipsnį jie įtakos neturi. Kita vertus, į baudžiamojoje byloje nustatytus kaltininko motyvus ir tikslus gali būti atsižvelgiama sprendžiant neteisėto prisijungimo prie informacinės sistemos perteklinio kriminalizavimo problemą – vertinant, ar kaltininko veika yra tokia pavojinga, kad turėtų būti laikoma nusikalstama.

Toks kaltės turinys reiškia, kad kaltininkas, jungdamasis prie informacinės sistemos, turi suvokti ne tik tai, jog pažeidžia apsaugos priemones, bet ir tai, kad tokie jo veiksmai yra neteisėti. Šiuo atveju galima paminėti baudžiamajai teisei svarbią nuostatą, kad asmuo savo elgesio pavojingumą gali įvertinti tik tada, kai suvokia nusikalstamos veikos faktines aplinkybes: „bent vienos reikšmingos (t. y. baudžiamajame įstatyme numatytos) faktinės aplinkybės nesuvokimas šalina galimybę kaltininkui suvokti konkretų savo elgesio pavojingumą, atitinkamai šalina ir jo tyčinę kaltę dėl nusikalstamos veikos <...>.“[339]

---

338 Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 437.

339 Bikelis, S. Tyčinė kaltė baudžiamosios teisės teorijoje ir praktikoje: daktaro disertacija. Vilnius: Mykolo Romerio universitetas, 2007, p. 48.

Taigi tyčinės kaltės reikalavimas leidžia eliminuoti atvejus, kai prie informacinės sistemos buvo prisijungta nesuvokiant tokio veiksmo neteisėtumo (pavyzdžiui, jau minėta, kad prieiga gali būti suteikta dėl netinkamo apsaugos priemonių veikimo) arba kai turint leidimą atliekamas įsiskverbimo testavimas, siekiant nustatyti silpnąsias informacinės sistemos saugumo vietas (etiškas įsibrovimas) ir pan.[340]

Nagrinėjant patį neteisėtumo požymį, buvo atkreiptas dėmesys į tai, kad teisėtų ir jiems priešingų veiksmų atskyrimas elektroninėje erdvėje bendriausia prasme yra susijęs su privačios ir viešosios erdvių ribų joje nustatymu: „ribų sukūrimas reiškia leidimą žmonėms suprasti, kad ribos egzistuoja, ar jos būtų fizinės, loginės ar teisinės.“[341] Kita vertus, analizuojant neteisėto prisijungimo prie informacinės sistemos veiką, kaltės požymis lemia, kad vien tik apribojimų buvimas ir jų reikalavimų nepaisymas nėra pakankamas konstatuoti, kad tokia veika buvo padaryta, – dar būtina nustatyti ir kaltininko minėtųjų ribų bei jų pažeidimo suvokimą. Toks reikalavimas reiškia, kad neišvengiamai turėtų būti įvertintas ir elektroninėje erdvėje nustatytų apribojimų aiškumas. Vadinasi, įvairios priemonės, kurių buvo imtasi apibrėžiant prisijungimo prie informacinės sistemos sąlygas, gali būti laikomos pakankamomis tik tada, jei jos vartotojui padeda efektyviai suvokti atitinkamų ribų egzistavimą. Mokslinėje literatūroje, nors ir kalbant ne apie prisijungimo prie informacinės sistemos, o prieigos prie duomenų apribojimus, pabrėžiama, kad įvairūs apribojimai turėtų būti matomi ir suvokiami būtent iš vartotojo perspektyvos, tai atitiktų jo patyrimą *internete kaip vietoje* (angl. *Internet-as-place)*[342]. Šio

[340] Be minėtųjų atvejų, teisine prasme kol kas sudėtinga išlieka atsakingo pažeidžiamumų atskleidimo politikos (angl. *responsible vulnerability disclosure policy)* sritis. Šios politikos tikslas – į pažeidžiamumų atskleidimo procesą įtraukti vadinamąsias „pilkąsias skrybėles“ (angl. *grey hats)* – nepriklausomus informacinių technologijų specialistus, kurie sutinka geranoriškai bendradarbiauti pažeidžiamumų atskleidimo procese. Mokslinėje literatūroje atkreipiamas dėmesys į tai, kad atsakingo pažeidžiamumų atskleidimo politika kol kas yra „pilkoji zona“, todėl balansuoja ties teisėtumo ir neteisėtumo riba (plačiau žr. Kinis, U. From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure procedure (hereinafter – RVDP): The Latvian approach. *Computer law & Security Review*, 2018, 34(3).

[341] Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2): 490.

[342] *Ibid*., p. 491.

ribų numatomumo kriterijaus taikymas leidžia įžvelgti panašumų su *vidinės perspektyvos* teorijos idėjomis, kurios į elektroninę erdvę leido pažvelgti kaip į virtualiąją realybę, o patį prisijungimą tapatinti su virtualiuoju įėjimu į sistemą. Tokios analogijos suteikia galimybių taikyti ir ekvivalentinio vertinimo principą bei atsižvelgti į asmens savo veiksmų elektroninėje erdvėje suvokimą. Vadinasi, lygiavertis vertinimas išreikštų idėją, kad nesvarbu, kokioje erdvėje asmuo veikia, visais atvejais turėtų būti nustatytas jo *ex ante* suvokimas, kad patekdamas į tam tikrą vietą jis neteisėtai pažeidžia nustatytas konfidencialumo ribas. Kadangi konstatuojant nusikalstamos veikos padarymą fizinėje erdvėje yra svarbus asmens ribų suvokimas (pavyzdžiui, vertinant kaltininko įsibrovimo veiksmus)[343], tai mažesni suvokimo reikalavimai neturėtų būti nustatomi elektroninėje erdvėje.

Apibendrinant galima teigti, kad neteisėto prisijungimo prie informacinės sistemos veika gali būti padaroma tik tiesiogine tyčia. Konstatuojant kaltę turėtų būti nustatoma, kad kaltininkas suvokė, jog darydamas žalą informacinės sistemos konfidencialumui neteisėtai prisijungė prie šios sistemos pažeisdamas jos apsaugos priemones, ir norėjo taip veikti. Tyčinė kaltė padeda išvengti nepagrįsto baudžiamosios atsakomybės taikymo už nekaltai ar dėl neatsargumo padarytas tokio pobūdžio veikas, nes inkriminuojant ją būtina nustatyti visų neteisėto prisijungimo prie informacinės sistemos sudėtyje aprašytų požymių suvokimą. Be to, pagrindžiant tyčinę kaltę, kaltininko suvokimas turėtų būti nustatomas taikant *vidinės perspektyvos* teoriją, atitinkamai ieškant tokio suvokimo pagrindimo analogijų fizinėje erdvėje. Nustačius ribas elektroninėje erdvėje, būtina įvertinti, ar jos yra akivaizdžios būtent iš asmens, nepaisiusio tokių apribojimų, pozicijų, o tai leistų kalbėti apie šių ribų pažeidimo numatomumą.

---

[343] Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 7 d. nutartyje baudžiamojoje byloje Nr. 2K-555/2010 buvo sprendžiama, ar kaltininkui inkriminuotina BK 178 straipsnio 2 dalyje numatyta nusikalstama veika. Šioje byloje nuteistasis teigė, kad įvykio metu jis nesuprato, jog įėjo į tarnybines patalpas. Dėl to teismas atskirai pareiškė nuomonę dėl nustatytų ribų aiškumo (kaip nurodė teismas, durys, skirtos kavinės klientams, buvo visiškai kitoje vietoje, o įėjus į patalpas, į kurias įsibrovė nuteistasis, virš laiptų, po kuriais buvo sukrautos alaus statinės, aiškiai matyti pašaliniams įeiti draudžiantis užrašas) ir padarė išvadą, kad nuteistasis tokius apribojimus suvokė.

Naujosios technologijos lemia poreikį naujai interpretuoti senąsias vertybes, bet jos gali rodyti ir naujų elgesio kodeksų poreikį, jei taikant technologijas atsiranda naujų veiksmų <...>.

J. Lourdu Vesna, D. Niveditha

III SKYRIUS

NETEISĖTAS ELEKTRONINIŲ DUOMENŲ PERĖMIMAS IR PANAUDOJIMAS (BK 198 STRAIPSNIS)

III SKYRIAUS TURINYS

1. Bendrieji neteisėto elektroninių duomenų perėmimo ir panaudojimo kriminalizavimo ypatumai

Baudžiamoji atsakomybė už neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamą veiką Lietuvoje pirmą kartą nustatyta 2003 m. įsigaliojus naujajam BK. Tiesa, iki 2007 m. BK 198 straipsnio pakeitimų tokia veika buvo vadinama kompiuterinės informacijos pasisavinimu ir skleidimu bei savo apimtimi buvo siauresnė nei šiuo metu BK nustatyta elektroninių duomenų perėmimo ir panaudojimo veika. Būtent po 2007 m., kai buvo pakeistas visas BK XXX skyrius, šio kodekso 198 straipsnyje pasikeitė šios nusikalstamos veikos baudžiamumas, bendrai vartojama su technologijomis susijusi terminija, į dispoziciją buvo įtraukta daugiau alternatyvių veikų, numatytos naujos nusikalstamą veiką kvalifikuojančios aplinkybės. Taigi šiais pakeitimais buvo patikslintas nusikalstamos veikos dalykas – juo laikoma ne įstatymo saugoma kompiuterinė informacija, o nevieši elektroniniai duomenys. Dispozicijoje, be informacijos pasisavinimo ir kitų jos skleidimo būdų, nurodomos elektroninių duomenų neteisėto stebėjimo, fiksavimo, perėmimo, įgijimo ir laikymo veikos. Neteisėto elektroninių duomenų perėmimo ir panaudojimo veikos sudėtyje numatyta šią veiką kvalifikuojanti aplinkybė, susijusi su didesne neviešų elektroninių duomenų svarba – jų strategine reikšme nacionaliniam saugumui, didele reikšme valstybės valdymui, ūkiui ar finansų sistemai.

Šiems pakeitimams įtakos turėjo ir Konvencijos dėl elektroninių nusikaltimų, ir Pamatinio sprendimo 2005/222/TVR nuostatos. Kita vertus, aptariant šiuos teisės aktus reikėtų atkreipti dėmesį, kad Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje kompiuterinių duomenų konfidencialumą pažeidžianti veika aprašyta gerokai siauriau nei įtvirtintoji BK 198 straipsnyje. Pamatiniame sprendime 2005/222/TVR tokia nusikalstama veika išvis tiesiogiai nenumatoma – jame elektroninių duomenų konfidencialumo apsauga gali būti susijusi tik su informacinės sistemos konfidencialumu. Neišsamus minėtajame sprendime pateikiamas nusikalstamų veikų sąrašas buvo koreguotas Direktyvoje 2013/40/ES. Jos 6 straipsnyje numatyta neteisėto duomenų perėmimo veika yra bene analogiška neteisėtos perimties veikai, apibrėžtai Konvencijos dėl elektroninių nusikaltimų 3 straips-

nyje. 2015 metais įgyvendinant minėtosios direktyvos nuostatas nebuvo keičiamas BK 198 straipsnis, o tai leidžia tvirtinti, jog, įstatymo leidėjo nuomone, esamos BK 198 straipsnio nuostatos tinkamai atspindi direktyvos nuostatas, todėl papildomi derinimo veiksmai nebūtini.

Konfidencialumo elektroninėje erdvėje apsaugai taikant baudžiamosios teisės priemones, užsienio valstybėse vyrauja skirtingas požiūris, kaip tai galima būtų padaryti ir kokia apimtimi elektroniniai duomenys turėtų būti saugomi. Tokio pobūdžio nusikalstamų veikų elektroninėje erdvėje kriminalizavimo praktikos įvairovę lėmė duomenų, kurie yra *laikomi informacinėje sistemoje*, ir duomenų, kurie yra *joje perduodami*, atskyrimas. Dėl to elektroninių duomenų konfidencialumo pažeidimus bendriausia prasme galima analizuoti dviem požiūriais: *pirma*, kaip neteisėtą prieigą prie duomenų, laikomų (saugomų) informacinėje sistemoje ir, *antra*, kaip neteisėtą duomenų, perduodamų informacinėje sistemoje, perėmimą. Teigtina, kad tokio atskyrimo pagrindu tapo Konvencijos dėl elektroninių nusikaltimų nuostatos, t. y. tos, kuriomis įpareigojama šią konvenciją ratifikavusias valstybes numatyti baudžiamąją atsakomybę už neteisėtą prieigą (2 straipsnis) ir neteisėtą perimtį (3 straipsnis). Valstybėms nustačius atitinkamas diskrecijos ribas, buvo sudarytos sąlygos skirtingai pažvelgti į galimus informacinės sistemos ir elektroninių duomenų konfidencialumo pažeidimų kriminalizavimo būdus, atitinkamai ir skirtingoms tokių veikų inkriminavimo problemoms kilti.

Analizuojant *informacinėje sistemoje laikomų duomenų* konfidencialumo pažeidimus, svarbu pabrėžti, kad kai kuriose užsienio valstybėse tokio pobūdžio veika dažniausiai yra siejama su neteisėta prieiga prie informacinės sistemos. Tokiais atvejais, kaip minėta, svarbiausiu neteisėtos prieigos veikos aspektu laikomas elektroninių duomenų, o ne informacinės sistemos konfidencialumas. Šis neteisėtos prieigos kriminalizavimo būdas pasirinktas, pavyzdžiui, Vokietijos baudžiamojo įstatymo 202a straipsnyje, kuriame kriminalizuotas duomenų šnipinėjimas (tokiai veikai būdingas duomenų, apsaugotų nuo neteisėtos prieigos, įgijimas, įveikiant apsaugą). Toks požiūris į neteisėtos prieigos veiką suformuotas ir Jungtinės Karalystės netinkamo naudojimosi kompiuteriais akto 1 straipsnyje, kuriame ji aprašyta kaip neteisėtas kompiuterio privertimas atlikti bet kokią funkciją siekiant gauti prieigą prie programos ar jame laikomų duomenų, arba suteikiant galimybę

tokią prieigą gauti. Kaip nurodoma literatūroje[344], tokiomis veikomis yra kėsinamasi į duomenų, *laikomų (saugomų) informacinėje sistemoje,* konfidencialumą. Anot J. Clougho, nusikalstamos veikos, „susijusios su neteisėta prieiga prie kompiuterio, plėtojosi iki bendresnių, susijusių su duomenų, laikomų kompiuteryje, apsauga“[345]. I. Waldenas irgi atkreipė dėmesį, kad minėtaisiais atvejais turimi mintyje *nejudami duomenys* (angl. *data at rest)*, t. y. „duomenys, esantys sistemoje, prie kurios kaltininkas yra gavęs prieigą arba padaręs joje pakeitimų“[346].

Antrąjį elektroninių duomenų konfidencialumo pažeidimo aspektą, t. y. neteisėtą duomenų, *perduodamų informacinėje sistemoje,* perėmimą, reikėtų sieti su kitu duomenų konfidencialumo pažeidimo lygiu. Bendriausia prasme šiuos duomenis galima apibūdinti kaip perduodamus tinklais (angl. *data in transmission)*[347], per telekomunikacijos sistemą[348] ir kt. Analizuojant nuolat kintančias elektroninių ryšių ypatybes, literatūroje pabrėžiama, kad neatsižvelgiant į tai, ar „elektroninis paštas yra perduodamas telekomunikacijų tinklais, o pranešimai – vietos tinklais (LAN) ar vaizdai yra siunčiami bevieliu ryšiu, visada yra potenciali galimybė, kad duomenys gali būti perimti“[349].

---

344 Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 183; Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 135; Blunn, A. S. Report of the Review of the Regulation of Access to Communications [interaktyvus. Žiūrėta 2018-07-24], Australija, 2005, p. 28. Prieiga per internetą: *<http://www.ag.gov.au/Publications/Documents/Blunn%20report%20of%20the%20review%20of%20the%20regulation%20of%20access%20to%20communications%20-%20August%202005/xBlunn%20Report%2013%20Sept.pdf>*; Computer law. Reed, C. (ed). Oxford: Oxford University Press, 2011, p. 715, 716.

345 Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 135.

346 Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 183.

347 *Ibidem*.

348 Blunn, A. S. Report of the Review of the Regulation of Access to Communications [interaktyvus. Žiūrėta 2018-07-24], Australija, 2005, p. 28, Prieiga per internetą: *<http://www.ag.gov.au/Publications/Documents/Blunn%20report%20of%20the%20review%20of%20the%20regulation%20of%20access%20to%20communications%20-%20August%202005/xBlunn%20Report%2013%20Sept.pdf>*.

349 Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 135.

Vykstant ryšių technologijų raidai, iš tiesų atsiranda ir naujų minėtųjų veikų padarymo būdų („nusikalstama veika seka galimybę“)[350], todėl jau aptartas duomenų skirstymas į *laikomus informacinėje sistemoje* ir *perduodamus duomenis* leidžia pabrėžti visapusį duomenų saugumo poreikį. O analizuojamuoju aspektu – ir apie būtiną subalansuotą duomenų, esančių elektroninėje erdvėje, konfidencialumo apsaugą.

Remiantis užsienio valstybių praktika kriminalizuojant perduodamų duomenų perėmimą matyti, kad daugelyje valstybių (Vokietijoje, Jungtinėje Karalystėje, Kipre, Jungtinėse Amerikos Valstijose ir kt.) tokie duomenų konfidencialumo pažeidimai yra kriminalizuoti kaip atskira veika. Pavyzdžiui, jau minėta, kad Vokietijos baudžiamojo įstatymo 202a straipsnyje numatyta atsakomybė už neteisėtą prieigą prie apsaugotų duomenų, jeigu buvo įveikta apsauga, o šio įstatymo 202b straipsnyje kalbama apie duomenų perėmimą techninėmis priemonėmis. Toks neteisėtos prieigos prie informacinėje sistemoje laikomų ir perduodamų duomenų atskyrimas pasirinktas ir Jungtinėje Karalystėje. Atsakomybė už neteisėtą perėmimą yra nustatyta 2000 m. Tyrimo įgaliojimų reguliavimo akto[351] 1 dalyje. Minėtajame akte neteisėtu perėmimu bendriausia prasme yra laikomas bet kokio pranešimo perėmimas jo perdavimo metu, jei tokie veiksmai buvo atlikti sąmoningai ir neturint teisėtų įgaliojimų atlikti perėmimą, be to, toks perėmimas turėtų būti atliktas bet kurioje Jungtinės Karalystės vietoje.

Taigi, kaip matyti, reikalavimo nustatyti baudžiamąją atsakomybę už neteisėtą duomenų perėmimą ištakos tiesiogiai siejamos su Konvencijos dėl elektroninių nusikaltimų 3 straipsniu. Direktyvos 2013/40/ES 6 straipsnyje tokia veika buvo numatyta kur kas vėliau. Konvencijos aiškinamojoje ataskaitoje nurodoma, kad jos 3 straipsnyje esančių nuostatų tikslas – „apsaugoti privatumo teisę perduodant duomenis“, neatsižvelgiant į elektroninių duomenų perdavimo formą – telefonu, faksu, elektroniniu paštu ar rinkmenų perdavimą (51 punktas). Direktyvos preambulės 9 punkte išaiškinta, kad „duomenų perėmimas apima pranešimų turinio klausymąsi, stebėjimą ar

[350] Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum*, 2011, 22: 150.

[351] Regulation of Investigatory Powers Act [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: <*http://www.legislation.gov.uk/ukpga/2000/23/section/1*>.

sekimą, duomenų turinio teikimą arba tiesiogiai, naudojantis prieiga prie informacinių sistemų ir naudojant šias sistemas, arba netiesiogiai, naudojant elektroninę slapto klausymosi įrangą taikant technines priemones, bet nebūtinai apsiribojama vien šiais būdais“. Taigi Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje įpareigojama nustatyti baudžiamąją atsakomybę už sąmoningą ir neteisėtą neviešo kompiuterinių duomenų perdavimo į kompiuterinę sistemą, iš jos ar jos viduje perimtį techninėmis priemonėmis. Šiame straipsnyje užsimenama ir apie elektromagnetinės emisijos iš kompiuterinės sistemos, perduodančios tokius kompiuterinius duomenis, perimtį. Panašiai neteisėto duomenų perėmimo veika yra aprašyta ir Direktyvos 2013/40/ES 6 straipsnyje, kuriuo remiantis baudžiamoji atsakomybė bendriausia prasme turėtų būti nustatoma už tyčinį neteisėtą neviešai perduodamų kompiuterinių duomenų perėmimą techninėmis priemonėmis, bent tais atvejais, kurie nelaikomi mažareikšmiais. Šiame straipsnyje, kaip ir Konvencijoje, minimas ir elektromagnetinės spinduliuotės perėmimas.

Analizuojant Konvencijos dėl elektroninių nusikaltimų 3 straipsnio nuostatas ir jos aiškinamojoje ataskaitoje pateiktus jų interpretavimo būdus, reikėtų pabrėžti keletą svarbių aspektų, dėl kurių valstybėms atsirado galimybė apriboti šios nusikalstamos veikos „plotį“. Siekiant išvengti neteisėto perėmimo veikos perteklinio kriminalizavimo, reikėtų atkreipti dėmesį į šiuos aspektus: *pirma*, konvencinės nuostatos leidžia susiaurinti neteisėto perėmimo veikos apibrėžtį į jos sudėtį įtraukiant šios nusikalstamos veikos padarymo turint nesąžiningą ketinimą požymį, taip pat jei buvo nustatyta, kad kompiuterinė sistema yra sujungta su kita kompiuterine sistema (3 straipsnis); *antra*, numatyta galimybė reikalauti, kad tokia veika būtų padaryta taikant technines priemones – pasiekiant duomenis tiesiogiai (gavus prieigą ir naudojantis kompiuterine sistema) arba netiesiogiai (taikant įvairias priemones, skirtas duomenims perimti)[352]; *trečia*, kadangi kompiuterinė sistema gali būti susijusi ir su radijo ryšiu, Konvencijos aiškinamojoje ataskaitoje teigiama, kad valstybės nėra įpareigotos kriminalizuoti bet kokios radijo transliacijos perėmimą, kuri, net ir būdama

[352] Kaip nurodoma Konvencijos aiškinamojoje ataskaitoje, techninių priemonių reikalavimas gali būti laikomas tuo apribojimu, kuris leidžia išvengti neteisėto perėmimo nusikalstamos veikos perteklinio kriminalizavimo (53 punktas)

nevieša, yra gana lengvai prieinama ir gali būti perimta, pavyzdžiui, mėgėjo (56 punktas)[353]; *ketvirta*, Konvencijos 3 straipsnyje minimas neviešas duomenų perdavimo perėmimas. Pačia sąvoka *neviešas* apibūdinamas perdavimo (komunikavimo) procesas, o ne perduotų duomenų pobūdis. Perduodami duomenys gali būti ir viešai prieinama informacija, bet perdavimas išlieka neviešu, jeigu jo dalyviai nori komunikuoti konfidencialiai (54 punktas). Beje, Direktyvos 2013/40/ES 6 straipsnyje dar numatoma, kad baudžiamoji atsakomybė turėtų kilti bent už tas veikas, kurios nėra mažareikšmės. Dėl to į nusikalstamos veikos sudėtį gali būti įtraukiami šie požymiai: techninių priemonių taikymas perimant duomenis, duomenų perdavimo neviešumas.

Analizuojant Lietuvos BK 198 straipsnyje numatytus neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėties požymius matyti, kad ir *duomenų, perduodamų informacinėje sistemoje*, ir *joje esančių duomenų* konfidencialumo pažeidimai yra kriminalizuoti tame pačiame BK straipsnyje[354]. Be to, konstruojant šios nusikalstamos veikos sudėtį, nebuvo atsižvelgta į jos susiaurinimo galimybes bandant išspręsti neteisėto elektroninių duomenų perėmimo ir jų panaudojimo perteklinio kriminalizavimo problemas – nusikalstama veika nėra susijusi, pavyzdžiui, su techninių priemonių taikymu. Viena vertus, galima pateisinti tokią įstatymo leidėjo poziciją – gana plačiai kriminalizuojant neteisėtą elektroninių duomenų perėmimą ir panaudojimą buvo siekiama nepalikti galimų spragų, kurios leistų išvengti baudžiamosios atsakomybės už elektroninėje erdvėje padarytas veikas. Kita vertus, BK 198 straipsnyje numačius itin daug alternatyvių veikų, jų akivaizdžiai nesusiejus su nusikalstamos veikos dalyku ir pačios nusikalstamos veikos taikymo neapribojus papildomais požymiais, kyla nemažai šios elektroninių duomenų

[353] Mokslinėje literatūroje aiškinama, kad tokie apribojimai yra tiesiogiai susiję su *Bluetooth* technologijomis ir kitais įrenginiais, kuriais radijo bangomis perduodami duomenys sąlygiškai trumpais atstumais (Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 138).

[354] Toks neteisėto elektroninių duomenų konfidencialumo pažeidimo veikos kriminalizavimo būdas pasirinktas ir kai kuriose kitose užsienio valstybėse. Pavyzdžiui, Prancūzijos baudžiamajame įstatyme atskirai kriminalizuota neteisėtos prieigos veika (323-1 straipsnis) ir neteisėtos perimties veika (226-15 straipsnis). Estijos baudžiamajame įstatyme atskirtas neteisėtas kompiuterinės sistemos panaudojimas (217 straipsnis) ir neteisėtas sekimas (137 straipsnis).

konfidencialumą pažeidžiančios nusikalstamos veikos inkriminavimo keblumų. Kadangi daugelį iš jų tikslinga aptarti interpretuojant atskirus šios veikos sudėties požymius, prieš pereinant prie detalesnės analizės būtų galima aptarti bendresnius BK 198 straipsnio taikymo sunkumus. Vienas iš svarbesnių yra siejamas su nusikalstamų veikų daugeto ir baudžiamojo įstatymo normų konkurencijos atskyrimu, atitinkamai ir teisingu kaltininko padarytų nusikalstamų veikų elektroninėje erdvėje kvalifikavimu.

Jau minėta, kad daugelį tradicinėmis laikomų nusikalstamų veikų perkėlus į elektroninę erdvę, pakito ir jų sudėties požymių aiškinimas. Būtent dėl plataus jų turinio interpretavimo atsirado galimybė užtikrinti ne tik ekvivalentų veiksmų fizinėje ir elektroninėje erdvėje vertinimą, bet ir „atrasti" informacinių technologijų taikymo požymį. Kita vertus, tai sukėlė ir diskusijų, t. y. kokiais atvejais kvalifikuojant tradicines nusikalstamas veikas, padarytas elektroninėje erdvėje, yra būtinos nuorodos ir į BK XXX skyriuje (tiksliau – BK 198 straipsnyje) numatytas nusikalstamas veikas. Tokia problema kilo dėl pernelyg plačios neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos apibrėžties, kai baudžiamoji atsakomybė yra nustatoma už įvairias alternatyvias veikas: neteisėtą neviešų elektroninių duomenų stebėjimą, fiksavimą, perėmimą, įgijimą, laikymą, pasisavinimą, paskleidimą ar kitokį panaudojimą. Dėl to neretai pasitaiko atvejų, kai iš baudžiamosios teisės pozicijų vertinant elektroninėje erdvėje padarytas veikas būtina nuspręsti, pagal kokius ir kiek straipsnių tokia veika turėtų būti kvalifikuojama. Toks sprendimas priklauso nuo to, ar konkrečiu atveju kalbama apie nusikalstamų veikų daugetą, ar vis dėlto apie baudžiamosios teisės normų konkurenciją.

Esant baudžiamosios teisės normų konkurencijai, „kelios baudžiamojo įstatymo normos gali būti pritaikytos konkrečiam juridiniam faktui (nusikaltimui). Tačiau galutinai iš visų normų, kurios gali būti pritaikytos nusikaltimo kvalifikavimui, iš tikrųjų parenkama tik viena"[355]. Kadangi tokiais atvejais vieną nusikalstamą veiką visiškai atitinka keletas tarpusavyje konkuruojančių normų, remiantis konkurencijos įveikimo taisyklėmis sprendžiama, kurią iš jų taikyti. Analizuojamuoju požiūriu itin aktuali bendrosios ir specialiosios nor-

[355] Pavilonis, V. Baudžiamosios teisės normų konkurencija. *Teisės problemos*, 1996, 2(12): 38.

mos konkurencijos įveikimo taisyklė, kai iš abiejų tarpusavyje konkuruojančių normų veikai kvalifikuoti pasirenkama specialioji norma. Vadinasi, atitinkamai konkuruojant BK 198 straipsnyje esančiai bendrajai normai ir kitoms normoms, kuriomis numatomi konkretesni elektroninėje erdvėje padarytos nusikalstamos veikos požymiai, taikytina būtent specialioji norma. Joje įtvirtinti nusikalstamos veikos sudėties požymiai visiškai atitiks padarytą nusikalstamą veiką, tokie atvejai nėra pripažįstami nusikalstamų veikų daugetu ir veika nekvalifikuojama papildomai pagal BK 198 straipsnį. Dėl to nereikėtų pritarti literatūroje reiškiamai nuomonei, kad konstatavus, jog tradicinės nusikalstamos veikos dalykas yra elektroniniai duomenys, padaryta veika (ar veikos) turėtų būti papildomai kvalifikuojama ir pagal BK 198 straipsnį[356], taip pat, kad BK 198 straipsnis inkriminuotinas visais atvejais, kai įvykdyta tapatybės vagystė (pavyzdžiui, BK 182, 186, 207, 214, 215 straipsniai)[357]. Manytina, kad tokios papildomos nuorodos į BK 198 straipsnį, neišsiaiškinus, ar BK straipsnis, kuriame numatoma tradicinė nusikalstama veika, iš tiesų nepritaikomas elektroninei erdvei, yra perteklinės ir gali neatitikti baudžiamosios teisės teorijoje bei teismų praktikoje nusistovėjusios bendrosios ir specialiosios normų konkurencijos įveikimo taisyklės bei ekvivalentinio vertinimo principo reikalavimų. Pastarojo principo pažeidimui būdinga tai, kad daugeliu atvejų griežtesnė baudžiamoji atsakomybė būtų taikoma tik dėl to, kad nusikalstamos veikos dalykas yra elektroninės formos (BK 198 straipsnyje numatyta nusikalstama veika priskiriama apysunkių nusikaltimų kategorijai). Beje, minėtaisiais atvejais nusikalstamų veikų daugeto neįžvelgiama ir kasacinės instancijos teismo praktikoje. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2015 m. sausio 6 d. kasacinėje nutartyje baudžiamojoje byloje Nr. 2K-138/2015, sprendžiant BK 168 ir 198 straipsniuose numatytų nusikalstamų veikų atribojimo klausimą, atkreipiamas dėmesys į bendrosios ir specialiosios normų atribojimo bei tradicinių nusikalstamų veikų, padarytų elektroninėje erdvėje, identifikavimo

---

356 Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 431.

357 Štitilis, D., *et al*. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai. Vilnius: Mykolo Romerio universitetas, 2011, p. 257

svarbą: *BK 168 straipsnyje kriminalizuotas asmens privataus gyvenimo pažeidimas ne tik fizinėje, bet ir elektroninėje erdvėje. Šiame straipsnyje nurodyti neteisėto informacijos apie asmens privatų gyvenimą atskleidimo ar panaudojimo veiksmai, palyginus su BK 198 straipsnyje numatytaisiais, yra konkretesni, tiesiogiai susiję būtent su asmens privataus gyvenimo neliečiamumo pažeidimais. BK 168 straipsnio 1 dalyje numatyta norma turi ir visus bendrojoje normoje (BK 198 straipsnio 1 dalis) nurodytus požymius, tačiau reguliuoja įstatymo leidėjo specialiai išskirtus privataus gyvenimo neliečiamumo pažeidimo atvejus. Todėl BK 168 straipsnio 1 dalyje nurodyta norma laikytina specialiąja, o BK 198 straipsnio 1 dalyje esanti – bendrąja. Antra, svarbu yra tai, kad viešas informacijos apie kito žmogaus privatų gyvenimą paskelbimas galimas ne tik fizinėje, bet ir elektroninėje erdvėje, todėl šioje erdvėje (pvz., elektroniniu paštu) paskelbta informacija turi ir visus elektroninių duomenų požymius. Taigi BK 198 straipsnio taikymas vien dėl to, kad nusikalstamos veikos dalykas, t. y. informacija apie kito žmogaus privatų gyvenimą, yra elektroninių duomenų formos, nepagrįstas.*

Apibendrinant galima teigti, kad BK 198 straipsnyje yra kriminalizuotas neteisėtas disponavimas *informacinėje sistemoje perduodamais* ir *joje laikomais* neviešais elektroniniais duomenimis. Dėl gana plačios šios nusikalstamos veikos apibrėžties kyla nemažai jos inkriminavimo problemų, susijusių su šios nusikalstamos veikos perteklinio kriminalizavimo grėsme, ir su sunkumais sprendžiant, ar konkrečiu atveju susiduriama su nusikalstamų veikų daugetu, ar su baudžiamosios teisės normų konkurencija. Tokia baudžiamojo teisinio reguliavimo padėtis verčia svarstyti ir jo koregavimo būtinumą.

2. Objektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai

2.1. Nusikalstamos veikos dalykas – nevieši elektroniniai duomenys

Duomenų konfidencialumą elektroninėje erdvėje pažeidžiančios nusikalstamos veikos dalyko išaiškinimo problemos įvairiose valstybėse yra sprendžiamos skirtingai. Daugelio iš jų teisėje (pavyzdžiui, Prancūzijos, Vokietijos ar Estijos) šis nusikalstamos veikos sudėties požymis baudžiamojo įstatymo lygiu yra neapibrėžtas. Kitose valstybėse (pavyzdžiui, Kipre, Bulgarijoje, Rusijoje) priešingai – bandoma pateikti nors ir bendrojo pobūdžio, bet svarbiausias elektroninių duomenų (informacijos) ypatybes atskleidžiančius apibrėžimus. Tokiais atvejais sulyginimo sunkumų kyla dėl dalykui įvardyti pasirinktų skirtingų terminų, pavyzdžiui, *kompiuterizuoti, kompiuteriniai duomenys, kompiuterinė informacija* ir kt.

Neteisėtas elektroninių duomenų perėmimo ir panaudojimo dalykas Lietuvos BK 198 straipsnio 1 dalies dispozicijoje yra įvardytas kaip nevieši elektroniniai duomenys. BK 198 straipsnio 2 dalyje pateikiamoje kvalifikuotoje neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtyje yra minimi strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turintys nevieši elektroniniai duomenys. Neatsižvelgiant į tai, apie kurį – platesnę ar siauresnę reikšmę – turintį dalyko požymį yra kalbama, jų struktūroje galima nustatyti du aspektus: *pirma*, technologinį (elektroniniai duomenys) ir, *antra*, teisinį (elektroninių duomenų neviešumas arba didesnė jų reikšmė). Dar reikėtų pabrėžti, kad nors Lietuvos BK nepateikiamas autentiškas BK XXX skyriuje vartojamų sąvokų išaiškinimas, kriterijus, leidžiančius priskirti duomenis elektroninių duomenų rūšiai, galima nustatyti remiantis Konvencijos dėl elektroninių nusikaltimų, Direktyvos 2013/40/ES nuostatais ir nacionalinės teisės aktais bei teismų praktika.

2.1.1. Elektroninių duomenų samprata

Analizuojant tiesiogiai su technologijomis susijusį neteisėto elektroninių duomenų perėmimo ir panaudojimo dalyko aspektą – pačius elektroninius duomenis, tenka spręsti ir technologijų bei terminologijos klausimą. Kaip matyti, jis tapo neišvengiamas nusikalstamų veikų sudėtyse tiesiogiai įtvirtinus technologijas apibrėžiančius terminus. Dėl to reikėtų aptarti tas baudžiamosios teisės srityje kylančias elektroninių duomenų interpretavimo problemas, kurios bendriausia prasme yra susijusios: *pirma*, su duomenų ir informacijos tarpusavio ryšio nustatymu; *antra*, elektroninių duomenų sąvoka.

Pirmoji problema yra aktuali dėl to, kad pasirinktas *duomenų* arba *informacijos* terminas lemia platesnį arba siauresnį požiūrį į alternatyviomis veikomis (stebėjimu, fiksavimu, įgijimu ir kt.) padaromus konfidencialumo pažeidimus. Be to, pagrindą analizuoti duomenų ir informacijos santykį suteikia 2007 metais priimti BK XXX skyriaus pakeitimai. 2000 m. įsigaliojusio BK XXX skyriuje apibrėžiant su elektroninių duomenų konfidencialumo pažeidimais susijusias normas, vietoj *duomenų* vartotas *informacijos* terminas (pavyzdžiui, BK 198 straipsnyje, kuriame buvo kriminalizuotas kompiuterinės informacijos pasisavinimas ir skleidimas). Toks pasirinktas sudėties požymių aprašymas mokslinėje literatūroje buvo nemažai kritikuojamas pabrėžiant, kad įstatymų leidėjas BK XXX skyriuje neįžvelgė duomenų ir informacijos skirtumo[358]. Vadinasi, siekiant ištaisyti šį trūkumą, 2007 metų pakeitimais BK XXX skyriuje buvo atsisakyta *kompiuterinės informacijos* termino ir pradėtas vartoti kitas, *elektroninių duomenų,* terminas. Tokios pasikeitusios įstatymo leidėjo pozicijos ištakų reikėtų ieškoti būtent nustatant duomenų ir informacijos skirtumus.

Vertinant duomenų ir informacijos sąsają, literatūroje pateikiama bendroji nuomonė, kad šios sąvokos nėra tapačios, todėl siekiant tikslumo jos abi turėtų būti vartojamos pagal savo tikrąją prasmę. Analizuojant duomenis svarbu pabrėžti, kad jiems suteikiama primityvi vienetinė reikšmė, kuri mokslininkų, nagrinėjusių įvairius duomenų ir informacijos tarpusavio ryšio aspektus, apibrėžiama vartojant *neap-*

[358] Civilka, M., *et al*. Informacinių technologijų teisė. Vilnius: NVO teisės institutas, 2004, p. 529.

dorotų faktų[359], *fundamentalių faktų be konteksto*[360], *pirminių apibūdinimų, neturinčių konkrečios reikšmės*[361], *simbolių grupių, kurių pranešimo reikšmės lygmuo yra žemiausias*[362] posakius. Jie reiškia būtent tai, kad duomenys yra nesiejami su jų galima reikšme adresatui. Vadinasi, duomenys yra tik potenciali informacija, t. y. „duomenys virsta informacija, kai tam tikram subjektui jie tampa suprantami“[363]. Dėl to duomenų suvokimo, jų prasmės, naudos davimo žmogui pabrėžimas, analizuojant informacijos sąvoką, matyti daugelio autorių darbuose[364]. Anot R. T. Potterio, „informacija duomenis reiškia tada, kai jie yra pateikiami taip, kad turi reikšmės ir vertės gavėjui“[365]. Panašų apibrėžimą pateikė C. K. Laudonas ir J. P. Laudon – jie teigia, kad informacija reiškia duomenis, kai šie „pateikiami tokia forma, kad būtų prasmingi ir naudingi žmogui“[366]. Maždaug taip pat informacija suprantama ir Lietuvos autorių darbuose: informacija – tai „duomenys, turintys prasmę“[367]. Tam tikrais atvejais literatūroje pabrėžiamas ir duomenų formos bei turinio tinkamumas naudoti, kuris leidžia

---

359 Laudon, K. C.; Laudon, J. P. Essentials of Management Information Systems. 3-iasis leidimas. New Jersey: Prentice-Hall, Inc., 1999, p. 8.

360 Gordon, J. R.; Gordon, S. R. Information systems. 2-asis leidimas. The Dryden Press: Harcourt Brace College Publisher, 1999, p. 6.

361 Potter, R. T., *et al*. Introduction to Information Systems: Supporting and Transforming Business. John Wiley & Sons, Inc., 2007, p. 5.

362 Dzemydienė, D.; Naujikienė, R. Informacinės sistemos. Duomenų struktūros ir valdymas. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2004, p. 12.

363 Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008, p. 7.

364 Potter, R. T., *et al*. Introduction to Information Systems: Supporting and Transforming Business. John Wiley & Sons, Inc., 2007, p. 5; Laudon, K. C.; Laudon, J. P. Essentials of Management Information Systems. 3-iasis leidimas. New Jersey: Prentice-Hall, Inc., 1999, p. 5; Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008, p. 7; Wacks, P. Personal Information: Privacy and the Law. Oxford: Clarendon Press, 1989, p. 25.

365 Potter, R. T., *et al*. Introduction to Information Systems: Supporting and Transforming Business. John Wiley & Sons, Inc., 2007, p. 5.

366 Laudon, K. C.; Laudon, J. P. Essentials of Management Information Systems. 3-iasis leidimas. New Jersey: Prentice-Hall, Inc., 1999, p. 8.

367 Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008, p. 7.

tenkinti žmonių informacinius poreikius[368]. Apibendrinant galima teigti, kad duomenys yra tik tam tikra „žaliava“[369] informacijai gauti. Apibrėžiant BK 198 straipsnyje numatyto nusikalstamos veikos dalyko požymius, į tokius aspektus atsižvelgiama ir teismų praktikoje: *Elektroninių duomenų ir informacijos sąvokos skiriasi – duomenys tampa informacija tik juos subjektyviai suvokus ir supratus (perskaičius, pamačius, išgirdus). Duomenys yra tik potenciali informacija*[370].

Kalbant apie duomenų ir informacijos santykį baudžiamosios teisės srityje, svarbu atkreipti dėmesį į tai, kad duomenų sąvoka yra platesnė nei informacijos sąvoka. Netinkamo termino pasirinkimas gali lemti pernelyg siauras nusikalstamų veikų, kuriomis pažeidžiamas konfidencialumas, inkriminavimo galimybes. Renkantis duomenų arba informacijos sudėties požymį nereikėtų pamiršti, kad informacinių procesų dalyviai yra ne tik žmonės, bet ir informacinės sistemos. Atitinkamai ne visi informacinės sistemos atliekami duomenų apdorojimo (tvarkymo) veiksmai ir jų rezultatai suvokiami bei matomi žmogui – potencialios informacijos gavėjui.

Dėl to BK 198 straipsnyje numatytos nusikalstamos veikos dalyką įvardijanti informacija ir šiam požymiui taikyti reikalingas duomenų suvokimas gali lemti, kad nuo neteisėto poveikio lieka neapsaugoti duomenys, esantys *priešinformacinėje* stadijoje[371]. Baudžiamajame įstatyme neturėtų būti įtvirtinti nusikalstamų veikų inkriminavimo apribojimai, priklausantys nuo to, ar pavyksta nustatyti duomenų suvokimo faktą. Tai leistų išvengti ir duomenų bei informacijos konfidencialumo apsaugos lygių diferencijavimo – grėsmių konfidencialumui gali kilti, be kita ko, ir „surenkant neapdorotus duomenis prieš juos transformuojant į informaciją, kuri gali būti naudojama žmogaus“[372]. Dėl to baudžiamajame įstatyme numačius duomenų, o ne informacijos

[368] Saulis, A.; Vasilecas, O. Informacinių sistemų projektavimo metodai: mokomoji knyga. Vilnius: Technika, 2008, p. 9–10.

[369] Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008, p. 7.

[370] Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendis baudžiamojoje byloje Nr. 1-234-825/2017.

[371] Atsižvelgiant į kaltininko tyčios kryptingumą, tokie atvejai galėtų būti vertinami tik iš parengtinės nusikalstamos veikos pozicijų.

[372] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 14.

sudėties požymį, analogiškos baudžiamosios teisės priemonės būtų pradėtos taikyti anksčiau nei duomenys virsta informacija. Esant tokiam požiūriui, galima daryti svarbią išvadą, jog informacinių technologijų srityje reiškiama nuomonė, kad *informacijos vertė sąlygiškai didesnė negu duomenų*[373], neturi įtakos nustatant baudžiamąją atsakomybę už įvairius elektroninių duomenų konfidencialumo pažeidimus. Konfidencialumo prasme ir duomenys, ir informacija, kvalifikuojant kaltininko padarytas veikas pagal BK 198 straipsnį, turėtų būti laikomi lygiaverčiais. Pavyzdžiui, toks požiūris aktualus tais atvejais, kai duomenų konfidencialumą bandoma apsaugoti perduodant duomenis ryšių tinklais tarp informacinių sistemų.

Remiantis užsienio valstybių praktika kriminalizuojant įvairius elektroninėje erdvėje padaromus konfidencialumo pažeidimus, matyti, kad teisėkūros lygmeniu ne visada pabrėžiama duomenų ir informacijos skirtumų svarba. Dėl to vienose valstybėse (pavyzdžiui, Vokietijoje, Portugalijoje, Kipre) nusikalstamų veikų, bendriausia prasme susijusių su neteisėta prieiga prie duomenų, dalykas yra įvardijamas kompiuterinių duomenų terminu, o kitose (pavyzdžiui, Rusijoje) vartojamas kompiuterinės informacijos arba tiesiog informacijos terminas. Vis dėlto šiam pastebėjimui būtinas ir tam tikras patikslinimas – nusikalstamos veikos dalyku laikant informaciją, gali būti nenurodomas jos ir duomenų skirtumas. Kita vertus, neretai šiuos terminus vertinti kaip sinonimus leidžia, pavyzdžiui, Rusijos autorių pateikti *kompiuterinės informacijos* kaip Rusijos baudžiamojo įstatymo 272 straipsnyje numatytos nusikalstamos veikos (neteisėtos prieigos prie kompiuterinės informacijos) dalyko apibrėžimai. Juose informacijai apibūdinti vartojamas būtent duomenų terminas, pavyzdžiui, kompiuterinė informacija apibrėžiama kaip „patys įvairiausi duomenys apie asmenis, daiktus, faktus, įvykius, reiškinius ir procesus, neatsižvelgiant į jų pavaizdavimo formą, kurie yra užfiksuoti kompiuterinėje laikmenoje arba perduodami telekomunikacijos kanalais tokios formos, kuri yra

[373] Dzemydienė, D.; Naujikienė, R. Informacinės sistemos. Duomenų struktūros ir valdymas. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2004, p. 12. Tokia išvada daroma dėl to, kad su duomenimis turėtų būti atliekami įvairūs veiksmai juos padarant tinkamais naudotis žmogui. Informacija gaunama apdorojus duomenis: tai galėtų būti formatavimas, filtravimas, sumavimas, analizė ar kitos sudėtingesnės operacijos.

tinkama apdoroti kompiuteriui“[374]. Be to, kompiuterinė informacija dar suprantama kaip „duomenys, esantys vienoje iš kompiuterinės informacijos laikmenų (kietasis diskas ar išorinės laikmenos <...>), kurie gali būti perduodami kompiuterių komunikacijos kanalais ir manipuliavimas jais galimas tik naudojant kompiuterį“[375].

Nustačius informacijos ir duomenų tarpusavio ryšį, galima pradėti nagrinėti antrąjį klausimą, kaip baudžiamosios teisės srityje turėtų būti suvokiami elektroniniai duomenys. Aiškinant šią sąvoką, tam tikrų sunkumų kyla dėl to, kad šalia jos dar vartojama kompiuterinių duomenų sąvoka, kuri būtent ir minima Konvencijoje dėl elektroninių nusikaltimų ir Direktyvoje 2013/40/ES.

Konvencijos dėl elektroninių nusikaltimų I skyriaus 1 straipsnio b punkte nurodyta, kad kompiuteriniai duomenys – „tai bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, taip pat programa, pagal kurią kompiuterinė sistema gali atlikti tam tikrą funkciją“. Direktyvos 2013/40/ES 2 straipsnio b punkte kompiuteriniai duomenys apibūdinami kaip „faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją“. Kaip matyti, svarbiausias šių apibrėžimų aspektas yra duomenų tinkamumas apdoroti informacinėje (kompiuterinėje) sistemoje. Remiantis informacinės sistemos veiklos principais, tampa akivaizdu, kad duomenų apdorojimo joje galimybės turėtų būti siejamos su duomenų forma, leidžiančia su jais atlikti įvairias operacijas (veiksmus). Dėl to Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje (25 punktas) kompiuteriniai duomenys yra siejami su elektroniniais ar kitos formos duomenimis, kuriuos įmanoma tiesiogiai apdoroti.

Pabrėžtina, kad Konvencijoje dėl elektroninių nusikaltimų ir Direktyvoje 2013/40/ES suformuluotos kompiuterinių duomenų sąvokų ištakos yra siejamos su aptartuoju ISO/IEC 2382-1:1996 standartu. Šiame standarte duomenys apibrėžiami kaip „formalizuotas

[374] Vetrov, N. I. Ugolovnoe pravo. Osobennaja chast: uchebnik [Criminal law. Special Part: Textbook]. 2-oe izd. Moskva: Juniti-dana: Zakon i pravo, 2002, p. 369.

[375] Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik [Russian criminal law. Special Part: Textbook]. Borzenkova, G. N.; Komissarova, V. S. (red.), Moskva: Zercalo-M, 2005, p. 283.

informacijos vaizdinys, tinkamas perduoti kitiems, suvokti ir apdoroti“. Be to, jame nurodoma, kad duomenys gali būti apdorojami rankiniu būdu arba automatinėmis priemonėmis, todėl ši duomenų savybė – jų *tinkamumas apdoroti automatinėmis priemonėmis,* minėtuosiuose teisės aktuose tapo pateiktos kompiuterinių duomenų sąvokos pagrindu. Dar manytina, kad būtent dėl to ir Konvencijoje dėl elektroninių nusikaltimų, ir Direktyvoje 2013/40/ES kompiuteriniai duomenys yra apibrėžiami bene identiškai.

Kaip minėta, dėl technologinio neutralumo principo taikymo daugumos valstybių baudžiamuosiuose įstatymuose kompiuterinių duomenų sąvoka nepateikiama, taip sudarant sąlygas su technologijomis susijusių teisės normų raidai. Tose valstybėse, kur vis dėlto bandoma apibrėžti šį nusikalstamos veikos dalyką, kompiuterinių duomenų sąvoka suformuluota gana abstrakčiai – svarbiausiu jos aspektu laikoma duomenų forma, leidžianti juos apdoroti informacinėje (kompiuterinėje) sistemoje. Pavyzdžiui, Bulgarijos baudžiamojo įstatymo[376] 93 straipsnio 22 punkte kompiuterizuoti duomenys apibūdinami kaip „bet koks faktų, informacijos ar sąvokų pateikimas tokia forma, kuri yra tinkama automatiniam apdorojimui, įskaitant kompiuterio programą“. Panašus kompiuterinių duomenų apibrėžimas pateikiamas ir Kipro įstatymo Nr. 22 (III) 04[377] 2 straipsnyje, kuriame nurodoma, kad kompiuteriniai duomenys yra „bet koks faktų, informacijos ar sąvokų pateikimas tokia forma, kuri gali būti apdorojama kompiuterinės sistemos, apimančios bet kurią kompiuterinę programą, galinčią priversti kompiuterį atlikti funkciją“. Tokie kompiuterinių duomenų apibrėžimai leidžia pastebėti ir gana didelę Konvencijos dėl elektroninių nusikaltimų bei Direktyvos 2013/40/ES nuostatų įtaką juos konstruojant. Vadinasi, būtent šių teisės aktų nuostatos lėmė bene identišką valstybių, esančių ES narėmis arba (ir) ratifikavusių minėtąją Konvenciją, suvokimą, ką reikėtų laikyti kompiuteriniais duomenimis. Beje, panašus požiūris į nusikalstamos

[376] Criminal Code of the Republic of Bulgaria [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: <*https://www.coe.int/en/web/cybercrime/country-profiles*>.
Bulgarijos Respublika Konvenciją dėl elektroninių nusikaltimų ratifikavo 2005 m. balandžio 7 d.

[377] Cyprus Law No. 22(III)04 [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: <*https://www.coe.int/en/web/cybercrime/country-profiles*>.
Kipro Respublika Konvenciją dėl elektroninių nusikaltimų ratifikavo 2005 m. sausio 19 d.

veikos, pažeidžiančios kompiuterinės informacijos konfidencialumą, dalyką yra susiformavęs ir tose valstybėse, kurios nepriklauso minėtųjų valstybių grupei. Pavyzdžiui, Rusijos baudžiamajame įstatyme kompiuterinę informaciją, kaip vieną iš informacijos rūšių, apibūdinantys požymiai (neteisėta prieiga prie kompiuterinės informacijos) yra įtraukti į 272 straipsnyje esančios nusikalstamos veikos sudėtį. Šiame straipsnyje kompiuterine informacija laikoma ta, kuri yra automatiškai apdorojamose laikmenose, kompiuteryje, kompiuterinėje sistemoje arba jų tinkle. Nors, kaip matyti, kompiuterinė informacija apibrėžiama remiantis ne *tinkamumo apdoroti kompiuterinėje sistemoje*, o tokios *informacijos buvimo vietos* kriterijumi, būtent jos buvimas sistemoje (suvokiamoje bendriausia prasme), tam tikroje jos dalyje ar laikmenoje sudaro sąlygas šią informaciją apdoroti automatiškai. Dėl to įvairūs autoriai, interpretuodami, kaip turėtų būti suprantama kompiuterinė informacija, taiko vieną iš šių kriterijų. Pavyzdžiui, kompiuterinė informacija yra apibrėžiama kaip ta, kuri yra „pateikta specialiu būdu, skirtu ir tinkamu jos automatizuotam apdorojimui, saugojimui ir perdavimui, esanti materialioje laikmenoje ir turinti savininką, nustačiusį jos sukūrimo, apdorojimo, perdavimo ir sunaikinimo tvarką“[378]. Kartais, vadovaujantis *informacijos buvimo vietos kriterijumi*, bandoma sukonkretinti (išvardijant galimus variantus), kur galima rasti tokio pobūdžio informacijos: „informacija, esanti operatyvioje kompiuterio atmintyje ar kitose kompiuterinėse laikmenose, ir prijungtose prie kompiuterio, ir išoriniuose kaupikliuose, įskaitant diskelius, lazerinius ir kitokius diskus.“[379] Be to, prieiga prie kompiuterinės informacijos laikoma neteisėta ir tais atvejais, kai perimama kompiuterių tinklais perduodama informacija. Vadinasi, galima teigti, kad taikant skirtingus – *tinkamumo apdoroti kompiuterių sistemoje* ir *informacijos buvimo vietos* – kriterijus, kompiuterinės informacijos apibrėžimas neišvengiamai šiek tiek skiriasi, bet neteisėtos prieigos prie informacijos dalyko specifinės savybės išlieka tos pačios. Kaip antai aiškus duomenų formos, leidžiančios ją apdoroti informacinėje

[378] Mazurov, V. A. Kompiuternye prestuplenija: klasifikacija i sposoby protivodeistvija [Computer crime: classification and ways of countraction]. Moskva: Paletip, 2002, p. 33.

[379] Ugalovnoe pravo Rossijskoj Federacii. Osobennaja chast: uchebnik [Criminal Law of the Russian Federation. Special part: The textbook]. Inogamova-Khega, L. V.; Rarog, A. I.; Chuchaeva, A. I. (red.) Moskva: INFRA-M: KONTRAKT, 2005, p. 502.

(kompiuterinėje) sistemoje, ir pačių duomenų buvimo tokioje sistemoje ryšys matomas duomenis analizuojant informacinių bei komunikacijos technologijų srityje. Bendriausia prasme duomenys joje apibrėžiami kaip „kompiuterio apdorojami objektai – visa, kas laikoma kompiuterio laikmenose“[380], arba kaip „faktų, sudarytų iš skaičių, ženklų ir simbolių, rinkinys, laikomas kompiuteryje tokiu būdu, kad jis gali būti apdorojamas kompiuteriu“[381].

Aptariant Lietuvos BK 198 straipsnio dispozicijoje nurodyto nusikalstamos veikos dalyko požymius, reikėtų pabrėžti, kad įgyvendinus konvencines ir Direktyvos 2013/40/ES nuostatas vis dėlto buvo pasirinkta ne kompiuterinių, o elektroninių duomenų sąvoka. Pats autentiškas elektroninių duomenų išaiškinimas dėl technologinio neutralumo principo taikymo BK nepateikiamas, bet tam tikrus elektroninių duomenų interpretavimo būdus galima matyti kituose nacionaliniuose teisės aktuose. Juose, kaip ir BK XXX skyriuje, vartojamas būtent elektroninių, o ne kompiuterinių duomenų terminas. Pavyzdžiui, Lietuvos Respublikos elektroninio parašo įstatymo (toliau – Elektroninio parašo įstatymas)[382] 2 straipsnio 2 dalyje elektroniniai duomenys apibūdinti kaip „visi duomenys, kurie tvarkomi informacinių technologijų priemonėmis“. Panašus elektroninių duomenų apibrėžimas yra pateikiamas ir Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. spalio 21 d. įsakymo Nr. 1V-1013 „Dėl Viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų saugumo ir vientisumo užtikrinimo taisyklių patvirtinimo“[383] 3 punkte. Jame elektroniniai duomenys apibrėžiami kaip „duomenys, pateikti tokia forma, kuri tinkama juos tvarkyti informacinėje sistemoje“. Dėl to aiškinant neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos dalyką – elektroninius duomenis – šių teisės aktų įtaka yra akivaizdi.

---

[380] Dagienė, V., *et al*. Enciklopedinis kompiuterijos žodynas. Vilnius: TEV, 2008, p. 96.

[381] Dictionary of Information Technology. 2-asis leidimas. Greasby, L.; Green, Th. (eds). Teddington: Peter Collin Publishing, 1996, p. 93.

[382] Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios*, 2000, Nr. 61-1827.

[383] Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. spalio 21 d. įsakymas Nr. 1V-1013 „Dėl Viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų saugumo ir vientisumo užtikrinimo taisyklių patvirtinimo“. *Valstybės žinios*, 2011, Nr. 130-6174.

Kaip matyti, būtent *tinkamumo apdoroti automatinėmis priemonėmis* kriterijus, taikomas konstruojant elektroninių duomenų sąvoką nacionalinėje teisėje ir laikomas pagrindu formuluojant kompiuterinių duomenų sąvoką minėtuosiuose tarptautiniuose bei ES teisės aktuose, parodo daug elektroninių ir kompiuterinių duomenų panašumų. Analizuojant pateiktus apibrėžimus, iš pirmo žvilgsnio gali atrodyti, kad svarbiausias kriterijus, kuriuo remiantis atribojamos šios sąvokos, yra duomenims apdoroti taikomos technologijos. Pavyzdžiui, Konvencijoje dėl elektroninių nusikaltimų nurodoma kompiuterinė sistema, o Direktyvoje 2013/40/ES – informacinė sistema. Ši atskyrimo problema yra siejama su minėtuoju technologijų ir terminologijos klausimu, nuolat kylančiu bandant apibrėžti įvairias technologijas žyminčias sąvokas. Šiuo požiūriu reikėtų atkreipti dėmesį į tai, kad aptariant neteisėto prisijungimo prie informacinės sistemos (BK 198[1] straipsnis) dalyko problematiką, buvo prieita prie išvados, kad analizuojant informacinę ir kompiuterinę sistemą bendriausia prasme mintyje turimos panašios technologijos. Dėl to ir kompiuteriniai, ir elektroniniai duomenys turėtų būti suvokiami panašiai[384], pirmumą teikiant būtent jų formai, o ne bandymams konkrečiai įvardyti technologijas, kuriomis apdorojami minėtieji duomenys[385]. Tai leistų išvengti BK 198 straipsnyje numatytos nusikalstamos veikos dalyko apibrėžties nepagrįsto susiaurinimo pavojaus.

Nuo minėtųjų elektroninių duomenų aiškinimų nėra nutolusi ir teismų praktika. Joje pateikiamas elektroninių duomenų kaip neteisėto elektroninių duomenų perėmimo ir panaudojimo dalyko aiškinimas yra bene analogiškas elektroninių duomenų sąvokai, įtvirtintai Elektroninio parašo įstatyme (beje, teismų sprendimuose dažniausiai į šį įstatymą pateikiama nuorodų). Kaip antai teismų praktikoje galima rasti išaiškinimų, kad BK 198 straipsnio 1 dalyje numatyto nusikaltimo dalykas yra elektroniniai duomenys, t. y. *duomenys, tvarkomi informacinių technologijų priemonėmis. Elektroniniai duomenys turi būti*

[384] Juo labiau kad Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje kompiuteriniai duomenys, kaip minėta, yra siejami su elektroniniais ar kitos tiesiogiai apdorojamos formos duomenimis (25 punktas).

[385] Tikėtina, kad kompiuterinių duomenų, kaip ir kompiuterinių sistemų, terminas dažniausiai vartojamas atkreipiant dėmesį į tai, jog kalbama apie sistemas, kurių pagrindą sudaro kompiuterių technologijos. Atitinkamai jomis apdorojami duomenys, kurie gali būti vadinami kompiuteriniais duomenimis.

arba sukurti elektronine forma, arba perkelti į tokią formą (pavyzdžiui, nuskenuotas knygos puslapis, surinktas tekstas) <...>. Elektroniniai duomenys apima ir kompiuterines programas arba programinę įrangą[386].

Teigtina, kad norint duomenis pripažinti elektroniniais, jie turėtų būti arba sukurti, arba perkelti į elektroninę formą. Be to, akivaizdu, kad tokios formos duomenys gali egzistuoti tik pačia bendriausia prasme suvokiamoje informacinėje sistemoje ar jos dalyje (ne tik kompiuteriuose, bet ir faksuose, mobiliuosiuose telefonuose, elektroninių ryšių tinkluose ar internete[387], taip pat įvairiuose informacijos kaupikliuose, pavyzdžiui, kompaktiniuose diskuose, USB atmintinėse ir kt.). Dėl to pagal BK 198 straipsnį nekvalifikuotini kėsinimaisi į tokių duomenų, iš kurių tik gali būti formuojami elektroniniai duomenys (pavyzdžiui, įvairūs užrašai, schemos ir pan.), bet jie dar neperkelti į tokią formą, konfidencialumą. Šie duomenys neatitinka specifinių elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos dalyko ypatybių. Kita vertus, dėl tokio aiškinimo kyla nemažai problemų sprendžiant, ar pagal BK 198 straipsnį kvalifikuotina veika, jei ją darant pasikeitė elektroninių duomenų forma.

Apibendrinant galima teigti, kad elektroniniams duomenims apibūdinti gali būti taikomi du – jų *tinkamumo apdoroti informacinėje sistemoje* ir tokių *duomenų buvimo vietos* – kriterijai, kurie padeda aiškiau suprasti, kokios ypatybės būdingos BK 198 straipsnyje pateikiamos nusikalstamos veikos dalykui. Pirmasis iš jų nurodo duomenų formą, kurią gali atpažinti informacinė sistema, atitinkamai sistema gali atlikti įvairius minėtųjų duomenų apdorojimo veiksmus. Antrasis kriterijus gali padėti apibūdinti elektroninius duomenis, bet jį taikant reikia gana detalių nuorodų į technologijas, kur konkrečiai informacinėje sistemoje galima rasti šiuos duomenis. Vertinant minėtuosius kriterijus, reikėtų atsižvelgti ir į glaudžią jų tarpusavio sąsają – galimybės apdoroti duomenis siejamos su jų specifine (elektronine) forma, kuri išlaikoma, jei duomenys yra įvedami į informacinę sistemą.

---

[386] Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendis baudžiamojoje byloje Nr. 1-234-825/2017; Vilniaus miesto 2 apylinkės teismo 2011 m. liepos 1 d. nuosprendis baudžiamojoje byloje Nr. 1-188-387/2011; Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje Nr. 1A-977/2011.

[387] Abramavičius, A., *et al.* Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 418.

2.1.2. Elektroninių duomenų formos kitimo įtaka juos pripažįstant BK 198 straipsnyje esančios nusikalstamos veikos dalyku

Kaip minėta, BK 198 straipsnyje numatytos nusikalstamos veikos dalykas yra viena iš duomenų rūšių – nevieši elektroniniai duomenys, kuriems identifikuoti taikomi du aptartieji *tinkamumo juos apdoroti informacinėje sistemoje* ir tokių *duomenų buvimo vietos* kriterijai. Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos aprašymo būdas lemia tai, kad kiekviena dispozicijoje nurodyta alternatyvi pavojinga veika (pavyzdžiui, įgijimas, laikymas, paskleidimas) turėtų būti siejama būtent su elektroniniais duomenimis ir jų konfidencialumo pažeidimais. Taip interpretuojamas šios nusikalstamos veikos dalykas rodo, kad įvairūs su duomenimis atliekami neteisėti veiksmai, esantys ne elektroninės formos (neatitinkantys minėtųjų kriterijų), į BK 198 straipsnio reguliavimo sritį nepatenka. Elektroninės duomenų formos svarba pabrėžiama ir teismų praktikoje – elektroninius duomenis *galima naudoti ir jais įvairiais būdais disponuoti išimtinai įrenginių, skirtų apdoroti elektroniniams duomenims, pagalba, todėl elektroninė duomenų forma yra esminis šios nusikalstamos veikos sudėties skiriamasis požymis, o vienas pagrindinių nusikaltimo įrankių – kompiuterinė technika ir programinė įranga (abi jos yra neatsiejamos viena nuo kitos naudojant nusikalstamai veikai)*[388]. Kita vertus, šis požiūris padeda atskleisti ir gana sudėtingas neteisėto elektroninių duomenų perėmimo bei panaudojimo inkriminavimo problemas, kurios kilo dėl pasirinkto minėtosios nusikalstamos veikos aprašymo būdo.

Sprendžiant, kokias ir kiek alternatyvių veikų padarė kaltininkas, sunkumų paprastai neturėtų kilti tais atvejais, kai elektroniniai duomenys nepraranda šios formos. Pavyzdžiui, vienoje iš baudžiamųjų bylų konstatuota, kad *R. R. įgijo, laikė, pasisavino, paskleidė neviešus elektroninius duomenis, tai yra <...> iš AB „(duomenys neskelbtini)“ <...> Vandenilio gamybos komplekso vandenilio įrenginio automatikos valdymo aparatinės patalpose esančio įrašymo įrenginio ir šiame įrenginyje esančio vaizdo archyvo <...> nukopijavo ir į išorinę įrašymo laikmeną neteisėtai įsirašė <...> informaciją apie AB „(duomenys neskelbtini)“ <...> įvykusį gaisrą, taip neteisėtai įgijo neviešus elektroninius duome-*

[388] Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendis baudžiamojoje byloje Nr. 1-234-825/2017.

nis, juos pasisavino, laikė, tai yra turėjo su savimi ir <...> šiuos neteisėtai įgytus, laikytus ir pasisavintus neviešus elektroninius duomenis apie AB „(duomenys neskelbtini)" kilusį gaisrą paskleidė interneto puslapyje <...>[389]. Atsižvelgiant į tai, R. R. pripažintas kaltu pagal BK 198 straipsnio 1 dalį.

Kiek kitokia padėtis susiklosto tada, kai neteisėtai disponuojama duomenimis, kurių elektroninę formą pavyksta išsaugoti tik nusikalstamos veikos pradžioje, o vėlesni kaltininko veiksmai atliekami su duomenimis, kurie jau yra nebe elektroninės formos, o turi materialiąją išraišką (pavyzdžiui, yra užrašyti ar išspausdinti). Tokiais atvejais kyla abejonių, ar kaltininkui inkriminuotinos tos BK 198 straipsnyje numatytos alternatyvios veikos, kurios padarytos disponuojant elektroninę formą praradusiais duomenimis. Pavyzdžiui, iš faktinių bylos aplinkybių gali paaiškėti, kad kaltininkas neteisėtai įgijo elektroninius duomenis, vėliau juos išspausdino ir paskleidė jau nebe elektroninės formos, o užfiksuotus popieriuje. Būtent į tokią probleminę situaciją, analizuojant duomenų kopijavimo teisinio vertinimo variantus, atkreiptas dėmesys ir literatūroje. Šiuo klausimu yra susiformavusios dvi skirtingos pozicijos – vienų autorių nuomone, kopijavimu gali būti laikomi tik tokie veiksmai, kai duomenys yra perkeliami iš vienos kompiuterinės laikmenos (kompiuterio) į kitą kompiuterinę laikmeną (kompiuterį)[390]. Kitiems autoriams[391] būdingas kiek lankstesnis požiūris – kopijavimu pripažįstami ir tie veiksmai, kuriais duomenys perkeliami iš elektroninės į bet kokią kitą formą. Remiantis pastarąja nuomone, kopijavimo būdas neturi įtakos kvalifikuojant veiką, nes baudžiamosios teisės priemonėmis yra saugomi elektroniniai duomenys, neatsižvelgiant į jų buvimo vietą (ar jie yra užfiksuoti popieriuje, ar išsaugoti išorinėje informacijos laikmenoje ir kt.).

---

[389] Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendis baudžiamojoje byloje Nr. 1-188-785/2009.

[390] Mazurov, V. A. Kompiuternye prestuplenija: klasifikacija i sposoby protivodeistvija [Computer crime: classification and ways of countraction]. Moskva: Paletip, 2002, p. 107.

[391] Vetrov, N. I. Ugolovnoe pravo. Osobennaja chast: uchebnik [Criminal law. Special Part: Textbook]. 2-oe izd. Moskva: Juniti-dana: Zakon i pravo, 2002, p. 370; Naumov, A. V. Rossijskoe ugolovnoe pravo: kurs lekcij [Russian criminal law: the course of lectures]. 4-asis leidimas. Moskva: Volters Kluver, 2007, p. 283.

Analizuojant BK 198 straipsnyje numatytas alternatyvias veikas vis dar lieka neaišku, kaip turėtų būti vertinami atvejai, kai, pavyzdžiui, elektroniniai duomenys neteisėtai išspausdinami ir laikomi kaip spausdintas variantas bei vėliau tokios formos paskleidžiami. Tada diskutuotina, ar kaltininkui gali būti inkriminuojamas ne tik elektroninių duomenų įgijimas, bet ir jų laikymas bei paskleidimas, jei įgyjami, laikomi ir paskleidžiami elektroninę formą praradę duomenys. Ši problema sprendžiama atsižvelgiant į tai, kam aiškinant BK 198 straipsnį bus teikiamas prioritetas, ar duomenų išraiškos formai (dalykui būdingoms savybėms), ar vis dėlto duomenų elektroninės formos reikalavimai bus keliami tik pirminiam duomenų šaltiniui. Kaip matyti iš negausios teismų praktikos, elektroninių duomenų konfidencialumo pažeidimai pripažįstami ir tada, kai elektroninių duomenų forma neišsaugoma visų kaltininko padarytų pavojingų veikų metu. Pavyzdžiui, vienoje iš baudžiamųjų bylų kaltininkas, be kitų nusikalstamų veikų, nuteistas ir pagal BK 198 straipsnio 1 dalį, t. y. jis *neteisėtai stebėjo neviešus elektroninius duomenis apie V. G., R. S., A. B., A. M., R. P., L. L., V. T., L. Ch., A. P., R. V., Z. K., J. K., J. Ch., R. M., V. M., A. G., V. G., D. R., S. Ž., V. B., V. V., A. J., S. D. vardą, pavardę, asmens kodą, gyvenamąją vietą, šeiminę padėtį, išduotus asmens tapatybės dokumentus, darbovietę, pajamas, šiuos duomenis neteisėtai įgijo, išspausdindamas valstybinės mokesčių inspekcijos kompiuterinės duomenų bazės išrašus (pažymas), po to neteisėtai įgytus neviešus minėtuosius elektroninius duomenis neteisėtai paskleidė <...> per kelis kartus perduodamas G. L*[392]. Iš šio teismo sprendimo matyti, kad aplinkybė, jog elektroniniai duomenys buvo išspausdinti ir tokios formos paskleisti, netrukdė teismui konstatuoti elektroninių duomenų stebėjimo, įgijimo ir paskleidimo. Manytina, kad tokią teismo poziciją lėmė tai, jog įgyti ir paskleisti buvo nevieši duomenys, kurių pirminis šaltinis išliko elektroninės formos, o pati padaryta veika laikyta tęstine[393]. Toks aiškinimas teismų praktikoje yra ne vienintelis. Kaip

[392] Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. baudžiamasis įsakymas byloje Nr. 1-617-885/2011.

[393] Minėtaisiais ir panašiais atvejais priėjus prie kitokios išvados būtų sukurta probleminė situacija, kai, pavyzdžiui, asmens, įgijusio prieš tai neteisėtai išspausdintus elektroninius duomenis, veiksmai pagal BK 198 straipsnį negalėtų būti kvalifikuojami (jei nenustatytas bendrininkavimo faktas). Be to, tikėtina, kad laikymo ir

antai Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendyje baudžiamojoje byloje Nr. 1-234-825/2017 paskleidimo veika yra susieta su elektroninių duomenų turinio, be kita ko, ir perkelto į materialiąją formą, paskleidimu:

Paskleidimu laikomas ir bet koks šių duomenų persiuntimas elektroninių ryšių tinklų pagalba, jų patalpinimas į vietas (pvz., tinklalapį internete), iš kur tampa prieinami kitiems asmenims (tai apima ir nuorodų į tokias vietas kūrimą ar rinkimą siekiant palengvinti priėjimą prie šių duomenų). Kitaip tariant, tai reiškia elektroninių duomenų turinio (ir kompiuterine forma, ir perkelto į materialinę formą) paskleidimą neapibrėžtam trečiųjų asmenų ratui, nepriklausomai kokiu būdu jis paskleistas: žodžiu, raštu ar kita materialia išraiška, per visuomenės informavimo priemones (knygas, laikraščius, žurnalus ar kitus leidinius, televizijos, radijo programas, kino ar kitą garso ar vaizdo studijos produkciją), išplatintas elektroninėmis priemonėmis, intraneto ar interneto tinklais, praneštas viešųjų renginių metu ir panašiai.

Viena vertus, tokia teismų praktika padeda spręsti BK 198 straipsnyje numatytų alternatyvių veikų inkriminavimo problemą, bet, kita vertus, toks neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymių interpretavimas nevisiškai atitinka šios nusikalstamos veikos aprašymą BK 198 straipsnio dispozicijoje. Jeigu šio BK straipsnio dispozicijoje neatskiriami *informacinėje sistemoje laikomi* ir *joje perduodami duomenys*, neišvengiamai tenka spręsti minėtąją dilemą: ar elektroninės duomenų formos išsaugojimas (kai pirminis šaltinis yra elektroniniai duomenys) yra viena iš būtinų baudžiamosios atsakomybės kilimo sąlygų, ar vis dėlto inkriminuojant BK 198 straipsnyje numatytą nusikalstamą veiką elektroninių duomenų formos reikalavimas turėtų būti taikomas tik pirminiam duomenų šaltiniui[394]. Dėl įstatymo leidėjo pasirinktos šios nusikalstamos veikos

paskleidimo veikos negalėtų būti inkriminuojamos asmeniui, kuris laikė ir paskleidė neteisėtai išsispausdintus elektroninius duomenis, net jei konstatuotas tęstinės nusikalstamos veikos faktas.

[394] Dėl pastarojo požiūrio, lemiančio gana platų normos aiškinimą, gali kilti ir papildomų problemų – pavyzdžiui, kaip vertintinos situacijos, kai duomenys išlieka tik materialiosios formos, t. y. nelieka pirminių elektroninių duomenų. Be to, dauguma neviešų elektroninių duomenų gali būti saugoma ir materialiosios formos, tada neteisėtai įgijus būtent tokios formos duomenis (nepriėjus prie elektroninių duomenų) nusikalstamai veikai kvalifikuoti taip pat galėtų būti taikomas BK 198 straipsnis.

konstrukcijos ir šiuo klausimu itin negausios teismų praktikos lieka atviras klausimas, kaip vertinti kaltininko veiksmus, jei visos nusikalstamos veikos metu duomenų forma buvo keičiama iš elektroninės į materialiąją. Šiuo požiūriu reikėtų atkreipti dėmesį į tai, kad nusikalstamos veikos sudėtyje numatant ir elektroninę, ir materialiąją formą galinčius įgyti duomenis (informaciją) kaip nusikalstamos veikos dalyką, BK yra vartojamas materialaus objekto, kurio turinys ar informacija apie jį, pavyzdžiui, yra tarnybos paslaptis (BK 296 straipsnis), valstybės paslaptis (BK 124 straipsnis). Tokiu atveju dėl duomenų (informacijos) formos kitimo iš elektroninės į materialiąją ar priešingai neturėtų kilti problemų inkriminuojant alternatyvias veikas. Kita vertus, BK 198 straipsnyje tiesiogiai vartojant elektroninių duomenų terminą šių duomenų formos kitimo problema lieka neišspręsta.

Vienas iš atvejų, kai kvalifikuojant veiką įmanoma lanksčiau pažvelgti į byloje nustatytą elektroninių duomenų formos kitimo faktą, galėtų būti siejamas su tęstine BK 198 straipsnyje numatyta nusikalstama veika. Kasacinės instancijos teismo praktikoje pabrėžiama, kad *tęstine veika taip pat gali būti pripažįstamos situacijos, kai pasikartojantys veiksmai nėra tapatūs ar vienarūšiai, tačiau jais įgyvendinamas tas pats veikos požymis arba alternatyvūs veikos požymiai. Veiksmai, kuriais įgyvendinami alternatyvūs veikos požymiai, paprastai pripažįstami tęstine nusikalstama veika, jei juos jungia vieninga kaltininko tyčia ir jie yra padaryti dėl to paties nusikalstamos veikos dalyko*[395]. Dėl to nustačius, kad pirminiai konfidencialumą pažeidžiantys veiksmai buvo padaryti naudojantis elektroninės formos duomenimis, vėlesnis tų pačių duomenų formos keitimas neturėtų sudaryti kliūčių inkriminuojant alternatyvias BK 198 straipsnyje numatytas veikas, jei nustatyta, kad jas sieja bendra kaltininko tyčia ir šios veikos yra padarytos dėl tų pačių duomenų (jų turinio). Be to, svarstytina, ar minėtųjų kvalifikavimo sunkumų negalėtų padėti išspręsti pakeista neteisėto elektroni-

Įtvirtinus tokį nusikalstamos veikos dalyko interpretavimą ir atitinkamai padarytų pavojingų veikų vertinimą, galima spėti, kad, be kita ko, neišvengiamai tektų įrodinėti, jog materialiąją formą turintys duomenys anksčiau turėjo kitą – elektroninę – formą. Be to, toks įrodinėjimas taptų būtinas tais atvejais, kai pirminiai elektroniniai duomenys yra išlikę, ir tais atvejais, kai pirminių elektroninių duomenų nebėra.

[395] 2016 m. balandžio 28 d. Teismų praktikos nagrinėjant baudžiamąsias bylas dėl sudėtingų pavienių nusikalstamų veikų ir nusikalstamų veikų sutapčių apžvalgos išvadų 3 punktas (*Teismų praktika* 44).

nių duomenų perėmimo ir panaudojimo dalyko formuluotė iš *neviešų elektroninių duomenų į materialųjį objektą, kurio turinys yra nevieši elektroniniai duomenys*. Be abejo, toks nusikalstamos veikos dalykas galėtų būti numatytas tik vietoj *informacinėje sistemoje laikomų*, o ne *joje perduodamų* neviešų elektroninių duomenų.

2.1.3. Elektroninių duomenų ir informacinės sistemos ryšys

Dėl informacinės sistemos ir elektroninių duomenų tarpusavio sąsajos kyla ir kita BK 198 straipsnyje numatyta nusikalstamos veikos dalyko interpretavimo problema. Iš pirmo žvilgsnio atrodančios visiškai nesusijusios sąvokos iš tikrųjų pagal Konvencijos dėl elektroninių nusikaltimų ir Direktyvos 2013/40/ES nuostatas yra tarpusavyje susipynusios. Jų sąsaja parodo dar vieną technologijų ir terminologijos klausimo aspektą, kuris yra svarbus sprendžiant, kiek nusikalstamų veikų kaltininkas padarė elektroninėje erdvėje ir ar jis pažeidė tik informacinės sistemos, ar ir elektroninių duomenų konfidencialumą.

Konvencijoje dėl elektroninių nusikaltimų ir Direktyvoje 2013/40/ES kompiuterinius duomenis ir kompiuterinę (informacinę) sistemą bandoma atskirti pateikiant atskiras jų apibrėžtis. Kaip minėta, Konvencijoje dėl elektroninių nusikaltimų kompiuterinė sistema suvokiama kaip „įtaisas ar tarpusavyje sujungtų įtaisų grupė, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja duomenis“. Panaši sąvoka, tik nurodant ne kompiuterinę, o informacinę sistemą, yra suformuluota Direktyvoje 2013/40/ES. Joje informacinė sistema yra apibrėžiama kaip „prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį kompiuterinių duomenų tvarkymą, taip pat kompiuteriniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugos ir priežiūros tikslais“. Kaip matyti, šiuose apibrėžimuose elektroninių duomenų ir informacinės sistemos ryšys yra perteikiamas remiantis bene svarbiausia informacinės sistemos funkcija – elektroninių duomenų apdorojimo (tvarkymo) pagal programą. Detaliau analizuojant elektroninių duomenų ir informacinės sistemos ryšį galima matyti gana įdomią padėtį – elektroninius duomenis tampa sudėtinga atskirti nuo informacinės sistemos tada, kai aiškinamas programinės įrangos statusas informacinei sistemai apdorojant elek-

troninius duomenis. Ši problema išryškėja minėtuosiuose dokumentuose elektroniniams duomenims priskyrus ir programą (programinę įrangą), pagal kurią sistema gali atlikti tam tikrą funkciją[396]. Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje pateikiant išaiškinimą, kas turėtų būti laikoma kompiuterinės sistemos sąvokoje minimu įtaisu ar tarpusavyje sujungtų įtaisų grupe, yra minima ir programinė įranga (23 punktas). Kaip antai *įtaisas* joje yra apibūdinamas pateikiant jo sudedamąsias dalis – aparatinę (angl. *hardware)* ir programinę (angl. *software)* įrangą. Šie komponentai yra būtini, nes aparatinė įranga be programinės pati savaime neturi duomenų apdorojimo gebėjimų[397]. Būtent dėl programinės įrangos kompiuteris yra laikomas *intelektualiu informacijos apdorojimo įrankiu*[398].

Toks minėtuosiuose dokumentuose išreikštas požiūris į elektroninių duomenų ir programinės įrangos (programos) ryšį nėra naujas. Jis atitinka bendrą suvokimą, kad kalbant apie kompiuterio darbui taikomas operacines sistemas ar programinę įrangą visais atvejais neišvengiamai turimi mintyje ir elektroniniai duomenys. Tai atspindi vieną iš klasikinių kompiuterio struktūros sudarymo idėjų, kad programai reikalingos komandos „užkoduojamos kaip ir apdorojamieji duomenys bei nesiskiria nuo kitos informacijos“[399]. Dėl to, pavyzdžiui, „operacine sistema vadinamas specialiųjų programų ir duomenų rinkinys, sukurtas kompiuterinės sistemos ištekliams valdyti,

---

396 Konvencijos dėl elektroninių nusikaltimų I skyriaus 1 straipsnio b punktas: „kompiuteriniai duomenys – tai bet kokia faktų, informacijos arba sąvokų pateiktis tokiu pavidalu, kad juos būtų galima apdoroti kompiuterine sistema, *taip pat programa, pagal kurią kompiuterinė sistema gali atlikti tam tikrą funkciją*“.
Direktyvos 2013/40/ES 2 straipsnio b punktas: „Kompiuteriniai duomenys“ – faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, *įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją*“.
Pamatinio sprendimo 2005/222/TVR 1 straipsnio b punktas: „Kompiuteriniai duomenys“ – tai faktai, informacija ar sąvokos, pateiktos tokia forma, kuri tinkama tvarkyti informacinėje sistemoje, *įskaitant programą, tinkamą tam, kad informacinė sistema atliktų funkciją*“.

397 Jonušauskas, S.; Bilevičienė, T.; Kažemikaitis, V. Įvadas į informatiką. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002, p. 14.

398 Kiškis, M., *et al.* Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006, p. 20.

399 Kanapeckas, P., *et al.* Kompiuterių elementai [elektroninis išteklius]. Kaunas: Technologija, 2011, p. 475.

kompiuterio programų kūrimui palengvinti ir šių programų vykdymui valdyti“[400]. Operacinės sistemos vartotojui suteikia bendrąsias kompiuterio valdymo paslaugas, o konkrečios užduotys atliekamos naudojantis taikomosiomis programomis, kurios bendriausia prasme apibūdinamos kaip komandos ir elektroninių duomenų visuma, būtina konkretiems veiksmams atlikti[401]. Be to, toks požiūris rodo ir dvejopą elektroninių duomenų statusą. Konvencijoje dėl elektroninių nusikaltimų ir Direktyvoje 2013/40/ES pateikiant atskirus elektroninių duomenų apibrėžimus bandoma juos atskirti nuo informacinės sistemos, bet aiškinant informacinės sistemos sąvoką elektroniniai duomenys neišvengiamai tampa šios sistemos dalimi. Vadinasi, galima laikyti pagrįsta literatūroje išsakytą nuomonę, kad „duomenys neturėtų būti matomi kaip kažkas atskiro nuo technologijų, nes visada egzistuoja dvejopumas vartojant šį terminą“[402]. Atsižvelgiant į tai, vienas iš diskusinių klausimų, sprendžiant duomenų ir informacinės sistemos atskyrimo problemą, yra tiesiogiai susijęs su kompiuterio programinės įrangos (programos) teisiniu vertinimu. Tokiu atveju galimybės atriboti duomenis ir informacinę sistemą priklausytų nuo to, ar programinė įranga (programa) būtų laikoma viena iš elektroninių duomenų formų, ar vis dėlto programinė įranga būtų atskirta nuo duomenų ir laikoma priemone, padedančia apdoroti duomenis (informacinės sistemos dalimi).

Šis vienas iš technologijų ir terminologijos problemos aspektų yra tiesiogiai susijęs su nusikalstamų veikų, kuriomis pažeidžiamas elektroninių duomenų ir informacinės sistemos konfidencialumas, kvalifikavimo problemomis. Nusikalstamos veikos dalykų – elektroninių duomenų ir informacinės sistemos – atskyrimu yra pagrįstas visų veikų aprašymas Konvencijoje dėl elektroninių nusikaltimų (2–5 straipsniai) ir Direktyvoje 2013/40/ES: šiuose dokumentuose atskirai numatytos veikos, pažeidžiančios informacinių sistemų ir atskirai – elektroninių duomenų saugumą (konfidencialumą, vientisumą ir prieinamumą). Beje, šiuo atskyrimu buvo vadovaujamasi ir konstruojant šių nusikals-

---

400 Dulinskas, D.; Dulinskienė, J. ECDL visiems: kompiuterinio raštingumo pagrindai. Kaunas: Informacinių technologijų mokymo centras, 2006, p. 15.

401 *Ibidem*.

402 Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 14–15.

tamų veikų sudėtis Lietuvos BK XXX skyriuje. Jame atskirai nustatyta atsakomybė už neteisėtą prisijungimą prie informacinės sistemos (198[1] straipsnis) ir neteisėtą elektroninių duomenų perėmimą bei panaudojimą (198 straipsnis) kaip konfidencialumo pažeidimus. Be to, atskirai kriminalizuotas neteisėtas poveikis elektroniniams duomenims (196 straipsnis) ir neteisėtas poveikis informacinei sistemai (BK 197 straipsnis) kaip integralumo ir prieinamumo pažeidimai. Aiškinant *techninio kompiuterių saugumo* turinį, anksčiau buvo pabrėžiama, kad baudžiamojo įstatymo saugoma vertybė yra skaidytina į dvi atskiras dalis – elektroninių duomenų ir informacinių sistemų konfidencialumą, integralumą bei prieinamumą. Viena vertus, toks atskyrimas yra pagrįstas (pavyzdžiui, elektroninių duomenų, kurie nėra programinė įranga, atveju), kita vertus, dėl glaudžios elektroninių duomenų ir informacinės sistemos sąsajos gali kilti klausimų, kiek nusikalstamų veikų kaltininkui turėtų būti inkriminuojama.

Kaip antai nusikalstama veika yra kvalifikuojama pagal BK 198[1] straipsnį, jei nustatoma, kad kaltininkas neteisėtai prisijungė prie informacinės sistemos pažeisdamas jos apsaugos priemones. BK 198 straipsnyje kaip atskira numatyta elektroninių duomenų konfidencialumą pažeidžianti veika, kuriai, be kitų alternatyvų, būdingas ir neteisėtas neviešų elektroninių duomenų stebėjimas ar kitoks jų panaudojimas. Taigi kaltininkas, neteisėtai prisijungdamas prie informacinės sistemos, gauna prieigą prie jos ir galimybes neteisėtai naudotis sistemos ištekliais, atitinkamai ir programine įranga. Atsižvelgiant į tai, ar programinė įranga yra laikoma informacinės sistemos dalimi ar elektroniniais duomenimis, neteisėtas jos taikymas ir veikimo stebėjimas gali būti kvalifikuojamas arba nekvalifikuojamas pagal BK 198 straipsnį. Dėl tokio „definicinio neaiškumo“[403] kyla teisės keblumų ir atitinkamai klausimų, kaip jie turėtų būti sprendžiami. Šių problemų ištakos doktrinoje siejamos su kompiuterio kaip fizinio vieneto, atskirto nuo jo apdorojamų duomenų, suvokimu vietoj to, kad į jį būtų žiūrima kaip į „virtualią mašiną, iš esmės neatskiriamai integruojančią aparatinę, programinę įrangą ir duomenis“[404]. Bandant rasti galimų šios problemos sprendimo būdų, reikėtų atkreipti dėme-

[403] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 160.

[404] *Ibidem*.

sį į tai, kad galimybę informacinei sistemai funkcionuoti suteikia ir aparatinė, ir programinė įranga, todėl nesant vienos iš jų duomenų apdorojimas taptų neįmanomas. Atitinkamai kaltininkui gavus prieigą prie informacinės sistemos, tolesni jo neteisėti veiksmai sistemoje negalimi be vienokio ar kitokio programinės įrangos pritaikymo. Tokiais atvejais svarstytina, ar nereikėtų programinės įrangos atskirti nuo elektroninių duomenų ir laikyti priemone, padedančia apdoroti duomenis informacinėje sistemoje. Vadinasi, įvairūs neteisėti kaltininko veiksmai, atliekami sistemoje tiesiogiai taikant programinę įrangą (programą), pagal BK 198 straipsnį kaip kitoks neteisėtas elektroninių duomenų panaudojimas nekvalifikuotini, nes šiuo atveju elektroniniai duomenys būtų laikomi informacinės sistemos dalimi. Vis dėlto toks bendrojo pobūdžio pastebėjimas neleidžia paneigti visų aplinkybių analizės svarbos, todėl galima pritarti mokslinėje literatūroje išsakomai nuomonei, kad „<...> skirtingas vertinimas galimas remiantis atliktos veikos pobūdžiu, patirta žala ir (ar) kaltininko kalte, bet ne abejotinu (elektroninių duomenų ir informacinės sistemos – *aut. past.*) ir nepagrįstu techniniu atskyrimu“[405].

Taigi apibendrinant galima teigti, kad informacinės sistemos ir elektroninių duomenų atskyrimo sunkumų kyla dėl to, kad pagal Konvencijos dėl elektroninių nusikaltimų bei Direktyvos 2013/40/ES nuostatas elektroniniais duomenimis pripažįstama ir programinė įranga (programa). Pati programinė įranga yra neatskiriama informacinės sistemos dalis – ir ji, ir aparatinė įranga padeda užtikrinti sistemos galimybes atlikti įvairius duomenų apdorojimo veiksmus. Kadangi BK XXX skyriuje atskirai kriminalizuoti elektroninių duomenų (198 straipsnis) ir informacinių sistemų konfidencialumo (198^1 straipsnis) pažeidimai, gali kilti neaiškumų, ar kaltininko dėl neteisėto programinės įrangos taikymo sistemoje atliekami neteisėti veiksmai turėtų būti kvalifikuojami pagal BK 198 straipsnį (kaip kitoks neteisėtas elektroninių duomenų panaudojimas). Tokiais atvejais siūlytina programinę įrangą atskirti nuo elektroninių duomenų ir ją laikyti tiesiog priemone, padedančia apdoroti duomenis informacinėje sistemoje. Be abejo, dėl tokios išvados negalima paneigti poreikio

[405] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 160.

įvertinti visas aplinkybes: veikos pobūdį, sukeltus padarinius, kaltininko tyčios kryptingumą ir kt.

2.1.4. Neviešų elektroninių duomenų samprata

Nepageidaujami veiksmai, kuriais pažeidžiamas neviešų elektroninių duomenų konfidencialumas, yra įvairūs: jais gali būti siekiama gauti, atskleisti ar naudoti tam tikros rūšies duomenis nesilaikant nustatytų tokių duomenų apsaugos reikalavimų. Dėl to reikėtų analizuoti du tarpusavyje susijusius aspektus – neviešų elektroninių duomenų sampratą ir dėl tokių duomenų neviešumo kylančius įvairius įpareigojimus elgtis su jais tinkamai (nesikišti, neatskleisti ir kt.).

Pats neviešumo požymis, kurį taikant apibūdinamas nusikalstamos veikos dalykas ir jis būtinas konstatuojant elektroninių duomenų konfidencialumo pažeidimus, yra tiesiogiai numatytas ir Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje, Direktyvos 2013/40/ES 6 straipsnyje, ir neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtyje (BK 198 straipsnis). Kita vertus, lyginant, kokiu požiūriu neviešumas apibūdinamas šiuose teisės aktuose, galima įžvelgti nemažai esminių skirtumų.

Konvencijoje dėl elektroninių nusikaltimų neviešumas padeda apibūdinti kompiuterinių duomenų perdavimo procesą. Šios konvencijos aiškinamojoje ataskaitoje jis interpretuojamas siejant ne su kompiuteriniais duomenimis, o su tokių duomenų perdavimu, t. y. „terminas *neviešas* apibūdina perdavimo (komunikavimo) proceso, bet ne perduodamų duomenų pobūdį“ (54 punktas). Vadinasi, siunčiami duomenys gali būti ir viešai prieinama informacija, bet komunikavimo dalyviai gali siekti, kad pats tokių duomenų perdavimas būtų konfidencialus. Analizuojant šios Konvencijos 3 straipsnyje numatytos neteisėtos perimties nusikalstamos veikos požymius tampa akivaizdu, kad toks aiškinimas aktualus kalbant apie informacinėje sistemoje perduodamų duomenų neteisėtą gavimą, o ne apie *nejudamus duomenis* (laikomus informacinėje sistemoje). Be to, Direktyvos 2013/40/ES 6 straipsnyje minimas neviešas duomenų perdavimo būdas, o ne nevieši elektroniniai duomenys.

Aiškinant BK 198 straipsnyje kriminalizuotą nusikalstamą veiką matyti, kad įstatymų leidėjas pasuko kiek kita linkme: neviešumą jis susiejo ne su duomenų perdavimo procesu, o su nusikalstamos veikos

dalyku – elektroniniais duomenimis. Viena vertus, tokį pasirinkimą galima paaiškinti tuo, kad minėtajame BK straipsnyje kriminalizuoti ne tik perduodamų, bet ir informacinėje sistemoje laikomų duomenų konfidencialumo pažeidimai, bet dėl minėtojo pasirinkimo kyla ir tam tikrų problemų. Viena iš jų – kaip reikėtų vertinti atvejus, kai taikant technines priemones perimami viešieji elektroniniai duomenys, nors patį komunikavimo procesą buvo siekiama išlaikyti konfidencialų. Be to, neaišku, ar baudžiamoji atsakomybė kaltininkui galėtų kilti ir tais atvejais, kai, pavyzdžiui, dėl pažeistų elektroninių duomenų apsaugos priemonių gaunama prieiga prie viešųjų elektroninių duomenų. Beje, elektroninių duomenų viešumo faktas, su pačiu elektroninių duomenų turiniu nesusipažinusiam kaltininkui gali būti ir nežinomas. Nagrinėjant šias situacijas kyla svarbiausias klausimas, ar neviešumą reikėtų sieti tik su duomenų turiniu, ar vis dėlto apie jį įmanoma kalbėti ir tada, kai prieiga prie tokių duomenų buvo pasunkinta. Pavyzdžiui, nustatant prieigos prie elektroninių duomenų kontrolę, siekiama apriboti galimybę pašaliniams asmenims sužinoti, kokie duomenys yra laikomi informacinėje sistemoje. Atsižvelgiant į esamą nusikalstamos veikos dalyko formuluotę, minėtaisiais atvejais BK 198 straipsnyje numatytos nusikalstamos veikos inkriminavimas taptų probleminis arba net neįmanomas, nors elektroninių duomenų konfidencialumo pažeidimai tam tikru požiūriu galėtų būti konstatuoti.

Aiškinant neviešų elektroninių duomenų sampratą, pirmiausia tikslinga aptarti patį viešumo suvokimą. Vadovaujantis lingvistiniu aiškinimu, *viešas* apibūdinamas kaip visiems skirtas, visuomenės naudojamas[406] ir bendrinėje kalboje gali būti pakeičiamas sinonimais neuždaras, neslepiamas[407]. Neriboto prieinamumo prie informacijos kriterijus taikomas ir Lietuvos Respublikos visuomenės informavimo įstatymo 2 straipsnio 79 punkte apibūdinant viešąją informaciją, kuri apibrėžiama kaip skirta viešai skleisti (išskyrus šio straipsnio 42 dalyje nurodytą informaciją, taip pat informaciją, kuri pagal Lietuvos Respublikos įstatymus negali būti viešai skleidžiama). Vadinasi, suteikiant viešumui priešingą reikšmę, t. y. kalbant apie neviešus elektroninius

[406] Dabartinės lietuvių kalbos žodynas. 7-asis pataisytas ir papildytas leidimas. Keinys, S. (vyr. red.). Vilnius: Lietuvių kalbos institutas, 2012, p. 928.

[407] Lyberis, A. Sinonimų žodynas. Vilnius: Lietuvių kalbos instituto leidykla, 2002, p. 558.

duomenis, būtina pabrėžti jų viešą neskelbtinumą, slaptumą ir konfidencialumą. Minėtieji aspektai svarbūs ir teismų praktikoje formuluojant neviešų elektroninių duomenų sampratą, kuria remiantis teigiama, kad *nusikaltimo dalykas – elektroniniai duomenys, tačiau ne bet kokie, o tik nevieši – skirti ne visiems, visuotinai nenaudojami*[408], taip pat, kad *nevieši elektroniniai duomenys – tai bet kokia informacija, kurios tvarkymui naudojamos informacinių technologijų priemonės bei su kuria susipažinti turi teisę ribotas asmenų ratas*[409].

Anot J. van der Hoveno, prieigos prie informacijos suvaržymus galima laikyti „informacinio neteisingumo" prevencija. Patį „informacinį neteisingumą" šis autorius aiškino atsižvelgdamas į M. Walzeno išsakytas idėjas apie „prieigos erdvę" ir jį susiejo su nepagarba riboms, kurios nustatomos minėtojoje srityje[410]. Taigi elektroninių duomenų neviešumo pažeidimais galima laikyti neleistiną nustatytų ribų ir duomenų sričių atskyrimo nepaisymą, duomenų perkėlimą už konfidencialumo erdvės ribų. Tokie atvejai galimi ir tada, kai nevieši duomenys yra žinomi tik šių duomenų subjektui, ir esant konfidencialiam ryšiui, t. y. tam tikromis sąlygomis patikėjus duomenis kitiems asmenims arba jiems leidus atlikti veiksmus, kurie suteikia galimybę sužinoti viešai skleisti neskirtus duomenis. Mainais duomenų gavėjas prisiima įsipareigojimus nepadaryti žalos duomenų subjektui ir neperduoti duomenų trečiajam asmeniui be duomenų subjekto sutikimo[411].

Santykiai, kuriems būdingas konfidencialumo aspektas, gali susiklostyti tarp įvairių subjektų, atitinkamai konfidencialumo įpareigojimų neretai atsiranda įvairiose srityse. Bendriausia prasme galima nurodyti du neviešumo pagrindus: *pirma*, objektyvųjį, kai elektroninių duomenų viešumo apribojimai nustatomi įstatymuose ar kituose teisės aktuose ir kt.; *antra*, subjektyvųjį, kai prieigos prie elektroninių duomenų apribojimų atsiranda dėl asmenų tarpusavio susitarimų ir

---

[408] Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendis baudžiamojoje byloje Nr. 1-234-825/2017.

[409] Kauno apygardos teismo 2017 m. rugsėjo 27 d. nuosprendis baudžiamojoje byloje Nr. N1-173-319/2017.

[410] Information technology and Moral Philosofy. Hoven, van den J.; Weckert, J. (eds). Cambridge, *et al.* Cambridge Univesity Press, 2008, p. 314.

[411] Manson, N. C.; O'Neill, O. Rethinking Informed Consent in Bioethics. Cambridge, *et al.* Cambridge University Press, 2007, p. 124.

pan. Vadinasi, sprendžiant klausimą, kas turėtų būti laikoma neviešais elektroniniais duomenimis, svarbu apibrėžti konfidencialumo (neviešumo) erdvės ribas. Literatūroje teigiama, kad kalbant apie konfidencialumą turima mintyje *įvairių rūšių* turinio apsauga, kai komunikuojančios šalys tokį turinį „siekia apsaugoti, yra susitarusios apsaugoti arba yra įpareigotos apsaugoti“[412]. Bendriausia prasme neviešumas tampa svarbus tada, kai duomenys gaunami konfidencialiai nuo kitų asmenų ir negali būti perduoti pašaliniams be duomenų subjekto sutikimo. Kadangi pasitaiko gana įvairių situacijų, tai diskusijos[413] dėl konfidencialumo užtikrinimo poreikio ar konkrečių įpareigojimų plėtojamos duomenis pagal atitinkamus kriterijus susiejant į tam tikras grupes. Pavyzdžiui, tai galėtų būti komercinės, profesinės ar kitų veiklos sričių duomenys, kurių konfidencialumą tikimasi apsaugoti. Toks neviešų elektroninių duomenų grupavimo būdas yra gana natūralus, nes minėtųjų duomenų kategorija yra itin plati, į ją patenka įvairaus pobūdžio duomenys. Neretai šie duomenys gali būti tarpusavyje siejami ne tik dėl paties jų turinio, bet ir dėl tam tikrų konfidencialumo užtikrinimo reikalavimų. Būtent apsaugos lygis – vienas iš išorinius duomenis apibūdinančių požymių ir laikytinas tuo kriterijumi, padedančiu suskirstyti duomenis į dvi grupes: viešuosius ir viešai neskelbiamus (neviešus) duomenis[414]. Dėl vidinio neviešų elektroninių duomenų grupavimo mokslinėje literatūroje atsirado galimybė suformuluoti „informacijos talpyklos modelį“, be to, į duomenis metaforiškai pažvelgti kaip į asmens „kvazifizinius daiktus“, kurie kaip ir tam tikra informacija gali būti slepiami, laikomi arba perkeliami,

---

412 Manson, N. C.; O'Neill, O. Rethinking Informed Consent in Bioethics. Cambridge, *et al.* Cambridge University Press, 2007, p. 126.

413 Panomariovas, A. Viešai neskelbiama informacija (paslaptis) baudžiamajame procese: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: Lietuvos teisės universitetas, 2001; Manson, N. C.; O'Neill, O. Rethinking Informed Consent in Bioethics. Cambridge, *et al.* Cambridge University Press, 2007, p. 126.

414 Tokius išorinius informacijos požymius, pavyzdžiui, apsaugos lygį (informacijai taikomi apsaugos reikalavimai), savalaikiškumą (operatyvumą), nematerialųjį pobūdį ir kt. A. Panomariovas analizavo kalbėdamas apie viešai neskelbiamos informacijos bendrąją sampratą iš baudžiamojo proceso pozicijų (plačiau žr. Panomariovas, A. Viešai neskelbiama informacija (paslaptis) baudžiamajame procese: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: Lietuvos teisės universitetas, 2001, p. 10).

perduodami[415]. Vadinasi, baudžiamosios teisės srityje nustačius disponavimą neviešais elektroninę formą turinčiais duomenimis, ne mažiau svarbu yra tinkamai išspręsti ir jau aptartą daugeto bei baudžiamojo įstatymo normų konkurencijos atribojimo klausimą (atsižvelgiant į tai, kad BK 198 straipsnyje yra numatyta bendroji elektroninių duomenų konfidencialumo pažeidimams taikoma norma).

Neviešų elektroninių duomenų skirstymas į grupes padeda aiškiau apibrėžti ir patį neviešumą, nes į atskirą „talpyklą" patenka tik tam tikros rūšies duomenys, vadinasi, paprasčiau atrasti ir vidinius šiuos duomenis siejančius kriterijus, be to, numatyti įpareigojimus, kurie, atsižvelgiant į „talpykloje" esančių duomenų pobūdį, padėtų nustatyti įvairių su jais atliekamų veiksmų reikalavimus. Neviešumo požymiui, kuriuo remiantis apibūdinamas teisinis elektroninių duomenų aspektas, nustatyti būtina kaskart įvertinti konkrečios rūšies elektroniniams duomenims numatytą disponavimo jais režimą. Taigi būtina atsižvelgti į reikalavimus, kurie gali būti suformuluoti įvairiuose teisės aktuose (įstatymuose, įstatymo įgyvendinamuosiuose teisės aktuose, vidaus dokumentuose bei kt.), ir nustatyti asmenų tarpusavio susitarimus bei kitas neatskleidimo įpareigojimą rodančias aplinkybes. Vadinasi, akivaizdu, kad elektroninių duomenų priskyrimas neviešų elektroninių duomenų kategorijai yra fakto klausimas ir vertintinas kiekvienoje konkrečioje byloje atsižvelgiant į įvairias aplinkybes, pagrindžiančias arba paneigiančias esamus disponavimo duomenimis apribojimus, specialiuosius reikalavimus arba procedūras. Literatūroje išreiškiama nuomonė, kad tokias ribas padeda nurodyti „tikslų detalizavimo ir naudojimo apribojimų"[416] idėja, kuria remiantis užtikrinama, kad duomenys būtų naudojami neperžengiant tos srities ribų, kurioms buvo duotas duomenų subjekto leidimas. Šie apsikeitimo elektroniniais duomenimis ribojimai suteikia galimybę neviešus elektroninius duomenis analizuoti kaip duomenų rūšį, kuriai taikomas tam tikras apsaugos lygis – atitinkami apsaugos reikalavimai.

Teismų praktikoje konstatuojant neviešų elektroninių duomenų konfidencialumo pažeidimus ir motyvuojant BK 198 straipsnyje nu-

---

[415] Manson, N. C.; O'Neill, O. Rethinking Informed Consent in Bioethics. Cambridge, *et al*. Cambridge University Press, 2007, p. 102, 107.

[416] Information technology and Moral Philosofy. Hoven, van den J.; Weckert, J. (eds). Cambridge, *et al*. Cambridge Univesity Press, 2008.

matytos nusikalstamos veikos inkriminavimo pagrįstumą, dažniausiai nurodomi tie teisės aktai, kuriuose nustatytos disponavimo elektroniniais duomenimis ribos (kurių konkrečiu atveju nebuvo laikomasi). Pavyzdžiui, vienoje iš baudžiamųjų bylų konstatuota, kad *R. R. įgijo, laikė, pasisavino, paskleidė neviešus elektroninius duomenis, tai yra <...> pasirašęs pasižadėjimą „dėl informacijos apdorojimo priemonių naudojimo sąlygų laikymosi“, kuriuo patvirtino, kad žino AB „(duomenys neskelbtini)“ informacijos saugos politiką bei ją įgyvendinančius dokumentus, nesilaikė pasižadėjimo ir pažeidė prisiimtus įsipareigojimus <...>*[417]. Teismas šioje byloje detaliai išvardijo duomenų skaitymo, keitimo, įtraukimo, kopijavimo, ištrynimo bei duomenų perdavimo pašaliniams asmenims ribojimus ir nustatęs, kad kaltininkas nesilaikė prisiimtų įsipareigojimų, priėjo prie išvados, kad jis padarė BK 198 straipsnyje numatytą nusikalstamą veiką, t. y. neteisėtai įgijo, laikė, pasisavino ir paskleidė neviešus elektroninius duomenis (internete paskelbė vaizdo įrašą apie bendrovėje įvykusį gaisrą). Teisės aktų įpareigojimų pažeidimai detaliai aptariami ir kituose teismų sprendimuose[418].

Taigi inkriminuojant neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamą veiką vienas iš kriterijų yra siejamas su teisiniu elektroninių duomenų požymiu – jų neviešumu. Šis požymis bendriausia prasme reiškia, kad elektroniniai duomenys yra slapti ir neskirti viešai naudoti. Atsižvelgiant į duomenų pobūdį, nustatomi atitinkami jų konfidencialumo apsaugos ribojimai. Jie suteikia galimybę neviešus elektroninius duomenis analizuoti kaip duomenų rūšį, kuriai taikomas tam tikras apsaugos lygis – atitinkami apsaugos reikalavimai, kurie gali būti suformuluoti įvairiuose teisės aktuose, kilti iš asmenų tarpusavio susitarimų bei kitų aplinkybių, rodančių neatskleidimo įpareigojimus.

---

[417] Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendis baudžiamojoje byloje Nr. 1-188-785/2009.

[418] Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. baudžiamasis įsakymas byloje Nr. 1-617-885/2011.

2.2. Pavojingos veikos

Nusikalstama neteisėto elektroninių duomenų perėmimo ir panaudojimo veika pasireiškia alternatyviomis neteisėto stebėjimo, fiksavimo, perėmimo, įgijimo, laikymo, pasisavinimo, paskleidimo ar kitokio neviešų elektroninių duomenų panaudojimo veikomis. Šios veikos BK 198 straipsnyje yra numatytos kaip alternatyvios, todėl baudžiamajai atsakomybei už neteisėtą elektroninių duomenų perėmimą ir panaudojimą kilti pakanka nustatyti bent vienos iš jų padarymo faktą. Be to, BK 198 straipsnyje aprašytos veikos yra laikomos viena tęstine nusikalstama veika, jei nustatoma, kad jos yra tos pačios atskiros nusikalstamos veikos sudėtinės dalys (epizodai) ir jas sieja bendra kaltininko tyčia. Tęstinė veika pripažįstama kaip pavienė nusikalstama veika, todėl ji neskaidoma dalimis dėl atskirų alternatyvių veikų ir kvalifikuojama taikant atitinkamą minėtojo straipsnio dalį. Kai faktinės bylos aplinkybės rodo, kad kaltininkas galėjo padaryti keletą alternatyvių veikų, itin svarbus tampa draudimas preziumuoti pavojingas veikas – kiekviena iš jų turi atskirą baudžiamąją teisinę reikšmę, todėl turi būti įrodinėjama atskirai, o ne išvedama iš kitų BK 198 straipsnyje nurodytų ir byloje neginčijamai įrodytų veikų. Toks reikalavimas Lietuvos Aukščiausiojo Teismo praktikoje yra susijęs ir su draudimu kelti skirtingus, t. y. mažesnius arba didesnius, reikalavimus įrodinėjant bei pagrindžiant padarytas veikas[419].

Remiantis BK 198 straipsnio dispozicijoje įtvirtintais įvairiais neteisėto duomenų įgijimo ir jų vėlesnio panaudojimo veiksmais, neteisėtam disponavimui neviešais elektroniniais duomenimis suteiktas gana platus turinys. Iš tokios įstatymo leidėjo pozicijos galima spręsti ir apie pasirinktą šios nusikalstamos veikos koncepciją – nustatyti baudžiamąją atsakomybę už elektroninių duomenų konfidencialumo pažeidimus įvairiuose jų tvarkymo proceso etapuose. Pats duomenų

[419] Tokia praktika išplėtota nusikalstamų veikų, susijusių su neteisėtu disponavimu narkotinėmis ar psichotropinėmis, nuodingosiomis ar stipriai veikiančiomis medžiagomis, baudžiamosiose bylose (pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2009 m. spalio 20 d. nutartis baudžiamojoje byloje Nr. 2K-P-218/2009, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. gruodžio 6 d. nutartis baudžiamojoje byloje Nr. 2K-482/2011, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. balandžio 5 d. nutartis baudžiamojoje byloje Nr. 2K-159/2011.

tvarkymas iš esmės „reiškia bet ką, kas gali būti padaryta duomenims arba su duomenimis“[420], todėl šis procesas leidžia kalbėti apie duomenų įgijimą, naudojimą, laikymą, sunaikinimą ir kitas operacijas. Beje, duomenų tvarkymas plačiai apibrėžiamas ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo[421] 2 straipsnio 4 dalyje. Joje duomenų tvarkymu pripažįstamas „bet kuris su asmens duomenimis atliekamas veiksmas: rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas (papildymas ar taisymas), teikimas, paskelbimas, naudojimas, loginės ir (arba) aritmetinės operacijos, paieška, skleidimas, naikinimas ar kitoks veiksmas arba veiksmų rinkinys“. Duomenų saugumas yra svarbus su jais atliekant įvairius veiksmus, todėl ir pats duomenų tvarkymo terminas vartojamas pačia plačiausia prasme. Manytina, kad būtent dėl to įstatymų leidėjas BK 198 straipsnio dispozicijoje numatė įvairias pavojingas veikas, rodančias duomenų konfidencialumo pažeidimus kuriame nors iš duomenų tvarkymo etapų. Šiuo požiūriu svarbu pabrėžti, kad Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje ir Direktyvos 2013/40/ES 6 straipsnyje numatyta tik neteisėtos perimties nusikalstama veika. Kitų alternatyvų šiuose teisės aktuose nenumatyta, todėl siekiant jas tinkamai interpretuoti būtina nustatyti, kaip tokios veikos yra suvokiamos aiškinant kitų BK esančių nusikalstamų veikų sudėtis. Tokia analizė gali padėti tinkamai atskleisti neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymių turinį, susiformavusį tradicinį požiūrį pritaikant ir „skaitmeniniam kontekstui“.

Aptariant minėtąsias BK 198 straipsnyje numatytas alternatyvias veikas matyti, kad daugelis iš jų pagal savo formuluotę yra panašios į tas, kurios įtvirtintos tradicinėmis laikomų nusikalstamų veikų sudėtyse. Pavyzdžiui, įgijimo, laikymo, platinimo, pasisavinimo ar kitokį neteisėtą disponavimą rodančias pavojingas veikas galima įžvelgti nusikalstamų veikų nuosavybei, turtinėms teisėms ir turtiniams interesams (pavyzdžiui, BK 182, 183, 189 straipsniai), finansų sistemai (pavyzdžiui, 214, 215 straipsniai), nusikalstamų veikų, susijusių su disponavimu ginklais, šaudmenimis, sprogmenimis, sprogstamo-

[420] Webster, M. Data protection in the financial services industry. Aldershot; Burlington (Vt.): Gower, 2006, p. 13.

[421] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*, 1996, Nr. 63-1479.

siomis medžiagomis (pavyzdžiui, 253 straipsnis), disponavimo narkotinėmis ar psichotropinėmis medžiagomis (pavyzdžiui, 259, 260, 263 straipsniai) ir daugelio kitų nusikalstamų veikų sudėtyse. Be to, įvairių BK straipsnių dispozicijose panašiai aprašytos ir tos veikos, kuriomis daromas neteisėtas poveikis nusikalstamos veikos dalykui, galinčiam ir neturėti materialiosios išraiškos (pavyzdžiui, 124, 166, 170, 296, taip pat minėtieji 214, 215 straipsniai). Kadangi pastarosios nusikalstamos veikos dėl savo pobūdžio negalėjo būti taikomos visų elektroninių duomenų konfidencialumo pažeidimo atvejais, tai BK 198 straipsnyje buvo numatyta bendroji neteisėto elektroninių duomenų perėmimo ir panaudojimo veika. Toks požiūris į elektroninės erdvės saugumą, kaip ir aptartosios neteisėtos prieigos prie informacinės sistemos atveju, rodo tradicinių doktrinų raidą. Kaip teigiama literatūroje, „probleminiai prieigos prie informacijos, duomenų ir kompiuterio programų klausimai tampa probleminiais prieigos prie vietos, erdvės ir daikto <...> klausimais“[422]. Tokia išvada suteikia galimybę analizuoti dviejų – *interneto kaip vietos* (angl. *Internet-as-place)* ir *informacijos kaip daikto* (angl. *Information-as-thing)* – metaforų derinį. Neteisėtas prisijungimas prie informacinės sistemos rodo įsibrovimo doktrinos plėtrą, o neteisėtas disponavimas elektroniniais duomenimis tam tikra apimtimi yra susijęs su pagrobimo (neteisėto įgijimo) doktrinos plėtra ir jos taikymu ne fizinėje, bet elektroninėje erdvėje. Reikėtų pabrėžti, kad šie doktrininiai pokyčiai nėra nauji – kriminalizuojant įvairius neteisėtus veiksmus, atliekamus su materialiosios išraiškos neturinčiais nusikalstamos veikos dalykais, panašių problemų kilo ir įsigaliojus 2000 m. BK. Pavyzdžiui, numačius baudžiamąją atsakomybę už neteisėtą naudojimąsi energija ir ryšių paslaugomis (BK 179 straipsnis).

BK 198 straipsnyje numatytai nusikalstamai veikai gali būti priskiriama įvairių alternatyvių veikų, todėl dabartinis straipsnio pavadinimas, turintis nurodyti jame esančios nusikalstamos veikos esmę, yra diskutuotinas. Kadangi ši nusikalstama veika, įvardijama kaip *neteisėtas elektroninių duomenų perėmimas ir panaudojimas*, yra apibūdinama pernelyg siaurai, tikslesniu pavadinimu galima būtų laikyti *neteisėtą disponavimą neviešais elektroniniais duomenimis*. Tiesa, teisės aktuose

[422] Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2): 434.

pasitaiko ir kitokių variantų, pavyzdžiui, Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. spalio 21 d. įsakymo Nr. 1V-1013 „Dėl viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų saugumo ir vientisumo užtikrinimo taisyklių patvirtinimo“ 3 punkte apibrėžiama manipuliacija elektroniniais duomenimis, kuri apibūdinama kaip elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų naudojimas. Atsižvelgiant į BK straipsnių, kuriuose aprašytos įvairios ir, be kita ko, neteisėtą poveikį materialiosios išraiškos galinčiam neturėti dalykui darančios veikos, pavadinimus, galima teigti, kad tikslesnis būtų ne manipuliavimo, o disponavimo terminas (pavyzdžiui, neteisėtas disponavimas informacija, kuri yra valstybės paslaptis (BK 124 straipsnis). Juo labiau kad BK manipuliavimo terminas yra vartojamas šiek tiek kitame kontekste ir siejamas su tikrovės neatitinkančios ar neišsamios informacijos skleidimu (BK 218 straipsnis).

2.2.1. Perėmimas

Perėmimo kaip pavojingos veikos ištakos išimtinai siejamos su Konvencijos dėl elektroninių nusikaltimų 3 straipsnio ir Direktyvos 2013/40/ES 6 straipsnio, kuriuose įtvirtinta neteisėto duomenų perėmimo (neteisėtos perimties) veika, nuostatomis. Dėl tokios sąsajos perėmimo veiką galima analizuoti tik iš *informacinėje sistemoje perduodamų*, bet ne minėtųjų *nejudamų* elektroninių duomenų neteisėto gavimo pozicijų. Nors toks sukonkretinimas padeda nustatyti perėmimo ir kitų neteisėto elektroninių duomenų gavimo veikų atskyrimo kriterijų, būtina apibrėžti ir pavojingos veikos pripažinimo perėmimu sąlygas. Teisingiau apsispręsti: *pirma*, kada elektroniniai duomenys yra perduodami informacinėje sistemoje; *antra*, kokių elektroninių duomenų neteisėtas perėmimas, atsižvelgiant į šių duomenų perdavimo informacinės sistemos ypatumus, yra kriminalizuotas BK 198 straipsnyje.

Nagrinėjant pirmąjį klausimą pabrėžtina, kad Konvencijos dėl elektroninių nusikaltimų 3 straipsnyje apibūdinamas duomenų, perduodamų iš kompiuterinės sistemos ir jos viduje, perėmimas. Šios Konvencijos aiškinamojoje ataskaitoje tokie atvejai yra detalizuojami išaiškinant, kad komunikavimas perduodant duomenis gali vykti ir pavienėje kompiuterinėje sistemoje (pavyzdžiui, duomenims paten-

kant iš CPĮ į ekraną arba spausdintuvą), ir tarp keleto vienam asmeniui priklausančių sistemų, kelių tarpusavyje sąveikaujančių kompiuterių arba asmeniui komunikuojant su kompiuteriu (naudojantis klaviatūra). Be to, nurodoma, jog baudžiamajai atsakomybei kilti gali prireikti papildomo elemento, t. y. komunikavimas turėtų vykti tarp dviejų sujungtų, bet per atstumą veikiančių kompiuterinių sistemų (55 punktas). Taigi didžiausia problema kaltininkui inkriminuojant duomenų perėmimą kyla sprendžiant, kada duomenys gali būti laikomi perduodamais informacinėje sistemoje, ir atitinkamai, kada galima kalbėti apie tokių duomenų perėmimą. Pavojingi perėmimo veiksmai yra tiesiogiai susiję su neteisėtu duomenų gavimu juos perduodant, bet iš Konvencijos aiškinamosios ataskaitos matyti, kad toks perdavimas galimas ir iš kompiuterinės sistemos į išorę, ir jos viduje (pavyzdžiui, asmeniui komunikuojant su kompiuteriu). Vadinasi, reikėtų nuspręsti, ar BK 198 straipsnio dispozicijoje minima perėmimo veika galima laikyti tik tuos veiksmus, kuriais neteisėtai gauti elektroninių ryšių tinklais[423] siųsti duomenys, ar ir tuos, kuriais gauti tik kompiuterio viduje perduodami duomenys.

Vidiniai duomenų perdavimo procesai, kai duomenys lieka kompiuteryje, yra neišvengiamai susiję su jo atliekamomis funkcijomis – vartotojas per įvesties įrenginius nurodydamas kompiuteriui įvairias komandas atlieka savo pageidaujamus veiksmus. Tokiais atvejais vartotojo siekiamų apdoroti duomenų perėmimo galimybė nepriklauso nuo to, ar mintyje turimas pavienis kompiuteris, ar elektroninių ryšių tinklais sujungtas su kitomis informacinėmis sistemomis. Bene klasikiniu pavyzdžiu, kaip yra atliekami tokie neteisėti perėmimo veiksmai, galėtų būti laikomas kenkimo programinės įrangos (pavyzdžiui, *Keylogger)* taikymas, kai ši, be kitų atliekamų funkcijų, gali fiksuoti ir kiekvieno vartotojo kompiuterio klaviatūra įvestą informaciją.

---

[423] Pagal Elektroninių ryšių įstatymo 3 straipsnio 16 punktą, elektroninių ryšių tinklas – tai „perdavimo sistemos ir (arba) komutavimo bei maršruto parinkimo įranga, kitos priemonės, įskaitant pasyviuosius tinklo elementus, leidžiančios perduoti signalus laidinėmis, radijo, optinėmis ar kitomis elektromagnetinėmis priemonėmis, įskaitant palydovinius tinklus, fiksuotuosius (kanalų ir paketų komutavimo, įskaitant internetą) ir judriuosius antžeminius tinklus, elektros perdavimo kabelines sistemas (kiek jos naudojamos signalams perduoti), tinklus, naudojamus radijo ir (arba) televizijos programoms transliuoti (retransliuoti), ir kabelinės televizijos bei mikrobangų daugiakanalės televizijos tinklus neatsižvelgiant į perduodamos informacijos pobūdį."

Analizuojant kitą – išorinį elektroninių duomenų perdavimo būdą, kai duomenys yra siunčiami elektroninių ryšių tinklais, būtina nustatyti, kada jie yra tokios būsenos. Literatūroje pabrėžiama, kad teisės normų, susijusių su duomenų perėmimu, raida pirmiausia vyko realiuoju laiku perduodamų duomenų perėmimo aplinkybėmis[424]. Kintant situacijai, kai vis dažniau naudojamasi balso pašto (VoIP) paslaugomis[425], taip pat plėtojantis elektroninio pašto, trumpųjų žinučių ir kitų elektroninių duomenų perdavimo paslaugoms, aktualūs tapo įvairūs konfidencialumo užtikrinimo būdai vertinant paslaugų teikėjo laikomus duomenis, kai šie, *pirma*, jau yra pristatyti ir, *antra*, dar nėra perduoti, bet laukia pristatymo. Tokiais atvejais bandoma nustatyti *saugojimo po duomenų perdavimo* ir *duomenų tarpinio saugojimo* skirtumus. Pirmuoju atveju galima kalbėti apie „saugomų komunikacijų konfidencialumą“[426], o antruoju reikėtų įvertinti, ar duomenys yra laikomi saugomais (esančiais) informacinėje sistemoje, ar vis dėlto yra perduodami elektroninių ryšių tinklais. Tokia problema kyla dėl paties duomenų perdavimo tinklais būdo. Kadangi šiuo atveju susiduriama su komunikacijos technologijomis ir įvairiais jų funkcionavimo aspektais, reikėtų prisiminti galimas jų veikimo vertinimo pozicijas – *išorinę* ir *vidinę perspektyvas*. Pavyzdžiui, žiūrint iš *vidinės perspektyvos,* internetas vartotojui sukelia vienos bendros komunikavimo sistemos iliuziją, bet nesuteikia informacijos, kaip veikia įrenginių visuma ar pavieniai įrenginiai atlikdami įvairias funkcijas, kai elektroninių ryšių tinklais perduodami duomenys. Dėl to į duomenų perdavimo procesus aktualu pažvelgti ir iš *išorinės perspektyvos*. Daugelis informacinių sistemų yra sujungtos, kad galėtų tarpusavyje komunikuoti – keistis elektroniniais duomenimis ir dalytis per atstumą esančiais ištekliais. Į tinklą sujungta sistema – tai „kompleksas informacijos šaltinių ir komunikavimo mazgų, sujungtų tinklu“[427]. Kiekvienas iš šių mazgų atlieka atskirą galutinę funkciją arba yra skirtas konkrečiam tikslui

[424] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 164.

[425] Plačiau žr. Kašėta, S.; Adomkus, T. Telefonijos informacijos ir VoIP sauga. Kaunas: Vitae Litera, 2008.

[426] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 164.

[427] El Gamal, A. A.; Kim, Y. H. Network Information Theory. Cambridge: Cambridge University Press, 2011, p. 1.

pasiekti. Tam, kad tinklo įrenginiai galėtų keistis duomenimis, prieš tai būtina duomenis sutvarkyti tokiu būdu, kuris leistų įrenginiui sėkmingai juos nukreipti į jų paskyrimo vietą, o kitam – juos priimti. Vadinasi, „perdavimas yra kompleksinis procesas ir priklauso nuo daugelio skirtingų operacijų“[428]. Pirmiausia duomenys skirstomi į mažesnius vienetus (paketus), prie kiekvieno tokio fragmento pridedama informacija (antraštė), kuri leidžia juos perduoti įvairiais tinklais iki numatytos vietos. Toks duomenų „pakavimo“ procesas internete vaizdžiai pateikiamas išaiškinant, kaip keičiamasi duomenimis taikant TCP (angl. *Transmission Control Protocol)* ir IP (angl. *Internet Protokol)* protokolą. TCP protokolas „suskaido siunčiamą informaciją porcijomis (paketais), sudeda juos į elektroninius vokus, ant jų užrašo gavėjo bei siuntėjo adresus“[429]. Taikant IP protokolą nustatoma, kokiu tinkamiausiu būdu suformuotas paketas turėtų būti siunčiamas internetu. Kai jis siunčiamas per interneto mazginius punktus, kiekviename iš jų nuskaitomas gavėjo adresas ir suformuotas paketas siunčiamas toliau. Vadinasi, „kiekvienas interneto elektroninis laiškas gali būti padalytas į kelis duomenų paketus, kurie gali keliauti pas adresatą visiškai skirtingais keliais“[430]. Vėliau TCP protokolas padeda surinkti tokius paketus ir vėl atkurti pradinę informaciją.

Panašus duomenų perdavimo principas būdingas įvairioms interneto paslaugoms – „kiekvienai paslaugai internete taikomas savas protokolas perduodant duomenų paketus iš vienos vietos į kitą“[431]. Remiantis informacijos paketų perdavimo būdu, bendriausia prasme galima kalbėti apie pranešimų siuntimo procesą kaip apie „saugomą ir persiunčiamą“[432] pristatymą. Apie saugojimą duomenų perdavimo

---

[428] Blundell, B. G. Computer Systems and Networks. London: Thomson: Middesex University Press, 2007, p. 244.

[429] Štitilis, D. Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: LTU, 2002, p. 13.

[430] *Ibidem*.

[431] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 165.

[432] Toks pranešimų perdavimo proceso apibūdinimas buvo suformuluotas byloje *United States v. Bradford C. Councilman*, no. 03-1383, United States Court of Appeals, 1 st Circuit, 2005 [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: <*http://media.ca1.uscourts.gov/cgi-bin/getopn.pl?OPINION=03-1383EB.01A*>.

procese užsimenama dėl to, kad pasitaiko atvejų, kai suformuoti paketai dėl įvairių priežasčių negali būti iš karto nusiųsti iš vieno tinklo taško į kitą, todėl jie yra tam tikram laikui sulaikomi tinklo mazguose ir vėlinami pristatyti (laikinai saugomi, kol pasieks galutinę paskyrimo vietą). Tai daroma dėl įvairių priežasčių: paketų apdorojimo tinklo mazge laiko, kad šis galėtų atlikti savo tiesiogines funkcijas (pavyzdžiui, parinkti maršrutą), paketų aptarnavimo eilės, kai šie laukia, kol bus išsiųsti anksčiau į tinklo mazgą patekę paketai, ir kt.[433] Vadinasi, galima teigti, kad duomenys dažnai, o galbūt ir nuolat, to paties siuntimo metu yra ir siunčiami, ir tam tikra prasme saugomi „saugykloje“ (net jei saugojimas trunka tik mikrosekundės dalį). Būtent dėl to ir kyla sunkumų nustatant, kuriais atvejais duomenys yra perduodami, o kuriais galėtų būti laikomi *nejudamais* (saugomais ar laikomais informacinėje sistemoje).

Apibrėždamas duomenų perdavimo informacinėje sistemoje pradžios ir pabaigos momentus, A. S. Blunnas atkreipė dėmesį, kad mokslinėje literatūroje reiškiamos trys tarpusavyje konkuruojančios nuomonės, t. y. pranešimas laikomas gautu, jei: *pirma*, jį perskaitė numatytas gavėjas; *antra*, pranešimas pasiekė kurią nors tarpinę grandį; *trečia*, jis yra saugomas ta prasme, kad yra *nejudamas*, t. y. nėra automatiškai persiunčiamas ir pasiekė tą adresą, iš kurio gali būti tiesiogiai prieinamas numatyto gavėjo[434]. Akivaizdu, kad numatytam gavėjui pristatomi duomenų fragmentai (paketai) bus nuolat sulaikomi įvairiose tarpinėse parinkto maršruto grandyse. Toks nuolatinis trumpalaikis duomenų saugojimas yra svarbus perdavimo proceso etapas, todėl bandymai visus šiuos užlaikymus atskirti nuo persiuntimų iš tikrųjų netenka prasmės. Į perdavimą turėtų būti žiūrima kaip į vientisą procesą, kuriam būdingas neišvengiamas trumpalaikis duomenų saugojimas ir jų persiuntimas siekiant juos pateikti numatytam adresatui. Vadinasi, šiuo požiūriu pavojingą veiką vertinant kaip perėmimą nesvarbu, kad siunčiami duomenys tam tikru momentu galėjo būti saugomi elektroniniu

---

[433] Plačiau žr. Plėštys, R., *et al*. Tinklų sauga. Kaunas: Vitae Litera, 2008, p. 37–41.

[434] Blunn, A. S. Report of the Review of the Regulation of Access to Communications. Australija, 2005, p. 28–29 [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: *<http://www.ag.gov.au/Publications/Documents/Blunn%20report%20of%20the%20review%20of%20the%20regulation%20of%20access%20to%20communications%20-%20August%202005/xBlunn%20Report%2013%20Sept.pdf>*.

būdu, jei tai yra duomenų perdavimo proceso sudedamoji dalis. Tokiu atveju duomenų perdavimo pabaigos momento nereikėtų sieti nei su gavėjo veiksmais peržiūrint duomenis (pranešimą), nei su tarpiniais saugojimais: pirmuoju atveju perdavimo pabaigos momentas kaskart gali skirtis, tai priklauso nuo to, kada bus peržiūrėti duomenys, nors patys duomenys jau nėra perdavimo procese (pavyzdžiui, yra saugomi serveryje); antruoju atveju vientisas perdavimo procesas yra nepagrįstai skirstomas dalimis. Atsižvelgiant į tai, sėkmingu perdavimu turėtų būti laikomas momentas, kai duomenys pasiekia tą adresą, iš kurio gali būti tiesiogiai prieinami numatyto gavėjo.

Šiuo požiūriu analizuojant BK 198 straipsnio dispozicijoje numatytą neteisėto perėmimo veiką matyti, kad išsamesnė diskusija, kaip reikėtų suvokti duomenų perėmimą, Lietuvos baudžiamosios teisės doktrinoje kol kas nevyksta. Tik keletas autorių yra pareiškę savo nuomonę kai kuriais jos vertinimo aspektais, pavyzdžiui, kad „elektroninių duomenų perėmimu laikomas elektroninių duomenų paėmimas ne iš konkretaus kompiuterio ar išorinės atminties įrenginių, bet elektroninių ryšių tinklais ar tarp kelių kompiuterių ar jo komponentų siunčiamų ir perduodamų duomenų užfiksavimas“[435]. Aiškinant neteisėto elektroninių duomenų perėmimo veiką, tokia pozicija yra bandoma remtis ir teismų praktikoje[436]. Nors, kaip matyti, vadovaujantis tokiu požiūriu nenumatoma galimybė neteisėtu perėmimu laikyti veiksmų, kuriais gaunami tik kompiuterio viduje perduodami elektroniniai duomenys. Atsižvelgiant į abstraktų neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos aprašymą, toks variantas vis dėlto neturėtų būti atmetamas. BK 198 straipsnio dispozicijoje nepateikiama nuorodų į elektroninio ryšio tinklus, būtiną informacinės sistemos sąsają su kitomis sistemomis, reikalavimus nustatyti kitą nei siuntėjas duomenų gavėją ar į kitas šios nusikalstamos veikos apibrėžtį siaurinančias aplinkybes. Gana plati nusikalstamos veikos apimtis bent jau baudžiamojo įstatymo lygiu nesuteikia pagrindo elektroninių duomenų perėmimą analizuoti tik iš išorinio duomenų perdavimo pozicijų (duomenis perduodant

[435] Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 432.

[436] Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendis baudžiamojoje byloje Nr. 1-234-825/2017.

elektroninių ryšių tinklais arba į išorinius informacinės sistemos įrenginius). Dėl to svarstytina, ar elektroninių duomenų perėmimu negalėtų būti laikomi ir tokie pavojingi kaltininko veiksmai, kai neteisėtai gaunami pačiame kompiuteryje perduodami duomenys. Beje, apie tokią neteisėtų veiksmų vertinimo galimybę užsimenama ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje, kurioje, kaip minėta, yra pabrėžiama ir asmens sąveika su paviene kompiuterine sistema, taip pat nurodomas vidinis duomenų perdavimas (55 punktas).

Iš baudžiamosios teisės pozicijų vertinant išimtinai tik išorinius duomenų perdavimo procesus ir sprendžiant perėmimo inkriminavimo kaltininkui galimybes, būtina atskirti neteisėtą elektroninių ryšių tinklais *jau perduotų* ir *dar tik siunčiamų duomenų* gavimą. Pirmuoju atveju duomenų perdavimo procesas jau yra pasibaigęs, nes jie jau pasiekė numatytą gavėją, taigi apie tokius duomenis jau galima kalbėti kaip apie saugomus (laikomus) informacinėje sistemoje, t. y. *nejudamus* duomenis. Tokiais atvejais kvalifikuojant kaltininko veiką tiksliau yra taikyti ne duomenų perėmimo požymį, o kitas alternatyvias neteisėtą duomenų gavimą apibūdinančias veikas (pavyzdžiui, neteisėtą elektroninių duomenų įgijimą). Vadinasi, inkriminuoti elektroninių duomenų perdavimą galima tik antruoju atveju, kai duomenys neteisėtai gaunami jų perdavimo metu, t. y. tol, kol jie dar nėra pristatyti numatytam gavėjui. Atsižvelgiant į jau pateiktus argumentus, tokios išvados neturėtų paneigti tai, kad duomenų perdavimo metu kaip šio proceso dalis yra neišvengiami tarpiniai duomenų saugojimai.

Antrasis probleminis aspektas, analizuojant pavojingos veikos pripažinimo perėmimu sąlygas, yra tiesiogiai susijęs su nusikalstamos veikos dalyku, t. y. kokių elektroninių duomenų neteisėtas perėmimas, atsižvelgiant į jų perdavimo informacinėje sistemoje ypatumus, yra kriminalizuotas BK 198 straipsnyje. Kaip minėta, elektroniniams duomenims identifikuoti gali būti taikomas *tinkamumo apdoroti informacinėje sistemoje* arba *duomenų buvimo vietos* kriterijus, bet juo remiantis duomenys tik priskiriami elektroninių duomenų rūšiai. Vadinasi, aptariant elektroninių ryšių tinklais siunčiamus duomenis, reikėtų atkreipti dėmesį ir į jų struktūrą – šiems duomenims priskiriami ne tik turinio (angl. *content data)*, bet ir srauto duomenys (angl.

traffic data)[437]. Bendrasis tokio atskyrimo tikslas yra „nustatyti skirtingus teisinius perdavimo (srauto duomenų) ir turinio (turinio duomenų) režimus“[438].

Konvencijos dėl elektroninių nusikaltimų 1 straipsnio d punkte srauto duomenys apibūdinami kaip perduodami kompiuterine sistema ir yra „suformuoti kompiuterinės sistemos, kuri sudaro ryšio grandinės dalį, ir rodantys perduotos informacijos kilmę, paskirtį, perdavimo kelią, laiką, datą, dydį, trukmę arba pagrindinės paslaugos rūšį“. Konvencijos aiškinamojoje ataskaitoje šie duomenys yra priskiriami kompiuterinių duomenų, kuriems taikomas specifinis teisinis režimas, kategorijai. Minėtieji duomenys yra sukurti kompiuterio komunikacijos grandinėje siekiant nustatytu maršrutu nusiųsti informaciją iš kilmės į paskyrimo vietą (28 punktas). Panašiai srauto duomenys apibūdinami ir Lietuvos Respublikos elektroninių ryšių įstatymo 3 straipsnio 57 punkte – tai duomenys, kurie „tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai“. Pranešimo turinio ir informacijos, kuri yra būtina jam pasiekti numatytą vietą, atskyrimas gana išsamiai atskleidžiamas mokslinėje literatūroje. Pateikiant tradicinio laiško pavyzdį, srauto duomenys yra prilyginami siuntėjo ir gavėjo adresui, pašto ženklui ir antspaudui, kurie paprasčiausiai leidžia laiškui pasiekti adresatą arba grįžti atgal pas siuntėją, o voke siunčiamas laiškas yra laikomas pranešimo turiniu, todėl gali būti lyginamas su turinio duomenimis[439]. Kaip matyti, apie tokį elektroninių duomenų atskyrimą būtina kalbėti dėl aptartojo duomenų perdavimo elektroninių ryšių tinklais principo – duomenis suskirsčius į mažesnius fragmentus (paketus), prie kiekvieno iš jų pridedama informacija (antraštė), kuri leidžia juos perduoti įvairiais tinklais iki numatytos vietos. Remiantis BK 198 straipsniu, elektroninių duomenų konfidencialumo pažeidimai konstatuotini nustačius ir turinio duomenų, ir su jais susijusių tinklo

[437] Šiuo požiūriu reikėtų atkreipti dėmesį į turinio ir srauto duomenų atribojimo problemą, nes, kaip matyti literatūroje, kai kuriais atvejais neįmanoma pasiekti aiškaus tokių duomenų atskyrimo (plačiau žr. Digital anonymity and the law: tensions and dimensions, edited by C. Nicoll; J. E. J. Prins; M. J. M. van Dellen. The Hague: T.M.C. Asser Press, 2003, p. 164–165).

[438] *Ibid*., p. 163.

[439] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 152.

srauto duomenų neteisėtą gavimą. Tokią išvadą galima daryti dėl gana bendrai, t. y. technologijų požiūriu neutraliai, įvardyto šios nusikalstamos veikos dalyko – elektroninių duomenų. Nors, kuri iš straipsnio dispozicijoje minimų pavojingų veikų – perėmimas ar fiksavimas – yra tinkamesnė siekiant neteisėtai gauti srauto duomenis, įmanoma nuspręsti tik išsiaiškinus perėmimo ir fiksavimo veikų tarpusavio ryšį.

2.2.2. Stebėjimas ir fiksavimas

Bene daugiausia interpretavimo sunkumų, analizuojant BK 198 straipsnio dispozicijoje numatytas pavojingas veikas, kyla dėl stebėjimo ir fiksavimo veikų. Atskleidžiant minėtųjų veikų turinį, įvairūs probleminiai klausimai yra neišvengiami dėl to, kad šios veikos nėra dažnai minimos BK, dėl jų nekyla diskusijų baudžiamosios teisės doktrinoje ar teismų praktikoje, nesuformuluotos galimos šių alternatyvų aiškinimo kryptys. Be to, pati neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtis, kokia yra įtvirtinta BK 198 straipsnyje, rodo neapibrėžtą ir neaiškumų keliantį stebėjimo bei fiksavimo veikų turinį. Interpretavimo įvairovę lemia tai, kad minėtosios pavojingos veikos tarsi gali būti analizuojamos atskirai iš *informacinėje sistemoje laikomų* ir *joje perduodamų elektroninių duomenų* neteisėto gavimo pozicijų. Tokia padėtis susiklosto dėl to, kad BK 198 straipsnio dispozicijoje elektroniniai duomenys kaip nusikalstamos veikos dalykas nėra sukonkretinami iki minėtųjų rūšių, o pati dispozicija nesuteikia galimybių stebėjimą ir fiksavimą susieti tik su *informacinėje sistemoje perduodamais* duomenimis. Klausimų dėl tokios sąsajos natūraliai gali kilti analizuojant, pavyzdžiui, BK 166 straipsnį, kuriame minimas ne sistemoje laikomų, o išimtinai elektroninių ryšių tinklais siunčiamų pranešimų stebėjimas, fiksavimas ir perėmimas. Be to, tokį požiūrį galima pagrįsti ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje pateikto perėmimo, taikant technines priemones, interpretavimu jį aiškinant per klausymąsi, sekimą ir kontroliavimą (53 punktas).

Aiškinantis *informacinėje sistemoje perduodamų duomenų* stebėjimo ir fiksavimo interpretavimo problemas, būtina aptarti jų atskyrimo nuo perėmimo veikos kriterijus. Kaip minėta, pavojingi perėmimo veiksmai yra tiesiogiai susiję su neteisėtu duomenų gavimu *juos perduodant*. Sunkumų atribojant perėmimo, stebėjimo ir fiksavimo veikas kyla dėl to, kad perėmimo procesas dažniausiai yra sie-

jamas ir su elektroninių duomenų stebėjimu bei fiksavimu. Aiškiau šį veikų ryšį įmanoma pavaizduoti pirmiausia išsiaiškinus, kaip suvokiamos pačios stebėjimo ir fiksavimo veikos. Anot BK 198 straipsnį komentavusių autorių, stebėjimas, neatskiriant *nejudamų* ir *perduodamų* duomenų, apibūdinamas „kaip veiksmas, dėl kurio asmuo įgyja galimybę elektroninius duomenis matyti ar kitaip atpažinti, tai yra asmuo savo veiksmų pasekmėje gali matydamas tuos duomenis juos arba analizuoti, arba ir neanalizuodamas suvokti, kad tai elektroniniai duomenys“[440]. Vadinasi, neteisėtas stebėjimas yra siejamas su elektroninių duomenų fiksavimu kaltininko mintyse, kai šie duomenys išlieka jo atmintyje ir nėra atkuriami nei elektronine, nei materialiąja forma (neužrašomi, nekopijuojami ar kt.).

Informacinėje sistemoje perduodamų elektroninių duomenų fiksavimą galima palyginti su jų „sugavimu“ ir atvaizdavimu. Toks duomenų „gaudymas“ tarsi leidžia sustabdyti jų srautą ir padaryti duomenis prieinamus kaltininko stebėjimui, analizei ir kt. Šis aiškinimas atitiktų ir bendrąją fiksavimo sampratą. Fiksuoti (lot. *fixus* – tvirtas, stiprus, nesuardomas) reiškia užrašyti, registruoti, žymėti, padaryti nejudamą, įtvirtinti[441], arba toks veiksmas gali būti apibūdinamas kaip „komanda veiksmui sustabdyti, „įšaldyti“[442]. Kadangi srautui stebėti dažniausiai būtinos specialios priemonės (programinė įranga, pavyzdžiui, įvairios tinklo srauto perėmimo programos, techninės priemonės), tai perduodamų elektroninių duomenų fiksavimas yra kaltininko taikomų priemonių veiklos rezultatas. Atsižvelgiant į šių priemonių ypatybes, jomis galima stebėti, analizuoti duomenis, interpretuoti duomenų paketus ir perrinkti jų srautą į originalius duomenis[443]. Akivaizdu, kad tokiais ir panašiais atvejais, norint stebėti (matyti ar atpažinti) siunčiamus konfidencialius elektroninius duomenis, būtina juos fiksuoti – programinė įranga, „sugavusi“ perduodamus duomenis, juos atvaizduoja programos lange kaltininkui peržiūrėti. Taigi, *pirma*, stebėjimas dažniausiai neatsiejamas nuo ankstesniojo ar ste-

[440] Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 432.

[441] Tarptautinių žodžių žodynas. 4-asis pataisytas ir papildytas leidimas. Vaitkevičiūtė, V. (red.). Vilnius: Žodynas, 2007, p. 336.

[442] Dagienė, V., *et al*. Enciklopedinis kompiuterijos žodynas. Vilnius: TEV, 2008.

[443] Česnys, A.; Juknius, J. Saugumo patikros ir etiško įsilaužimo technologijos. Kaunas: Technologija, 2011, p. 71.

bėjimo metu atliekamo perduodamų duomenų fiksavimo; *antra*, pats neteisėtas programinės įrangos veikimas tinkle (fiksuojant duomenis) gali būti prilyginamas tinklo srauto stebėjimui; *trečia*, fiksavimas bendriausia prasme irgi galėtų būti laikomas elektroninių duomenų perėmimu. Pavyzdžiui, literatūroje elektroninių duomenų perėmimas apibrėžiamas kaip elektroninių ryšių tinklais ar tarp kelių kompiuterių ar jo komponentų siunčiamų ir perduodamų duomenų užfiksavimas[444]. Be to, kaip teigiama Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte, perėmimas yra suvokiamas pačia bendriausia prasme, kaip klausymasis, sekimas ar kontroliavimas.

Taigi dėl tokio stebėjimo, fiksavimo ir perėmimo veikų išskaidymo į atskiras BK 198 straipsnyje numatytas alternatyvas kyla nemažai jų atribojimo problemų, nes pagal savo prasmę artimoms veikoms įvardyti pasirinkti skirtingi terminai. Beje, galimų užuominų, kokiais kriterijais remiantis galima būtų šias veikas vieną nuo kitos atriboti, kol kas nepateikiama nei baudžiamosios teisės doktrinoje, nei teismų praktikoje. Vadinasi, bandant minėtiesiems požymiams suteikti specifinę reikšmę, atitinkamai ir atskirą turinį, svarstytina:

pirma, ar atskiriant fiksavimo ir perėmimo veikas negalėtų būti atskiriamas srauto ir turinio duomenų gavimas. Tokiu atveju fiksavimas sietinas su srauto duomenų nuskaitymu, t. y. tų duomenų (antraščių), kuriais buvo pažymėti duomenų paketai ir kurie atpažįstami tinklo įrenginiuose, fiksavimu. O duomenų perėmimas reikštų turinio duomenų gavimą, t. y. pačios siunčiamos informacijos, kuri siuntimo metu buvo suskaidyta į tam tikro dydžio duomenų paketus. Nors ir netiesiogiai, bet tokio spėjimo pagrindu galėtų tapti BK 166 straipsnis. Jame elektroninių ryšių tinklais siunčiamų pranešimų gavimas aprašytas kaip jų perėmimas, fiksavimas ar stebėjimas. Pačiame straipsnyje su pokalbių elektroninių ryšių tinklais privatumo pažeidimais yra siejamos fiksavimo, klausymo ar stebėjimo veikos. Kaip matyti, išlikus toms pačioms fiksavimo ir stebėjimo veikoms, antruoju atveju vietoj perėmimo yra numatyta klausymo veika, kuri iš esmės parodo pokalbio turinio sužinojimą. Galima spėti, kad neteisėtam asmens pokalbių turinio girdėjimui vietoj perėmimo buvo pasirinkta tinkamesnė – būtent klausymo – veika. Vadinasi, galima

[444] Abramavičius, A., *et al.* Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 432.

daryti prielaidą, kad neteisėtas pranešimų perėmimas BK 166 straipsnyje yra siejamas būtent su jų turinio gavimu. Taikant analogišką aiškinimą, elektroninių duomenų turinio sužinojimą BK 198 straipsnyje galėtų atspindėti būtent šių duomenų perėmimo veika. Šiuo požiūriu atkreiptinas dėmesys ir į tai, kad neteisėtas elektroninių ryšių tinklais perduodamų duomenų gavimas bene visada bus susijęs ir su srauto, ir su turinio duomenų gavimu;

antra, ar įstatymų leidėjas, atskirdamas fiksavimą ir perėmimą, nesiekė fiksavimo susieti tik su siunčiamų duomenų nuskaitymu, kai jų srautui, t. y. pačiam duomenų perdavimui, įtakos nedaroma – srautas toliau keliauja nuo siuntėjo iki gavėjo. Perėmimu būtų laikomi tokie kaltininko veiksmai, kuriems būdingas neteisėtas poveikis pačiam duomenų srautui tinkle. Tai galėtų būti ir siunčiamų duomenų perėmimas, kai šie nepasiekia numatyto gavėjo, ir veiksmai, kuriais, pavyzdžiui, yra perimama sesijos kontrolė, serveryje sėkmingai nustačius teisėto vartotojo tapatybę[445].

Apibendrinant minėtuosius bandymus atskirti fiksavimą nuo perėmimo pabrėžtina, kad pateikti aiškinimai nėra išvedami iš Konvencijos dėl elektroninių nusikaltimų nuostatų – joje nedaromas srauto ir turinio duomenų gavimo, duomenų srauto nuskaitymo ir poveikio pačiam srautui skirtumas. Vadinasi, pasirinkus vieną iš atribojimo problemos sprendimo būdų, tampa aišku, kad jis būtų laikomas tik nacionalinėje teisėje numatytu neteisėto perėmimo veikos aiškinimo ypatumu. Artimiausias Konvencijos dėl elektroninių nusikaltimų nuostatoms ir tam tikram paaiškinimui nacionalinėje teisėje (atsižvelgiant į BK 166 straipsnyje numatytos nusikalstamos veikos požymius) galėtų būti pirmasis pastebėjimas, kad siekiant atskirti fiksavimą nuo perėmimo turėtų būti daromas skirtumas tarp neteisėto srauto ir turinio duomenų gavimo. Toks aiškinimas ir technologiniu požiūriu nebūtų labai specifinis, nors, be abejo, atsižvelgiant į tokio pobūdžio nusikalstamų veikų padarymo mechanizmą, kaltininkui bene visada tektų inkriminuoti ne tik perėmimo, bet ir fiksavimo bei stebėjimo veikas. Siekiant įtvirtinti minėtąjį požymių interpretavimą, būtina tolesnė diskusija baudžiamosios teisės doktrinoje, be to, tokią nuomonę ateityje galėtų pagrįsti arba paneigti ir besiklostanti teismų praktika.

[445] Plačiau apie sesijų perėmimo metodus žr.: Česnys, A.; Juknius, J. Saugumo patikros ir etiško įsilaužimo technologijos. Kaunas: Technologija, 2011, p. 76–78.

Kaip minėta, antrasis elektroninių duomenų stebėjimo ir fiksavimo interpretavimo probleminis aspektas tampa aktualus tada, kai šios veikos analizuojamos iš *informacinėje sistemoje laikomų (nejudamų)* duomenų neteisėto gavimo pozicijų. Pereinant prie *nejudamų* duomenų stebėjimo analizės, reikėtų atkreipti dėmesį į tai, kad dėl paties stebėjimo suvokimo didesnių problemų nekyla – tokia veika gali būti apibūdinama kaip jų matymas, analizavimas, duomenų fiksavimas kaltininko mintyse, kai šie nėra atkuriami nei elektronine, nei materialiąja forma. Tokią veiką sudėtinga vertinti dėl kito jos aspekto, t. y. stebėjimo perteklinio kriminalizavimo grėsmės. Neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtyje stebėjimas numatomas kaip alternatyvi veika, vien jos padarymo pakanka baudžiamajai atsakomybei pagal BK 198 straipsnį kilti. Inkriminuojant taip aprašytą nusikalstamą veiką, nereikalaujama nustatyti papildomų tokios veikos pavojingumą rodančių aplinkybių, pavyzdžiui, techninių priemonių taikymo, kaltininko nusikalstamų ketinimų, tam tikro besitęsiančios veikos pobūdžio ar kitų veikos pavojingumą didinančių veiksnių. Apie vieną iš tokių, t. y. techninių priemonių taikymą, užsimenama ir Konvencijos dėl elektroninių nusikaltimų aiškinamajame rašte – nors kalbama apie perėmimą, jame atkreipiamas dėmesys ir į tokio pobūdžio nusikalstamos veikos perteklinio kriminalizavimo grėsmę. Sprendžiant šią problemą, valstybėms suteikiama galimybė apriboti nusikalstamos neteisėto perėmimo veikos taikymą jos sudėtyje numatant ir techninių priemonių taikymo reikalavimą (53 punktas). Kadangi BK 198 straipsnyje tokių veikos pavojingumą didinančių požymių nenumatyta, informacinėje sistemoje laikomų elektroninių duomenų stebėjimo veika rodo sunkiai nuspėjamą šio BK straipsnio apimtį, kai bet koks žvilgtelėjimas į neviešus elektroninius duomenis gali būti laikomas apysunkiu nusikaltimu. Vadinasi, svarbu atkreipti dėmesį į tai, kad pavojingumo prasme stebėjimas kaip veika gali pasireikšti labai įvairiai, todėl neturėtų būti automatiškai nustatoma ir inkriminuojama.

Šiuo požiūriu reikėtų atkreipti dėmesį, kad Lietuvos Aukščiausiojo Teismo praktikoje, siekiant išvengti formalaus baudžiamojo įstatymo taikymo, ne kartą buvo pabrėžiama nusikalstamų ir vertinant iš baudžiamosios teisės pozicijų nepavojingų veikų atskyrimo svarba. Teismas tvirtino, kad *jei veika turi konkrečios nusikaltimo sudėties požymius, tačiau iš esmės nepadaro žalos baudžiamojo įstatymo saugomiems*

visuomeniniams santykiams arba kitiems teisiniams gėriams ar nesukelia realaus pavojaus tokiai žalai atsirasti, yra objektyvios prielaidos išvadai, kad tokia veika vertintina kaip nereikšminga baudžiamojo įstatymo saugomoms vertybėms[446]. Kadangi neviešų elektroninių duomenų stebėjimo veika yra baigta nuo stebėjimo veiksmų pradžios, tai diskusiniais atvejais, pagrindžiant tokių veiksmų pavojingumą, svarbu nustatyti ne tik patį stebėjimo faktą, bet ir kitas žalos baudžiamojo įstatymo saugomiems teisiniams gėriams kilimą arba akivaizdžią tokios žalos kilimo grėsmę rodančias aplinkybes. Stebėjimo pavojingumą gali pagrįsti, pavyzdžiui, kaltininko ketinimai gavus duomenis padaryti kitų nusikalstamų veikų, duomenų apsaugos priemonių pažeidimai, įvairių techninių priemonių, skirtų duomenims gauti, taikymas, neteisėti kaltininko veiksmai prisijungiant prie informacinės sistemos ir tokiu būdu gaunant prieigą prie duomenų, nuolatiniai stebėjimo veiksmai, stebimų duomenų kiekis, žalos sukėlimas ir kt. Beje, BK 198 straipsnį komentavę autoriai, apibūdindami stebėjimą, irgi atkreipė dėmesį į tai, kad šie veiksmai „pasižymi tam tikru pastovumu ir užima tam tikrą laiko tarpą“[447].

Kitas klausimas yra susijęs su dviejų BK 198 straipsnio dispozicijoje numatytų alternatyvų – fiksavimo ir įgijimo – atskyrimo sunkumais. Kaip teigiama literatūroje, fiksavimui yra būdingas „elektroninių duomenų paėmimas savo dispozicijon bei jų fizinis perkėlimas į savo kontroliuojamą informacijos laikmeną“. Kartu nurodoma, kad toks „paėmimas gali pasireikšti elektroninių duomenų (bylos, aplanko) perkėlimu, nukopijavimu į kaltininko kompiuterį, išorinę laikmeną ar jo naudojamą serverį internete, vaizduoklio vaizdo duomenų filmavimas į kaltininko vaizdo kasetę, garso įrašo įrašymas ir pan.“[448] Vis dėlto toks fiksavimo suvokimas kelia problemų šią veiką atribojant nuo elektroninių duomenų įgijimo, kuris bendriausia prasme gali būti apibūdintas kaip elektroninių duomenų gavimas, neatsižvelgiant

---

[446] Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. sausio 24 d. nutartis baudžiamojoje byloje Nr. 2K-86/2006, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 21 d. nutartis baudžiamojoje byloje Nr. 2K-560/2010.

[447] Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 432.

[448] *Ibidem*.

į jų gavimo būdą[449]. Dėl tokio sutapimo kyla diskusijų, kokiais kriterijais vadovaujantis gali būti atskiriamos šios beveik analogiškos veikos. Pačių kriterijų, kaip ir aptartojo fiksavimo bei perėmimo atribojimo atveju, nei baudžiamosios teisės doktrinoje, nei teismų praktikoje nepateikiama. Tiesa, teismų praktikoje pasitaiko pavienių atvejų, kai kaltininkas yra pripažįstamas kaltu padaręs nusikalstamą veiką, numatytą BK 198 straipsnio 1 dalyje, t. y. neteisėtai stebėjęs ir fiksavęs neviešus elektroninius duomenis. Kita vertus, teismų praktikoje nenurodomi kriterijai, kuriais remiantis jam inkriminuotos būtent šios alternatyvos. Pavyzdžiui, vienoje iš baudžiamųjų bylų konstatuota, kad *Ž. Š., pasinaudojęs <...> notaro biurui suteiktu prisijungimo vardu <...> ir slaptažodžiu <...>, ikiteisminio tyrimo metu tiksliai nenustatytu laiku ir vietoje, iš kompiuterių su kintamais IP adresais (duomenys neskelbtini) 386 kartus neteisėtai prisijungė prie Registro centro duomenų bazės bei stebėjo ir fiksavo neviešus elektroninius duomenis apie privačių asmenų turimą kilnojamąjį ir nekilnojamąjį turtą, tokiu būdu padarė <...> notarų biurui 5 606 Lt turtinę žalą. Savo veiksmais Ž. Š. padarė nusikalstamą veiką, numatytą Lietuvos Respublikos BK 198 str. 1 d.* Be to, nuosprendyje nurodoma, kad *Ž. Š. savo reikmėm prisijungdavo prie Registro centro duomenų bazės iš skirtingų kompiuterių, kurie priklausė jam, draugams, interneto kavinėms*[450]. *Prisijungdavo tikslu gauti duomenis apie asmenų nekilnojamąjį turtą.* Nors elektroninių duomenų įgijimas bendriausia prasme suvokiamas kaip jų gavimas, vis dėlto lieka neaišku, kokiais kriterijais vadovaujantis kaltininkui buvo inkriminuotas neviešų elektroninių duomenų fiksavimas, o ne jų įgijimas.

Nors galima teigti, kad informacinėje sistemoje *saugomų (laikomų) elektroninių duomenų* fiksavimo ir įgijimo veikos iš esmės yra analogiško turinio, bet jas kaip alternatyvas numačius BK 198 straipsnio dispozicijoje neišvengiamai tenka ieškoti galimų jų atribojimo kriterijų. Šiuo požiūriu svarstytina, ar fiksavimo nuo elektroninių

---

[449] Pavyzdžiui, aiškinant neteisėtą *informacijos įgijimą* remiantis BK 124 straipsniu (neteisėtas disponavimas informacija, kuri yra valstybės paslaptis), be įvairių kitų įgijimo būdų, dar nurodomas įrašymas ir fotografavimas (Abramavičius, A., *et al.* Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 432, p. 102).

[450] Vilniaus rajono apylinkės teismo 2009 m. rugsėjo 8 d. nuosprendis baudžiamojoje byloje Nr. 1-278-298/2009.

duomenų įgijimo, be kita ko, nebūtų galima atskirti remiantis tuo, kad inkriminuojant fiksavimą nekiltų problemų dėl duomenų formos pakeitimo iš elektroninės į materialiąją (pavyzdžiui, elektroninius duomenis užrašant, išspausdinant ar kt.).

Apibendrinant galima teigti, kad bene didžiausia problema, kylanti analizuojant stebėjimo ir fiksavimo veikas, yra susijusi su neaiškia įstatymo leidėjo pozicija kriminalizuojant elektroninių duomenų konfidencialumo pažeidimus. Atviras lieka klausimas, ar minėtųjų veikų dalykas yra tik informacinėje sistemoje *perduodami*, ar ir joje *laikomi* elektroniniai duomenys. Atsižvelgiant į Konvencijos dėl elektroninių nusikaltimų nuostatų aiškinimą, panašių veikų įtvirtinimo BK ypatumus ir įvertinus nusikalstamos veikos perteklinio kriminalizavimo riziką, siūlytina stebėjimo ir fiksavimo veikas (kaip ir perėmimo veiką) susieti tik su informacinėje sistemoje *perduodamų duomenų* neteisėtu gavimu.

2.2.3. Įgijimas

Neteisėta elektroninių duomenų įgijimo veika, nors ir laikoma viena iš neteisėtos prieigos prie duomenų išraiškos formų, tokia, kokia ji yra įtvirtinta BK 198 straipsnio dispozicijoje, tiesioginės sąsajos su Konvencijos dėl elektroninių nusikaltimų nuostatomis neturi. Kaip minėta, daugelyje valstybių neteisėta prieiga prie duomenų iš dalies yra siejama su neteisėta prieiga prie informacinės sistemos (pasirinkus vieną iš galimų neteisėtos prieigos prie sistemos kriminalizavimo variantų). Dėl to siekiant atskleisti ir nuosekliai išaiškinti neteisėto elektroninių duomenų įgijimo turinį, svarbu nustatyti, kaip tokio pobūdžio pavojinga veika interpretuojama kitų kategorijų baudžiamosiose bylose.

Analizuojant baudžiamosios teisės teorijoje pareikštas nuomones ir teismų praktikoje pateikiamus neteisėto įgijimo aiškinimus matyti, kad bendriausia prasme įgijimas suprantamas kaip bet kokie kaltininko veiksmai, kuriuos atlikdamas jis neteisėtai gauna nusikalstamos veikos dalyką. Pavyzdžiui, teismų praktikoje nusikalstamų veikų finansų sistemai bylose įgijimas apibūdinamas kaip „veiksmai, kuriuos atlikę asmenys *gauna* netikrą, suklastotą ar svetimą mokėjimo instrumentą arba įrangą, kompiuterinę programą ar kitokią priemonę, tiesiogiai skirtą ar pritaikytą netikriems, suklastotiems mokėjimo instrumentams ar jų dalims gaminti arba tikriems mokėjimo instrumentams

klastoti“[451]. Bene analogišką įgijimo sąvoką pateikia BK 214 straipsnį komentavę autoriai. Jų nuomone, įgijimas – tai bent vienos elektroninės mokėjimo priemonės „*gavimas* už atlygį ar be jo bet kokia forma“[452]. Literatūroje analizuojant disponavimo pornografinio turinio dalykais sudėties požymius, įgijimas (įsigijimas) yra suprantamas kaip „bet kokie veiksmai, kuriais asmuo realiai *gauna* tam tikrą daiktą“[453]. Neteisėtas nusikalstamos veikos dalyko įgijimas, kaip ir jo gavimas, vienodai aiškinamas ir nusikalstamų veikų, susijusių su disponavimu narkotinėmis ar psichotropinėmis medžiagomis, bylose. Remiantis susiformavusia teismų praktika, šiose bylose įgijimu yra laikomi veiksmai, „kuriuos atlikęs asmuo *gauna* psichotropinių ar narkotinių medžiagų“[454], bei daugeliu kitų atvejų. Vadinasi, pati įgijimo veika aiškinama gana plačiai, į jos turinį įtraukiant bet kokius veiksmus, kuriuos atliekant gaunamas nusikalstamos veikos dalykas. Kita vertus, analizuojant BK 198 straipsnio dispozicijoje aprašytas alternatyvas matyti, kad neteisėto elektroninių duomenų įgijimo turinys yra susiaurintas.

Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtyje elektroninių duomenų gavimas apibūdinamas keliomis alternatyviomis veikomis: stebėjimu, fiksavimu, perėmimu ir įgijimu. Nors įgijimui dažniausiai suteikiama gana plati reikšmė, BK 198 straipsnio dispozicijoje jis yra suskirstytas į tam tikrų specifinių aspektų turinčias veikas. Įgijimo ir fiksavimo atskyrimo probleminiai aspektai jau buvo analizuoti, bet vis dar aktualu kiek plačiau aptarti perėmimo ir įgijimo veikų tarpusavio santykį. Elektroninių duomenų perėmimas ir įgijimas pagal savo prasmę yra artimos veikos, bet jas abi įtvirtinus nusikalstamos veikos sudėtyje, neišvengiamai tenka elektroninius duomenis skirstyti į *laikomus (saugomus)*

---

[451] Lietuvos Aukščiausiojo Teismo senato 2005 m. gruodžio 29 d. nutarimo Nr. 55 „Dėl teismų praktikos nusikalstamų veikų finansų sistemai baudžiamosiose bylose (BK 214, 215, 219, 220, 221, 222, 223 straipsniai)“ 5 punktas. *Teismų praktika*, 2005, Nr. 24.

[452] Abramavičius, A., *et al*. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai). Vilnius: Registrų centras, 2010, p. 32.

[453] Žėkas, T. Vaiko išnaudojimas pornografijai: baudžiamieji teisiniai ir kriminologiniai aspektai: daktaro disertacija. Vilnius: Vilniaus universitetas, 2011, p. 130.

[454] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2009 m. spalio 20 d. nutartis baudžiamojoje byloje Nr. 2K-P-218/2009.

informacinėje sistemoje ir *šioje sistemoje perduodamus*. Kai perėmimas yra susijęs išimtinai tik su elektroninių ryšių tinklais ar pačiame kompiuteryje perduodamų duomenų gavimu, tai siekiant išvengti dubliavimo tokie veiksmai turėtų būti eliminuojami iš alternatyvios neteisėto įgijimo veikos. Vadinasi, apie neteisėtą įgijimą reikėtų kalbėti tik tais atvejais, kai neteisėtai gaunami informacinėje sistemoje laikomi (saugomi), t. y. *nejudami,* elektroniniai duomenys. Šiuos duomenis galima įgyti įvairiais būdais: kaltininkui pačiam tiesiogiai prie jų priėjus, elektroninius duomenis nusipirkus, gavus veltui arba mainais, juos parsisiuntus elektroninių ryšių tinklais, išviliojus apgaule, grasinant ar kokiu nors kitu būdu.

Dėl tokio minėtųjų veikų aiškinimo ir perėmimas, ir įgijimas įgyja atskirą reikšmę, todėl šios veikos nelaikomos viena iš kitos išplaukiančiomis. Kai kuriais atvejais perimti duomenys kaltininko vėliau gali būti neteisėtai įgyti (pavyzdžiui, perkant) iš šiuos duomenis perėmusių asmenų, bet perėmimas nėra vienintelis būdas gauti elektroninius duomenis. Dėl to galimi atvejai, kai duomenis kaltininkas įgyja iš kitų asmenų, kurie šiuos duomenis gavo ne perėmimo būdu. Atitinkamai abejonių kelia literatūroje reiškiama nuomonė, kad „elektroninių duomenų įgijimas yra vėliau po perėmimo vykstantis veiksmas, kurio metu asmuo realiai gauna šiuos duomenis“[455]. Vis dėlto perėmimas neturėtų būti laikomas pirminiu duomenų įgijimo etapu, o šioms nusikalstamoms veikoms suteikus atskirą reikšmę, jos rodytų skirtingus ir dažniausiai nesusijusius neteisėto elektroninių duomenų gavimo būdus.

Elektroninius duomenis apibrėžiant remiantis *tinkamumo juos apdoroti informacinėje sistemoje* kriterijumi, tampa akivaizdu, kad neprarasdami tokios formos jie gali egzistuoti tik sistemoje, tam tikroje jos dalyje ar išoriniuose informacijos kaupikliuose (pavyzdžiui, kompaktiniuose diskuose, USB atmintinėse ir kt.). Diskusijų, kiek ir kokias nusikalstamas veikas padarė kaltininkas, gali kilti nustačius, kad jis pagrobė kurią nors iš minėtųjų priemonių kartu su joje esančiais neviešais elektroniniais duomenimis. Tokiais atvejais sprendžiama, ar kaltininko veiksmai iš baudžiamosios teisės pozicijų vertintini tik kaip, pavyzdžiui, vagystė (BK 178 straipsnis) ar plėšimas (BK 180 straipsnis) dėl materialiųjų objektų pagrobimo, ar kaltininko veikai kvalifikuoti

[455] Abramavičius, A., *et al.* Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 432.

turėtų būti taikoma ir atitinkama BK 198 straipsnio dalis dėl elektroninių duomenų neteisėto įgijimo. Analizuojant neteisėtą elektroninių duomenų įgijimą, šiuo požiūriu literatūroje pagrįstai neginčijama galimybė kaltininkui inkriminuoti ir neteisėtą elektroninių duomenų įgijimą, jeigu nustatoma, kad jo tyčiniai veiksmai buvo nukreipti į tokių duomenų gavimą. Vadinasi, pagal BK 198 straipsnį „kvalifikuojami ir tie atvejai, kai kaltininkas, siekdamas perimti elektroninius duomenis, pasisavina patį kompiuterį ar jo techninę įrangą (standųjį diską), išorinės atminties įrenginius (diskelius, magnetinius optinius diskus, kompaktinius diskus, DVD diskus ar magnetines juostas), kuriuose tokie duomenys yra“[456]. Panašiai teigiama, kad neteisėta prieiga prie įstatymo saugomos informacijos konstatuotina ne tik tada, kai prie jos prasiskverbiama naudojantis mokslo laimėjimais ir technika, bet ir tais atvejais, kai neteisėta prieiga gaunama tradiciniais būdais: pagrobiant pačias informacijos laikmenas ar techninę įrangą, kurioje yra saugoma informacija[457].

Apibendrinant siūlytina atskirti neteisėto perėmimo ir įgijimo veikas pagal tai, kokie duomenys – *informacinėje sistemoje laikomi* ar *joje perduodami* – buvo gauti. Be to, neviešų elektroninių duomenų įgijimu, atsižvelgiant į kaltininko tyčinių veiksmų kryptingumą, pripažintinas ir sistemos komponentų, kuriuose laikomi elektroniniai duomenys, gavimas. Tokiais atvejais kaltininko veika, be nuorodų į BK 178 ir 180 straipsnius, taip pat kvalifikuotina pagal atitinkamą BK 198 straipsnio dalį[458].

2.2.4. Laikymas

BK 198 straipsnio dispozicijoje esančios pavojingo laikymo, kaip ir jau aptarto įgijimo, veikos ištakų reikėtų ieškoti ne tarptautinėje ar

---

[456] Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 432.

[457] Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik [Russian criminal law. Special Part: The textbook]. Borzenkova, G. N.; Komissarova, V. S. (red.), Moskva: Zercalo-M, 2005, p. 286; Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik [Russian criminal law. Special Part: The textbook]. Revina, V. P. 2-asis pataisytas ir papildytas leidimas. Moskva: Justicinform, 2010, p. 252.

[458] Šiuo požiūriu ir vėl būtina pabrėžti bendrosios BK 198 straipsnyje numatytos ir kituose BK straipsniuose įtvirtintų specialiųjų normų (pavyzdžiui, BK 167, 210 straipsniai) nustatymo ir atskyrimo svarbą.

ES, o nacionalinėje teisėje. Ši su elektroninių duomenų konfidencialumo pažeidimais susijusi veika nėra numatyta nei Konvencijos dėl elektroninių nusikaltimų, nei Direktyvos 2013/40/ES nuostatose. Vadinasi, siekiant nuosekliai išaiškinti laikymo veiką, būtina atsižvelgti į tai, kaip ji suprantama lyginant su kitomis nusikalstamomis veikomis, kuriose numatomas toks sudėties požymis.

Teismų praktikoje laikymas įvairių kategorijų baudžiamosiose bylose suvokiamas bene vienodai – kaip nusikalstamos veikos dalyko buvimas kaltininko žinioje, arba kitaip – kaip jų turėjimas. Pavyzdžiui, nusikalstamų veikų finansų sistemai bylose laikymas apibrėžiamas kaip nusikalstamos veikos dalykų, numatytų BK 214 straipsnyje, *buvimas kaltininko žinioje*, „neatsižvelgiant į jų turėjimo laiko trukmę ar buvimo vietą (su savimi, patalpoje ar kitoje vietoje)“[459]. Bene analogiška laikymo sąvoka pateikiama ir nusikalstamų veikų, susijusių su disponavimu narkotinėmis ar psichotropinėmis medžiagomis, bylose aiškinant šių medžiagų laikymo požymį. Jose laikymu pripažįstamas nusikalstamos veikos dalykų *buvimas kaltininko žinioje,* neatsižvelgiant į jų turėjimo laiko trukmę ar buvimo vietą (su savimi, patalpoje, slėptuvėje ar kitose vietose)[460] arba „bet koks faktinis psichotropinių ar narkotinių medžiagų *turėjimas,* neatsižvelgiant į laiką, kiekį ar jų buvimo vietą“[461]. Panašiai laikymo veika yra aiškinama ir mokslinėje literatūroje, pavyzdžiui, interpretuojant disponavimo pornografinio turinio dalykais sudėties požymius. Anot T. Žėko, šiose bylose „laikymas apibrėžiamas per *turėjimo* ir *valdymo* sąvokas“[462]. Į tokį veikos interpretavimą turėtų būti atsižvelgiama aiškinant ir ne-

[459] Lietuvos Aukščiausiojo Teismo senato 2005 m. gruodžio 29 d. nutarimo Nr. 55 „Dėl teismų praktikos nusikalstamų veikų finansų sistemai baudžiamosiose bylose (BK 214, 215, 219, 220, 221, 222, 223 straipsniai)“ 5 punktas. *Teismų praktika*, 2005, Nr. 24.

[460] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2009 m. spalio 20 d. nutartis baudžiamojoje byloje Nr. 2K-P-218/2009, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. balandžio 19 d. nutartis baudžiamojoje byloje Nr. 2K-162/2011.

[461] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gegužės 11 d. nutartis baudžiamojoje byloje Nr. 2K-185/2010.

[462] Žėkas, T. Vaiko išnaudojimas pornografijai: baudžiamieji teisiniai ir kriminologiniai aspektai: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: Vilniaus universitetas, 2011, p. 134.

teisėtą neviešų elektroninių duomenų laikymą, bet, palyginti su tradiciniu suvokimu, išplečiant jų turėjimo galimybes ne tik fizinėje, bet ir elektroninėje erdvėje. Apie laikymą iš elektroninės erdvės pozicijų būtina kalbėti dėl pačios analizuojamos nusikalstamos veikos dalyko specifikos – duomenys pripažįstami elektroniniais duomenimis, jei jie gali būti apdorojami informacinėje sistemoje. Elektroninė duomenų forma dažniausiai yra išsaugoma, jeigu jie yra sistemoje (jos dalyse arba išoriniuose informacijos kaupikliuose), vadinasi, ir neteisėtas laikymas yra siejamas su jų buvimu tokioje vietoje. Nuorodų į duomenų laikymą elektroninėje erdvėje galima įžvelgti ir BK 198 straipsnį komentavusių autorių pateiktoje laikymo sąvokoje. Kaip teigiama, laikymas yra „bet koks faktinis elektroninių duomenų turėjimas neprikla usomai nuo turėjimo laiko, jų buvimo vietos (su savimi, patalpoje, kompiuterio atmintyje, savo elektroninio pašto serveryje ir pan.)“[463]. Šiam analogišku aiškinimu yra remiamasi ir teismų praktikoje, akcentuojant elektroninių duomenų turėjimą kaltininko žinioje[464].

Nors nei teismų praktikoje, nei literatūroje neginčijama, kad neteisėtas laikymas gali būti apibūdinamas atsižvelgiant į nusikalstamos veikos dalyko turėjimą (buvimą) kaltininko žinioje, bet šią veiką analizuodami pagal BK 198 straipsnį kai kurie autoriai savo darbuose laikymui ir turėjimui nepagrįstai bando suteikti skirtingas prasmes. Pavyzdžiui, abejonių kelia išvada, kad „tapatybės vagystės <...> antrosios stadijos elementas – su tapatybe susijusios informacijos turėjimas – LR BK nėra kriminalizuotas, o baudžiamąją atsakomybę užtraukia tik neviešų elektroninių duomenų ir svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių laikymas“[465]. Kalbant apie tapatybės vagystę[466] elektroninėje erdvėje, vis dėlto reikėtų pri-

[463] Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 432–433.

[464] Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendis baudžiamojoje byloje Nr. 1-234-825/2017.

[465] Štitilis, D., *et al*. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai. Vilnius: Mykolo Romerio universitetas, 2011, p. 256.

[466] Tapatybės vagystės sąvoka, vertinant ją iš baudžiamosios teisės pozicijų, nėra tiksli, nes vagystės dalyku ir baudžiamosios teisės teorijoje, ir teismų praktikoje neginčijamai pripažįstami, be kita ko, tik materialiąją išraišką ir ekonominę vertę turintys objektai. Kita vertus, ši sąvoka vartojama kaip tiesioginis *identity theft* vertinys.

pažinti, kad su asmens tapatybe susijusių elektroninių duomenų laikymas ir yra jų turėjimas kaltininko žinioje (nesvarbu, ar minimi BK 198, 198[2], 214 ar kiti straipsniai).

Kadangi laikymo veika yra trunkamoji, tai jos pradžios momentas yra siejamas su elektroninių duomenų patekimu kaltininko žinion, o pabaigos – su šios veikos nutraukimu (arba dėl paties kaltininko veiksmų, arba dėl nuo jo valios nepriklausančių aplinkybių). Vadinasi, vien pats elektroninių duomenų turėjimo faktas rodo baigtą neteisėto elektroninių duomenų perėmimo ir jų panaudojimo veiką, neatsižvelgiant į ankstesnius (pavyzdžiui, įgijimo, perėmimo) ar tolesnius kaltininko veiksmus (pavyzdžiui, paskleidimo). Atsižvelgiant į tai, kad baudžiamoji atsakomybė už elektroninių duomenų laikymą kyla tik kai tokie duomenys patenka kaltininkui, būtina nustatyti, kada jis gavo įvairių materialiųjų priemonių, kuriose laikomi elektroniniai duomenys (pavyzdžiui, USB atmintinių, kompaktinių diskų ir kt.), arba kada šie duomenys yra kaltininko gauti jam prieinamoje vietoje elektroninėje erdvėje (pavyzdžiui, elektroninio pašto serveryje, kitame serveryje, žinant prisijungimo būdą, prisijungimo duomenis ir kt.). Visais minėtaisiais atvejais inkriminuojant laikymo veiką yra svarbu konstatuoti ir kaltininko galimybę prieiti prie elektroninių duomenų, daryti jiems poveikį, t. y. priimti sprendimą dėl tolesnio jų likimo. Remiantis teismų praktika, šią aplinkybę rodo tai, kad, pavyzdžiui, kaltininkas duomenis laikė savo kontroliuojamose informacijos laikmenose (išoriniame duomenų kaupiklyje, asmeniniame nešiojamajame kompiuteryje)[467], duomenis įrašė į išorinę laikmeną ir juos turėjo su savimi[468].

Darant išvadą, kad kaltininkas neteisėtai laikė neviešus elektroninius duomenis, būtina atsižvelgti ir į subjektyvų momentą, t. y. ar jis suvokė, kad savo žinioje neteisėtai turi neviešus elektroninius duomenis. Šis aspektas svarbus tada, kai duomenys yra gauti, pavyzdžiui, elektroniniu paštu ar yra kitose kaltininkui prieinamose vietose, jei šių duomenų jis dar nespėjo peržiūrėti. Tokiais atvejais subjektyvus momentas leidžia pagrįsti arba paneigti laikymo veiką. Jei kaltininkui žinoma, kad jis neteisėtai gavo neviešus elektroninius duomenis ir gali daryti jiems poveikį, peržiūrėjimo arba nespėjimo jų peržiūrėti faktas

[467] Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje Nr. 1-1430-276/2011.

[468] Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendis baudžiamojoje byloje Nr. 1-188-785/2009.

šią veiką pripažįstant laikymu ar jos baigtumui įtakos negali turėti. Beje, tokios pozicijos laikomasi ir disponavimo pornografinio turinio dalykais bylose, kai „žinojimo" momentas tampa svarbus sprendžiant, ar kas nors laiko (turi) savo žinioje pornografinę medžiagą[469].

2.2.5. Pasisavinimas

Pasisavinimo požymis neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtyje buvo numatytas jau 2003 metais įsigaliojus naujajam BK[470]. Nors šis požymis BK 198 straipsnio dispozicijoje išliko ir po 2007 metų BK XXX skyriaus pakeitimų, bet, kaip matyti, elektroninių duomenų pasisavinimo turinys pakito iš esmės. Skirtingo, nors ir vienodai įvardyto, sudėties požymio interpretavimo poreikis kilo dėl 2007 metų pakeitimų BK 198 straipsnyje atsiradus įvairių pavojingų veikų alternatyvų. Iki 2007 metų pasisavinimas minėtojo straipsnio dispozicijoje buvo numatytas kaip vienintelis požymis, reiškiantis kompiuterinės informacijos gavimą, o po 2007 metų aprašant neteisėtą elektroninių duomenų gavimą įtvirtintos ir stebėjimo, fiksavimo, perėmimo bei įgijimo veikos. Vadinasi, siekiant atskirti pasisavinimą nuo kitų minėtųjų veikų, šiam požymiui būtina suteikti atskirą turinį, taip išvengiant dispozicijoje esančių požymių dubliavimosi. Be to, užtikrinant nuoseklų pasisavinimo požymio aiškinimą ir BK vidinę darną, būtina atsižvelgti į jo interpretavimą kitų nusikalstamų veikų sudėtyse.

Remiantis pavieniais bandymais atskleisti elektroninių duomenų pasisavinimo turinį, literatūroje bendriausia prasme šis požymis yra siejamas su elektroninių duomenų gavimu. Pavyzdžiui, pasitaiko nuomonių, kad pasisavinimas – tai „elektroninių duomenų paėmimo sulyginimas su perėmimu, tačiau šiuo atveju duomenys nekeliauja ryšių tinklais, bet asmuo turi galimybę perimti duomenis, esančius konkrečioje tinklo ar informacinės sistemos vietoje ar laikmenoje"[471]. Šis

[469] Žėkas, T. Vaiko išnaudojimas pornografijai: baudžiamieji teisiniai ir kriminologiniai aspektai: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: Vilniaus universitetas, 2011, p. 142.

[470] Iki 2007 metų BK 198 straipsnio pakeitimų ši nusikalstama veika buvo vadinama kompiuterinės informacijos pasisavinimu ir skleidimu.

[471] Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 433.

apibrėžimas kelia klausimą, kaip tokiu būdu aiškinamą pasisavinimo požymį galima atskirti nuo neteisėto elektroninių duomenų įgijimo. Tiesa, tokią nuomonę pareiškę BK 198 straipsnį komentavę autoriai elektroninių duomenų įgijimu laikė kitą, po perėmimo, einantį etapą, „kurio metu asmuo realiai gauna šiuos duomenis“[472]. Dėl tokio aiškinimo nelengva nustatyti ne tik įgijimo bei perėmimo, bet ir įgijimo bei pasisavinimo požymių skirtumus, jie gali būti dubliuojami. Vadinasi, darytina prielaida, kad įstatymų leidėjas, BK 198 straipsnio dispozicijoje įtvirtinęs gana daug alternatyvių neteisėtą elektroninių duomenų gavimą nurodančių požymių, pasisavinimui siekė suteikti atskirą turinį. Kadangi nuoseklus pasisavinimo aiškinimas yra gana svarbus, jo interpretavimas turėtų kisti gana radikaliai – randant elektroninių duomenų pasisavinimo ir turto pasisavinimo bendrumų. Be abejo, siekiant elektroninei erdvei pritaikyti turtinių nusikalstamų veikų doktrinoje ir teismų praktikoje pateiktus pasisavinimo išaiškinimus, turėtų būti nusprendžiama, ar tokie minėtojo požymio aiškinimai ir kokios apimties galėtų būti taikomi „skaitmeniniame kontekste“.

Vadovaujantis susiformavusia teismų praktika, turto pasisavinimu laikoma veika, kai kaltininkas jam patikėtą ar jo žinioje esantį svetimą turtą tyčia neteisėtai neatlygintinai paverčia savo turtu, t. y. ima elgtis su svetimu turtu kaip su savu ir taip padaro žalos turto savininkui[473]. Toks aiškinimas svarbus dėl keleto aspektų: *pirma*, jis padeda nurodyti specifinį subjekto santykį su nusikalstamos veikos dalyku. Būtent šis santykis literatūroje[474] ir teismų praktikoje laikomas vienu iš kriterijų,

---

[472] *Ibid*., p. 432.

[473] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. gegužės 5 d. nutartis baudžiamojoje byloje Nr. 2K-104/2009, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2007 m. kovo 20 d. nutartis baudžiamojoje byloje Nr. 2K-123/2007, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 25 d. nutartis baudžiamojoje byloje Nr. 2K-396/2006, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. gegužės 30 d. nutartis baudžiamojoje byloje Nr. 2K-330/2006.

[474] Bukelienė, D. Baudžiamoji atsakomybė už turto pasisavinimą ir turto iššvaistymą (teoriniai ir praktiniai aspektai). Vilnius: Eugrimas, 2008, p. 132; Sinkevičius, E. Neteisėtas banko kredito gavimas arba panaudojimas ir jų kvalifikavimas. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002, p. 169–172.

leidžiančių turto pasisavinimą atskirti nuo kitų nusikalstamų veikų nuosavybei, turtinėms teisėms ir turtiniams interesams; *antra*, konstatuojant pasisavinimą turėtų būti nustatomas turtinės žalos padarymo faktas kaltininkui neteisėtai užvaldžius svetimą turtą[475]. Kita vertus, kyla nemažai problemų šiuos kriterijus taikant elektroninėje erdvėje, t. y. sprendžiant, ką įstatymų leidėjas siekė kriminalizuoti elektroninių duomenų pasisavinimu.

Remiantis pirmuoju kriterijumi, kuris taikomas apibūdinant specifinį kaltininko santykį su turtu, kaip matyti iš BK 183 straipsnio dispozicijos, reikalaujama konstatuoti, kad turtas buvo jam patikėtas arba buvo jo žinioje. Tokių specialiųjų įgaliojimų išaiškinimas yra suformuluotas teismų praktikoje, be to, įvairių šių įgaliojimų aiškinimo aspektų pateikiama ir literatūroje. Neplėtojant diskusijos dėl turto pripažinimo patikėtu ar esančio kaltininko žinioje, bendriausia prasme teigtina, kad patikėtas turtas – „tai einamų pareigų, specialių pavedimų, sutarčių ar kitu teisiniu pagrindu kaltininko valdomas svetimas turtas <...>, į kuriuos kaltininkas turi teisiškai apibrėžtus įgalinimus (pavyzdžiui, ir yra materialiai atsakingas už šį turtą ar turtinę teisę)“[476]. Pagal teismų praktiką, esančiu kaltininko žinioje yra laikomas toks turtas, kai kaltininkas dėl savo einamų pareigų turi teisę pavaldiems ar kitiems asmenims, kuriems šis turtas patikėtas, duoti nurodymus dėl jo panaudojimo[477]. Tokius aiškinimus įprasta taikyti kaltininkui inkriminuojant turto pasisavinimą, bet BK 198 straipsnyje numačius elektroninių duomenų pasisavinimo požymį neišvengiamai kyla klausimų, kiek ir kaip minėtasis kriterijus turėtų būti aiškinamas nustatant elektroninių duomenų konfidencialumą pažeidžiančią nusikalstamą veiką. Juo labiau kad apie minėtąjį *elektroninių duomenų kaip daikto* palyginimą įmanoma kalbėti tik metaforiškai.

---

475 Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2008 m. gruodžio 9 d. nutartis baudžiamojoje byloje Nr. 2K-368/2008, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-76/2009.

476 2015 m. kovo 19 d. „Teismų praktikos turto pasisavinimo ir turto iššvaistymo baudžiamosiose bylose apžvalga (BK 183 ir 184 straipsniai)“ 4.1 išvada. *Teismų praktika*, 2015, Nr. 42.

477 *Ibidem*.

Taikant kaltininko specifinio santykio su elektroniniais duomenimis kriterijų, didžiausia problema kyla dėl to, kad dažniausiai teisėtą prieigą prie neviešų elektroninių duomenų nustatytomis sąlygomis turi kelių kategorijų asmenys: *pirma*, tie, kurie tiesiogiai tvarko elektroninius duomenis kaip pirminį šaltinį (pavyzdžiui, užtikrina elektroninių duomenų įvedimą į duomenų bazę, jų tvarkymą ir kt.); *antra*, tie, kurie tiesiogiai nedirba su pirminiu šaltiniu, bet dėl darbo funkcijų ar sutarčių turi prieigą prie minėtųjų duomenų (pavyzdžiui, duomenų bazių vartotojai, kurie gali peržiūrėti jose esančius neviešus elektroninius duomenis ir kt.). Šiuo klausimu kol kas nekilo diskusijų nei baudžiamosios teisės doktrinoje, nei teismų praktikoje, todėl sudėtinga spręsti, kuriems iš minėtųjų asmenų galėtų būti taikoma pasisavinimo veika. Siekiant tikslumo reikėtų atkreipti dėmesį į tai, kad teismų praktikoje gana retai pasitaiko atvejų, kai kaltininkui inkriminuojant BK 198 straipsnyje numatytą nusikalstamą veiką nustatoma, kad jis turėjo teisėtą prieigą prie elektroninių duomenų. Kita vertus, apie nuoseklią BK 198 straipsnyje numatytų požymių taikymo praktiką kalbėti irgi sudėtinga – tokiais atvejais kaltininkui inkriminuojamas neteisėtas duomenų stebėjimas ir fiksavimas[478], neteisėtas stebėjimas ir įgijimas[479] arba neteisėtas įgijimas ir pasisavinimas[480].

Antrasis turto pasisavinimo požymis yra siejamas su turtinės žalos padarymu kaltininkui neteisėtai užvaldžius svetimą turtą. Teismų praktikoje pripažįstama, kad turto pasisavinimas laikomas baigtu neteisėtai užvaldžius svetimą turtą ir turint realią galimybę juo naudotis ar disponuoti[481]. Nors, skirtingai nei turto pasisavinimo atveju, kai dėl turto netekimo nukentėjusysis patiria turtinę žalą, elektroninių

[478] Vilniaus rajono apylinkės teismo 2009 m. rugsėjo 8 d. nuosprendis baudžiamojoje byloje Nr. 1-278-298/2009.

[479] Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. baudžiamasis įsakymas byloje Nr. 1-617-885/2011.

[480] Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendis baudžiamojoje byloje Nr. 1-188-785/2009.

[481] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. gegužės 30 d. nuosprendis baudžiamojoje byloje Nr. 2K-330/2006, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 25 d. nutartis baudžiamojoje byloje Nr. 2K-396/2006, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2008 m. gruodžio 9 d. nutartis baudžiamojoje byloje Nr. 2K-368/2008, Lietuvos Aukščiausiojo Teismo Bau-

duomenų pasisavinimo atveju kalbėti apie panašią žalą gana sudėtinga. Teisėtą prieigą prie duomenų turintis kaltininkas gali juos gauti kur kas paprasčiau – jam nereikia originalo, nes elektroniniai duomenys gali būti išspausdinami, užrašomi ar gaunami kitais panašiais veiksmais. Tokiais atvejais, kai nepadaroma jokio poveikio pirminiam elektroninių duomenų šaltiniui, tenka kelti klausimą ir dėl pačios žalos nustatymo: tiesioginio elektroninių duomenų netekimo nustatyti nepavyktų, nes duomenys lieka nukentėjusiajam (nors žalos konfidencialumui yra padaryta).

Nei baudžiamosios teisės doktrinoje, nei teismų praktikoje kol kas aiškiai neapibrėžtas elektroninių duomenų pasisavinimo požymis suteikia galimybę bendriausia prasme diskutuoti dėl keleto jo aiškinimo būdų. Pavyzdžiui, *pirma*, laikantis gana plataus požiūrio pasisavinimas galėtų būti inkriminuojamas tais atvejais, kai neviešus elektroninius duomenis neteisėtai gauna asmuo, kuriam buvo suteikta prieigos prie jų teisė. Kadangi tokiu būdu gaunant elektroninius duomenis nepadaroma neigiamo poveikio pirminiam jų šaltiniui, tai šie duomenys lieka nepakitę, nors kartu ir atitenka kaltininkui; *antra*, gana siauras požiūris į elektroninių duomenų pasisavinimą būtų artimesnis turto pasisavinimo aiškinimui. Tada pasisavinimas inkriminuotinas nustačius, kad kaltininkas priklausė tai kategorijai asmenų, kurie yra tiesiogiai atsakingi už elektroninių duomenų kaip pirminio šaltinio tvarkymą. Pačiai žalai būdingas toks duomenų netekimas, kai elektroniniai duomenys lieka tik kaltininkui. Be to, neatmestinos ir kitos galimos specialaus subjekto bei žalos kilimo, arba priešingai – jos kaip požymio atsisakymo, variacijos.

Neviešų elektroninių duomenų pasisavinimui dėl šių duomenų ypatybių tradicinis turto pasisavinimo suvokimas gali būti taikomas tik tiek, kiek tai padeda atskleisti pačią pasisavinimo veikos esmę. Atsisakius elektroninei erdvei sunkiai pritaikomų kriterijų, apie elektroninių duomenų pasisavinimą galima būtų kalbėti kaip apie neteisėtą kaltininko tapimą faktiniu neviešų elektroninių duomenų turėtoju, kai jam konkrečiomis sąlygomis buvo suteikta prieigos prie tokių duomenų teisė.

---

džiamųjų bylų skyriaus teisėjų kolegijos 2009 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-76/2009.

2.2.6. Paskleidimas

Apibūdindamas neteisėtus neviešų elektroninių duomenų perdavimo kitiems asmenims veiksmus, įstatymų leidėjas į analizuojamos nusikalstamos veikos sudėtį įtraukė duomenų paskleidimo požymį. Atsižvelgiant į BK nuostatas matyti, kad tokia pavojinga veika, apibūdinanti BK informacijos kaip nusikalstamos veikos dalyko atskleidimo veiksmus, nėra vienintelė. Dėl to pagal savo prasmę artimi paskleidimui galėtų būti laikomi šie požymiai: informacijos perdavimas (BK 119, 210, 217, 296 straipsniai), atskleidimas (125, 211, 297 straipsniai), perleidimas (124 straipsnis), jos paskelbimas (168 straipsnis) ir kt. Be to, BK 198 straipsnio redakcijoje, galiojusioje iki 2007 metų, paskelbimas buvo minimas šalia kitų panašaus pobūdžio – informacijos paskelbimo ir platinimo – veikų. Tik po 2007 metų pakeitimų minėtiesiems kaltininko veiksmams apibūdinti buvo pasirinkta viena elektroninių duomenų paskleidimo veika, kuri, galima teigti, turėjo susieti visas įmanomas neteisėto duomenų perdavimo tretiesiems asmenims veikas.

Aiškinantis, koks turinys suteiktas elektroninių duomenų paskleidimo veikai, aktualu nustatyti, kokiuose kituose BK straipsniuose ji numatyta ir kaip yra interpretuojama palyginti su kitomis nusikalstamomis veikomis. Tokių nusikalstamų veikų BK nėra daug – tai šmeižimas (BK 154 straipsnis), melagingas pranešimas apie visuomenei gresiantį pavojų ar ištikusią nelaimę (BK 285 straipsnis) ir mirusiojo atminimo paniekinimas (BK 313 straipsnis). Nors išsamiausiai apie paskleidimo turinį kalbama analizuojant šmeižimo nusikalstamos veikos sudėties požymius, kartu galima matyti, kad tokia veika suvokiama panašiai kaip ir kitų minėtųjų nusikalstamų veikų atveju. Taigi paskleidimas bendriausia prasme suvokiamas kaip informacijos pranešimas bent vienam kitam asmeniui, neatsižvelgiant į kaltininko pasirinktą tokio pranešimo būdą. Taip paskleidimą apibūdino ir BK 154 straipsnį komentavę autoriai. Anot jų, paskleidimas – tai „informacijos pranešimas kuriuo nors būdu bent vienam asmeniui, išskyrus nukentėjusįjį“[482]. Panašių nuomonių apie platinimą yra pareiškę ir kiti mokslininkai. Anot jų, platinimu yra laikomas informacijos pranešimas „bent vienam pašaliniam asmeniui, nepriklausomai nuo to, ar

[482] Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 196.

šis pranešimas buvo išplatintas toliau“[483], ar nukentėjusysis dalyvavo tokių kaltininko veiksmų metu[484], taip pat neatsižvelgiant į pasirinktą tokių veiksmų atlikimo būdą[485] (beje neretai minimas ir informacijos platinimas elektroninėje erdvėje). Žvelgiant į platesnį paskleidimo teisinį kontekstą matyti, kad paskleidimo veiksmai taip suvokiami ne tik baudžiamosios, bet ir civilinės teisės doktrinoje. Joje paskleidimas aiškinamas kaip „duomenų perdavimas bet kokiomis priemonėmis <...> bent vienam asmeniui, išskyrus tą, apie kurį tie duomenys skleidžiami“[486]. Patys paskleidimo būdai gali būti labai įvairūs: pranešimas vienam ar daugeliui asmenų pokalbio metu, sakant viešąją kalbą, per visuomenės informavimo priemones, paskleidžiant elektroninėje erdvėje, perduodant už atlygį arba be jo ir kt.

Toks turinys yra tinkamas ir paskleidimo veikai, numatytai neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtyje, bet šiam aiškinimui reikia ir patikslinimo dėl tam tikros paskleidimo specifikos elektroninėje erdvėje. Minėtosiose paskleidimo interpretacijose daugiau dėmesio skiriama aktyviems kaltininko veiksmams perduodant duomenis, bet neužsimenama apie kokias nors duomenų siūlymo apraiškas elektroninėje erdvėje. Tiksliau, kyla problema nustatant, ar paskleidimą reikėtų sieti tik su duomenų perdavimu (įvairiais būdais, pavyzdžiui, siunčiant elektroninėje erdvėje, perduodant įrašytus į laikmeną ar kt.), ar kaip tokia veika galėtų būti pripažįstamas ir duomenų padarymas prieinamais elektroninėje erdvėje (pavyzdžiui, juos paskelbiant tinklalapyje, padarant prieinamus per P2P kompiuterių tinklą ir kt.). Toks kaltininko veiksmų atskyrimas literatūroje dažniausiai analizuojamas iš neteisėto turinio medžiagos

---

483 Kurs ugolovnogo prava: uchebnik [The course of criminal law: The textbook]. Kuznecoba, N. F.; Tjazhkova, I. M. (red). Moskva: Zercalo-M, 2002, p. 233.

484 Naumov, A. V. Rossijskoe ugolovnoe pravo: kurs lekcij [Russian criminal law: the course of lectures]. 4-asis leidimas. Moskva: Volters Kluver, 2007, p. 154.

485 Ugalovnoe pravo Rossijskoj Federacii. Osobennaja chast: uchebnik [Criminal Law of the Russian Federation. Special Part: The textbook]. Inogamova-Khega, L. V.; Rarog, A. I.; Chuchaeva, A. I. (red.) Moskva: INFRA-M: KONTRAKT, 2005, p. 98; Rossijskoe ugolovnoe pravo: v dvukh tomakh: uchebnik [Russian criminal law: In two volumes: The textbook]. 5-asis pataisytas ir papildytas leidimas. Rarog, A. I. (red). Moskva: Proftekhobrazobanie, 2005, p. 107.

486 Mikelėnas, V., *et al*. Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. Asmenys. Vilnius: Justitia, 2002, p. 66.

platinimo pozicijų, bet ši problema išlieka aktuali ir nagrinėjant BK 198 straipsnyje numatytą nusikalstamą veiką. Pirmuoju atveju kaltininko veiksmai yra labiau siejami tarsi su informacijos „stūmimu“ iš siuntėjo šios informacijos gavėjui, o antruoju – „procesas yra panašesnis į gavėjo informacijos traukimą iš siuntėjo“[487]. Šis skirtumas leidžia nustatyti atskirus „stūmimo“ ir „traukimo“ duomenų perdavimo būdus (angl. *push and pull techniques)*[488]. Akivaizdu, kad duomenų „stūmimo“ veiksmai rodo aktyvią kaltininko veiką paskleidžiant elektroninius duomenis, o galimybių prieiti prie duomenų suteikimas yra susijęs su pasyviu kaltininko elgesiu, kai „traukimo“ veiksmus atlieka elektroninių duomenų gavėjas.

Analizuojant elektroninių duomenų paskleidimą remiantis BK 198 straipsniu, reikėtų pripažinti, kad tokiai veikai, nesiaurinant paskleidimo turinio, turėtų būti priskiriami abu minėtieji atvejai. Vadinasi, neatsižvelgiant į tai, kuris – siuntėjas ar gavėjas – inicijavo duomenų perdavimo procesą, ir aktyvūs duomenų perdavimo veiksmai (konkrečiam asmeniui ar neapibrėžtai jų grupei), ir sąlygų prieiti prie duomenų sudarymas turėtų būti pripažįstami paskleidimu. Apie tokią interpretavimo galimybę literatūroje užsimenama ir komentuojant BK 198 straipsnį: „elektroninių duomenų paskleidimas reiškia elektroninių duomenų teikimą viešumai, jų garsinimą ir darymą žinomais arba bet kokį perdavimą kitiems asmenims.“[489] Kartu pripažįstama ir tai, kad paskleidimu turėtų būti laikomas ir „elektroninių duomenų <...> patalpinimas į vietas (pavyzdžiui, tinklalapį internete), iš kur jie tampa prieinami kitiems asmenims (tai apima ir nuorodų į tokias vietas kūrimą <...> siekiant palengvinti priėjimą prie šių duomenų)“[490]. Beje, tokių elektroninio paskleidimo vertinimo tendencijų matyti ir teismų praktikoje – joje paskleidimu laikomi ne tik aktyvūs kaltininko veiksmai neteisėtai perduodant duomenis tretiesiems asmenims, bet ir sąlygų, leidžiančių peržiūrėti duomenų turinį, sudarymas juos

---

[487] Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007, p. 183.

[488] Cybercrime and Jurisdiction: a global survey. Koops, B. J., Brenner, S. (eds). The Hague: T.M.C. Asser Press, 2006, p. 198–201.

[489] Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009, p. 433.

[490] *Ibidem*.

paskelbiant elektroninėje erdvėje. Pavyzdžiui, vienoje iš baudžiamųjų bylų paskleidimo veiksmas buvo atliktas perduodant išspausdintus Valstybinės mokesčių inspekcijos kompiuterinės duomenų bazės išrašus (pažymas) trečiajam asmeniui[491]. Dar vienas sąlygų prieiti prie elektroninių duomenų sudarymo pavyzdys galėtų būti neviešų elektroninių duomenų apie bendrovėje kilusį gaisrą paskelbimas interneto tinklalapyje: <*http://rutube.ru*>[492]. Beje, minėtuoju atveju nustatant veikos baigtumo momentą įtakos neturėtų daryti tai, ar nors vienas žmogus spėjo peržiūrėti neviešus elektroninius duomenis.

2.2.7. Kitoks panaudojimas

Į neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėtį kaip alternatyvą įtraukus kitokio neviešų elektroninių duomenų panaudojimo požymį šiai nusikalstamai veikai suteikta plati apibrėžtis – minėtasis požymis rodo nebaigtinį neteisėto disponavimo elektroniniais duomenimis veikų sąrašą. Remiantis jo formuluote galima teigti, kad tokia veika itin dažnai gali būti vertinama kaip kitų nusikalstamų veikų padarymo būdas, pavyzdžiui, jei neteisėtai naudojantis neviešais elektroniniais duomenimis yra sukčiaujama (BK 182 straipsnis), neteisėtai prisijungiama prie informacinės sistemos (elektroninės bankininkystės sistemos, elektroninio pašto ar pan.) ir daugeliu kitų atvejų. Pavyzdžiui, vienoje iš baudžiamųjų bylų kaip neteisėtas elektroninių duomenų panaudojimas pripažintas banko naudotojo ID, banko slaptažodžio ir banko kodo panaudojimas prisijungiant prie elektroninės bankininkystės sistemos. Šioje baudžiamojoje byloje teismas konstatavo, kad kaltininkas padarė įvairias nusikalstamas veikas, numatytas (BK 198 straipsnio 1 dalyje, 300 straipsnio 1 dalyje, 182 straipsnio 1 dalyje, 215 straipsnio 1 dalyje), bet lieka neaišku, kodėl kaltininkui nebuvo inkriminuota BK 198[1] straipsnyje numatyta neteisėto prisijungimo prie informacinės sistemos nusikalstama veika[493]. Nors kitoks neviešų elektroninių duomenų panaudojimo

[491] Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-617-885/2011.

[492] Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendis baudžiamojoje byloje Nr. 1-188-785/2009.

[493] Šilalės rajono apylinkės teismo 2010 m. lapkričio 4 d. baudžiamasis įsakymas byloje Nr. 1-121-799/2010.

požymis yra tiesiogiai numatytas BK 198 straipsnio dispozicijoje, literatūroje pasitaiko nuomonių, kad pagal dabartinį teisinį reguliavimą baudžiamoji atsakomybė nekyla, pavyzdžiui, už veiksmus, „kai asmuo, neteisėtai panaudodamas prisijungimo duomenis, neteisėtai prisijungė prie kito asmens *Facebook* profilio ir šio asmens vardu per šį profilį pradėjo platinti seksualinio pobūdžio informaciją“[494]. Su tokia pozicija nelengva sutikti, nes, be kita ko, baudžiamoji atsakomybė už neteisėtą prisijungimą prie informacinės sistemos yra numatyta BK 198[1] straipsnyje.

Vadinasi, problemų analizuojant kitokio neviešų elektroninių duomenų panaudojimo veiką turėtų kilti ne tik dėl to, ar ji gali būti inkriminuojama kaltininkui panaudojus duomenis darant kitas nusikalstamas veikas, bet ir sprendžiant baudžiamojo įstatymo normos visumos bei normos-dalies konkurencijos įveikimo klausimą. Šis klausimas aktualus dėl to, kad kitokio neviešų elektroninių duomenų panaudojimo veika neretai gali tapti kitų nusikalstamų veikų padarymo būdu. Baudžiamosios teisės doktrinoje laikomasi bendros nuomonės, kad nusikalstamos veikos yra vertinamos pagal jų sutaptį, jeigu į visumą įtraukta dalis yra pavojingesnė nei pati visuma. Teigiama, kad tokiais atvejais „ji negali būti aprėpta tokios visumos ir turi būti kvalifikuota atskirai, t. y. pagal dviejų arba daugiau nusikaltimų sutaptį“[495]. Šį normų konkurencijos įveikimo klausimą sprendžiant elektroninių nusikalstamų veikų srityje, neišvengiamai tenka atkreipti dėmesį ir į neteisėto elektroninių duomenų perėmimo bei panaudojimo nusikalstamos veikos baudžiamumą. BK 198 straipsnio 1 dalies sankcijoje numatyta maksimali ketverių metų laisvės atėmimo bausmė, atitinkamai šioje dalyje nustatyta nusikalstama veika yra priskiriama apysunkių nusikaltimų kategorijai (BK 11 straipsnio 4 dalis). Vadinasi, praktikoje gali pasitaikyti atvejų, kai neteisėto neviešų elektroninių duomenų panaudojimo veika turės būti inkriminuojama su kitomis kaltininko padarytomis veikomis pagal sutaptį. Pavyzdžiui, sprendžiant minėtojo neteisėto prisijungimo prie informacinės sis-

[494] Štitilis, D., *et al*. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai. Vilnius: Mykolo Romerio universitetas, 2011, p. 260.

[495] Pavilonis, V. Baudžiamosios teisės normų konkurencija. *Teisės problemos*, 1996, 2(12): 45.

temos (BK 198[1] straipsnis) ir kitų nusikalstamų veikų, kurios buvo padarytos neteisėtai panaudojant neviešus elektroninius duomenis, inkriminavimo klausimus. Šiais atvejais iš tiesų gali kilti dilema, ar tokio teisinio reguliavimo nelemia netinkamas baudžiamojo įstatymo normų suderinamumas ir ar tikrai įstatymų leidėjas siekė nustatyti būtent tokias plačias BK 198 straipsnio taikymo galimybes.

2.2.8. Pavojingų veikų neteisėtumo vertinimas

Lietuvos BK neteisėtas disponavimas neviešais elektroniniais duomenimis nėra susijęs su neteisėta prieiga prie informacinės sistemos, šios nusikalstamos veikos kaip atskiros yra kriminalizuotos skirtinguose BK 198 ir 198[1] straipsniuose. Nors neteisėta prieiga prie informacinės sistemos dažniausiai lemia ir neteisėtą prieigą prie joje laikomų duomenų, kita vertus, teisėta prieiga prie sistemos neleidžia iš anksto preziumuoti, kad šioje sistemoje nebuvo padaryta neviešų elektroninių duomenų konfidencialumo pažeidimų. Dėl tokio įstatymo leidėjo požiūrio galima atskirti elektroninių duomenų ir informacinės sistemos konfidencialumo pažeidimus, vadinasi, galima pritarti ir literatūroje išsakomai nuomonei, kad „tose jurisdikcijose, kuriose dėmesio centre yra prieiga prie duomenų, leistinumo klausimas turėtų būti užduodamas dėl kiekvienos tokios prieigos“[496].

Iš BK 198 straipsnyje pateikiamo elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos aprašymo matyti, kad BK konfidencialumo pažeidimai, atliekant įvairius neteisėtus veiksmus su neviešais elektroniniais duomenimis, yra gana plačiai kriminalizuoti. Toks nusikalstamos veikos sudėties požymių aprašymas galėjo būti pasirinktas dėl to, kad pati „informacinio privatumo“[497] sritis (taip ji įvardijama literatūroje) yra gana plati, dėl to atsiranda galimybė analizuoti įvairius neteisėtus veiksmus, kuriais nesilaikoma nustatytų disponavimo neviešais elektroniniais duomenimis įpareigojimų. Vadinasi, prie tokių apribojimų bendriausia prasme gali būti priskiriami reikalavimai susilaikyti nuo mėginimų sužinoti neviešus elektroninius duomenis, neatskleisti jų kitiems ir kt. Atsižvelgiant į tai,

[496] Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010, p. 76.

[497] Manson, N. C.; O'Neill, O. Rethinking Informed Consent in Bioethics. Cambridge, *et al*. Cambridge University Press, 2007, p. 98.

BK 198 straipsnio dispozicijoje įtvirtinta nemažai alternatyvių pavojingų veikų, kuriomis pažeidžiami nustatyti apribojimai įvairiose duomenų tvarkymo etapuose: stebėjimas, fiksavimas, perėmimas, įgijimas ir pasisavinimas kaip neviešų elektroninių duomenų neteisėtas gavimas; neviešų elektroninių duomenų laikymas; tokių duomenų paskleidimas kaip neteisėtas perdavimas kitiems asmenims ir kitoks duomenų panaudojimas. Nustatant šių pavojingų veikų neteisėtumą, kaip ir pačių pavojingų veikų įrodinėjimo atveju, galioja draudimas preziumuoti nusikalstamos veikos sudėties požymius – kiekvienos pavojingos veikos neteisėtumą būtina konstatuoti atskirai. Kaip minėta, BK 198 straipsnis yra siejamas ir su *informacinėje sistemoje laikomų* (*nejudamų*), ir *informacinėje sistemoje perduodamų* neviešų elektroninių duomenų konfidencialumo pažeidimais, vadinasi, neteisėtumą irgi galima analizuoti atskirai iš duomenų konfidencialumo ir komunikacijos konfidencialumo pozicijų.

Disponavimo neviešais elektroniniais duomenimis neteisėtumui būdinga tai, kad asmuo, gaudamas prieigą ar atlikdamas kitus veiksmus su neviešais elektroniniais duomenimis, neturi teisėto leidimo tokiems veiksmams. Kaip minėta, elektroniniai duomenys priskiriami neviešų duomenų kategorijai atsižvelgiant į daugelį aplinkybių, be kita ko, ir pačių duomenų rūšį. Be to, minėtosios aplinkybės svarbios nustatant, ar egzistavo asmens, gavusio duomenis ar atlikusio su jais tam tikrus veiksmus, ir duomenų subjekto įsipareigojimas išlaikyti elektroninių duomenų konfidencialumą. Toks bendrasis reikalavimas reikštų, kad asmuo, siekiantis gauti neviešus elektroninius duomenis ar atlikti su jais kitus disponavimo veiksmus, turėtų laikytis nustatytų reikalavimų, kokiu būdu jis gali gauti duomenis ir atlikti su jais susijusius veiksmus. Pavyzdžiui, teismų praktikoje neviešų *nejudamų* elektroninių duomenų konfidencialumo pažeidimai konstatuotini tuo atveju, kai nesilaikoma neviešų elektroninių duomenų disponavimo apribojimų, numatytų juridinių asmenų informacijos saugos politikos ir ją įgyvendinančiuose dokumentuose. Vienoje iš baudžiamųjų bylų nustatyta, kad R. R. buvo pasirašęs *pasižadėjimą „Dėl informacijos apdorojimo priemonių naudojimo sąlygų laikymosi“, kuriuo patvirtino, kad žino AB „(duomenys neskelbtini)“ informacijos saugos politiką bei ją įgyvendinančius dokumentus, nesilaikė pasižadėjimo ir pažeidė prisiimtus įsipareigojimus* <...>. Be to, byloje konstatuota,

kad R. R., pažeisdamas prisiimtus įsipareigojimus[498], *iš įrašymo įrenginio ir šiame įrenginyje esančio vaizdo archyvo, bylos „Incident2“, kuriame buvo aplankalas „Footage“ su jame esančiu vaizdo įrašu pavadinimu „Kaminasl_10.119.11.14_2009-05-24_19-14-00(l).mpeg4“, nukopijavo ir į išorinę įrašymo laikmeną neteisėtai įsirašė „Vidinio naudojimo“, pagal nutylėjimą priskirtą informaciją apie AB „(duomenys neskelbtini)“ <...> įvykusį gaisrą, taip neteisėtai įgijo neviešus elektroninius duomenis, juos pasisavino, laikė, tai yra turėjo su savimi ir <...> šiuos neteisėtai įgytus, laikytus ir pasisavintus neviešus elektroninius duomenis apie AB „(duomenys neskelbtini)“ kilusį gaisrą paskleidė interneto puslapyje <...>*[499]. Atsižvelgdamas į tai, teismas padarė išvadą, kad R. R. nusikalstama veika kvalifikuotina pagal BK 198 straipsnio 1 dalį. Taigi remiantis besiformuojančia teismų praktika galima teigti, kad kaltininko veiksmų neteisėtumas dažniausiai nustatomas tada, jei su neviešais elektroniniais duomenimis buvo atliekami veiksmai pažeidžiant nustatytą tokio pobūdžio duomenų disponavimo tvarką.

Analizuojant neteisėtumą kitu – elektroninių ryšių konfidencialumo pažeidimų požiūriu, tampa aktualūs Konvencijos dėl elektroninių nusikaltimų 3 straipsnio, Direktyvos 2013/40/ES 6 straipsnio nuostatos ir Konvencijos aiškinamojoje ataskaitoje pateikiami išaiš-

---

[498] Pavyzdžiui, „skaityti, keisti, įtraukti, kopijuoti ar ištrinti AB „(duomenys neskelbtini)“ duomenis, tik kai tai susiję su darbo funkcijomis“ 7 punktą, „neperžiūrinėti duomenų, esančių AB „(duomenys neskelbtini)“ informaciniuose ištekliuose, jeigu tai nesusiję su priskirtų funkcijų ar pareigų vykdymu“ 8 punktą, „neteikti pašaliniams asmenims ar su tokia informacija susipažinti neturintiems teisės AB „(duomenys neskelbtini)“ darbuotojams AB „(duomenys neskelbtini)“ informacinėse sistemose esančios informacijos, nebent to reikalauja darbo funkcijos, nustatyta vidaus darbo tvarka ar tai įpareigotų daryti taikomi teisės aktai“ 9 punktą, be to, pažeisdamas AB „(duomenys neskelbtini)“ informacijos saugos politikos 11.2.2 punktą, kuriuo nustatyta, kad „AB „(duomenys neskelbtini)“ informaciniai ištekliai yra skirti naudoti tik AB „(duomenys neskelbtini)“ verslo tikslais“ bei 7.5.1 punktą, kuriuo „turi būti užtikrinta, kad be leidimo informacija nebus perduota (išsiųsta) už Bendrovės ribų. Tretieji asmenys (rangovai), kurių paslaugoms (prekėms) teikti (tiekti, gauti) yra reikalinga Bendrovės informacija, turi būti sudarę su bendrove atitinkamas informacijos neatskleidimo ir (ar) konfidencialumo sutartis, arba kitokia forma prisiėmę atitinkamus įsipareigojimus. Tokiuose susitarimuose turėtų būti numatytos informacijos saugos sąlygos ir taikoma atsakomybė“.

[499] Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendis baudžiamojoje byloje Nr. 1-188-785/2009.

kinimai. Aiškinamojoje ataskaitoje pabrėžiama, kad baudžiamoji atsakomybė už kompiuterinių duomenų perimtį kyla tada, kai tokia veika yra padaroma tyčia ir neturint teisės atlikti tokius veiksmus. Patys perėmimo veiksmai gali būti ir leistini, pavyzdžiui, jei duomenis perimantis asmuo turi teisę tokius veiksmus atlikti, jeigu jis veikia remdamasis nurodymais arba suteiktais įgaliojimais (įskaitant įgaliotą testavimą arba apsaugos veiksmus) arba kai sekimas yra sankcionuotas atsižvelgiant į nacionalinį saugumą ar yra atliekamas tyrimo subjektų siekiant atskleisti nusikalstamas veikas (58 punktas). Beje, tokios elektroninių duomenų perėmimo teisėtumo sąlygos numatomos ir nacionaliniuose teisės aktuose, pavyzdžiui, Lietuvos Respublikos baudžiamojo proceso kodekso[500] nuostatose, reglamentuojančiose kitų procesinių prievartos priemonių taikymą (pavyzdžiui, elektroninių ryšių tinklais perduodamos informacijos kontrolę, jos fiksavimą ir kaupimą (154 straipsnis). Teisėtumo sąlygos nustatomos ir Lietuvos Respublikos kriminalinės žvalgybos įstatyme[501], kurio 10 straipsnyje numatyta susirašinėjimo ir kitokio susižinojimo slaptos kontrolės atlikimo tvarka. Be to, svarbu atkreipti dėmesį į tai, kad neviešų elektroninių duomenų perėmimo sąlygos gali būti numatomos ir sudarant įvairius komunikavimo dalyvių susitarimus, pavyzdžiui, jei elektroninių duomenų perėmimas vyksta testuojant informacinės sistemos veiklą, ieškant sistemos saugumo silpnųjų vietų ir kt. Vadinasi, neviešų elektroninių duomenų perėmimo neteisėtumą rodo tai, kad padaryti veiksmai neatitinka jiems atlikti nustatytų teisėtumo kriterijų. Draudimas neturint faktinių elektroninių ryšių paslaugų vartotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti pranešimų turinį ir srauto duomenis ar juos peržiūrėti bei atskleisti arba sudaryti sąlygas tokius duomenis gauti yra suformuluotas Elektroninių ryšių įstatymo 61 straipsnyje (išskyrus jame konkrečiai nurodytus atvejus). Šiais draudimais siekiama apsaugoti ryšio slaptumą, dėl kurio nepaisymo sudaromos sąlygos pažeisti ir neviešų informacinėje sistemoje perduodamų elektroninių duomenų konfidencialumą.

[500] *Valstybės žinios*, 2002, Nr. 37-1341.

[501] *Valstybės žinios*, 2012, Nr. 122-6093.

2.3. Nusikalstamą veiką kvalifikuojantys požymiai

Elektroninius duomenis apibūdinantis požymis – jų strateginė reikšmė nacionaliniam saugumui ar didelė reikšmė valstybės valdymui, ūkiui ar finansų sistemai – rodo didesnę neviešų elektroninių duomenų svarbą ir yra taikomas BK 198 straipsnio 2 dalyje konstruojant kvalifikuotą neteisėto disponavimo elektroniniais duomenimis nusikalstamos veikos sudėtį. Tokio sudėties požymio konstrukcija, kaip ir analogiškai BK 198[1] straipsnio 2 dalyje apibūdintos informacinės sistemos atveju, leidžia nustatyti ne tik *technologinį*, bet ir *teisinį* nusikalstamos veikos dalyko aspektą. Elektroninių duomenų požymis, dėl kurio kyla technologijų ir terminologijos klausimas, buvo ir anksčiau analizuojamas, todėl daugiausia dėmesio reikėtų skirti jo teisiniam aspektui – strateginei reikšmei nacionaliniam saugumui ir didelei reikšmei valstybės valdymui, ūkiui ar finansų sistemai.

Dėl pasirinkto nusikalstamų veikų elektroninių duomenų ir informacinės sistemos konfidencialumui kriminalizavimo būdo, kai baudžiamoji atsakomybė už neviešų elektroninių duomenų ir informacinių sistemų konfidencialumo pažeidimus yra numatyta skirtinguose BK 198 ir 198[1] straipsniuose, būtina atskirti ypatingą reikšmę turinčias informacines sistemas nuo ypatingos reikšmės elektroninių duomenų. Dėl to didesnė ir sistemos, ir elektroninių duomenų reikšmė, remiantis esamu nusikalstamų veikų aprašymu, turėtų būti įrodinėjama atskirai. Jeigu informacinė sistema pripažįstama kaip turinti strateginės reikšmės nacionaliniam saugumui arba didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai, tai joje tvarkomi duomenys dažniausiai irgi gali turėti didesnę reikšmę nurodytoms sritims. Nors tokiais atvejais kyla problema, ar galima taikyti prezumpciją, kad *visi* ypatingos svarbos informacinėje sistemoje tvarkomi duomenys irgi turi didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai, o jų konfidencialumo pažeidimai yra kriminalizuoti BK 198 straipsnio 2 dalyje. Kaip minėta, pati informacinė sistema, kai į ją žvelgiama plačiau, t. y. kartu su jos taikomuoju aspektu, yra skirta įvairiems organizacijos tikslams pasiekti, numatytoms funkcijoms atlikti, taigi ir tam tikro darinio funkcionavimui užtikrinti, todėl šioje sistemoje gali būti apdorojami įvairiausios reikšmės duomenys net ir tuo atveju, jei pati informacinė sistema yra ypatingos svarbos. Dėl to galima teigti, kad neteisėtas prisijungimas prie informacinės sistemos,

atitinkančios BK 198[1] straipsnio 2 dalyje numatytus požymius, ne visais atvejais leidžia kalbėti apie didesnę reikšmę turinčių elektroninių duomenų konfidencialumo pažeidimus – duomenų, kuriais buvo neteisėtai disponuojama, reikšmė turėtų būti įvertinama atskirai. Atitinkamai ypatingos reikšmės informacinės sistemos konfidencialumo pažeidimai gali būti laikomi tik viena iš vertintinų, bet ne lemiamą reikšmę turinčių aplinkybių, kai duomenys pripažįstami nusikalstamos veikos dalyku, numatytu BK 198 straipsnio 2 dalyje.

Strateginės reikšmės nacionaliniam saugumui, didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai turinčių elektroninių duomenų interpretavimą pasunkina tai, kad nei doktrinoje, nei nacionaliniuose teisės aktuose, nei teismų praktikoje nepateikiama aiškių kriterijų, kaip nustatyti tokio pobūdžio duomenis. Lingvistinis BK 198 straipsnio 2 dalyje vartojamų terminų aiškinimas yra neinformatyvus, pavyzdžiui, viena iš žodžio *strateginis* reikšmių, ją susiejus su elektroniniais duomenimis, bendriausia prasme leidžia kalbėti apie suteikiančius pranašumą[502] elektroninius duomenis arba esminius, svarbius bendriesiems kovos tikslams pasiekti[503] duomenis. Nacionaliniuose teisės aktuose taip pat pateikiami tik bendrojo pobūdžio informacinių išteklių skirstymai į rūšis ir nustatomas gana abstraktus tokio skirstymo kriterijus. Pavyzdžiui, analizuojant valstybės informacines sistemas ir informacinius išteklius, galima pateikti Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo[504] 3 straipsnį, kuriame nurodomos valstybės informacinių išteklių rūšys: ypatingos svarbos, svarbūs, žinybinės svarbos ir kiti valstybės informaciniai ištekliai. Toks skirstymas yra pagrįstas gana abstrakčiu grupavimo kriterijumi, t. y. kiek valstybės informacinės sistemos apdorojama informacija yra svarbi. Ypatingos svarbos valstybės informaciniai ištekliai yra siejami su visai valstybei svarbia informacija, svarbūs valstybės informaciniai ištekliai – su kelioms institucijoms svarbia informacija, o žinybinės svarbos – su vienai institucijai svarbia informacija, bet pačios informacijos svarbos vertinimo kriterijai šiame įstatyme nepateikiami.

---

[502] Khokins, Dzh. M. The Oxford Dictionary of the English Language. Moskva: OOO «Izdatelstvo Actrel», OOO «Izdatelstvo AST», 2001, p. 704.

[503] Tarptautinių žodžių žodynas. Bendorienė, A., *et al*. (sud.); Kinderys, A. (ats. red.). Vilnius: Alma littera, 2001, p. 707.

[504] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. *Valstybės žinios,* 2011, Nr. 163-7739.

Viena vertus, galima pritarti tokiai interpretavimo laisvei, nes ypatingos svarbos elektroninių duomenų suvokimas laikui bėgant gali keistis. Kaip buvo pabrėžta analizuojant kritines informacines sistemas, ypatinga svarba visada yra susijusi su perspektyvos klausimu. Kita vertus, dėl tokio lankstaus nusikalstamos veikos dalyko aiškinimo kyla ir tam tikrų abejonių, kokie duomenys priskirtini strateginės reikšmės nacionaliniam saugumui, didelės reikšmės valstybės valdymui, ūkiui ar finansų sistemai turintiems elektroniniams duomenims. Vienas iš šios problemos sprendimo būdų – kaip orientacinius kriterijus *mutatis mutandis* taikyti tuos, kuriais leidžiama spręsti apie ypatingą sistemos svarbą atitinkamoms BK 198[1] straipsnio 2 dalyje nurodytoms sritims. Vadinasi, remiantis *nukentėjusiųjų*, *ekonominio poveikio* ir *poveikio visuomenei* kriterijais, bendriausia prasme būtų galima atsižvelgti į potencialių nukentėjusiųjų skaičių, žalos dydį, ekonominius nuostolius, poveikį visuomenės pasitikėjimui ir kita.

Sprendimas, ar elektroniniai duomenys yra itin svarbūs sritims, nurodytoms BK 198 straipsnio 2 dalyje, galėtų būti susijęs ne tik su duomenų turiniu, bet ir su jų kiekiu. Tam tikrais atvejais atsižvelgiant į neviešų elektroninių duomenų kiekį galima nustatyti, kad pavieniai duomenys, kurie dėl savo turinio nelaikomi ypatingos svarbos, šią savybę įgyja dėl neteisėto disponavimo tokiais duomenimis kiekio. Pavyzdžiui, svarstytina, ar nereikėtų pripažinti, kad didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turi Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos duomenų bazėje esantys duomenys apie fizinius asmenis (asmens darbovietė, pajamos, išduoti asmens tapatybės dokumentai ir kt.), jei buvo nustatytas neteisėto disponavimo itin dideliu ir per ilgesnį laiką sukauptu tokių elektroninių duomenų kiekiu atvejis. Be to, ar neteisėtu disponavimu ypatingos svarbos duomenimis negalėtų būti pripažintas disponavimas itin dideliu ir per ilgesnį laiką sukauptu elektroninių duomenų, esančių *Sodros* centrinėje klientų duomenų bazėje, kiekiu. Analizuojant teismų praktiką matyti, kad tokių atvejų kol kas nepasitaikė, nors neteisėtas disponavimas minėtaisiais duomenimis konstatuotas Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. baudžiamajame įsakyme baudžiamojoje byloje Nr. 1-617-885/2011 ir Vilniaus miesto 1 apylinkės teismo 2008 m. rugsėjo 5 d. nuosprendyje baudžiamojoje byloje Nr. 1-17-296/2008. Šiaulių

miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamajame įsakyme baudžiamojoje byloje Nr. 1-617-885/2011 nustatyta, kad V. Š. neteisėtai disponavo Valstybinės mokesčių inspekcijos duomenų bazėje kaupiamais duomenimis apie fizinius asmenis – jis įsigijo ir paskleidė duomenis apie dvidešimt du fizinius asmenis. Manytina, kad tokia V. Š. veika pagrįstai kvalifikuota pagal BK 198 straipsnio 1 dalį, nes tokio elektroninių duomenų kiekio nepakanka kalbėti apie tokių duomenų didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai. Kiek kitokia padėtis matyti Vilniaus miesto 1 apylinkės teismo 2008 m. rugsėjo 5 d. nuosprendyje baudžiamojoje byloje Nr. 1-17-296/2008, kuriame konstatuotas neteisėtas disponavimas *Sodros* centrinės klientų duomenų bazės 1999–2004 metų duomenimis. Ypatinga tokių elektroninių duomenų reikšmė šioje byloje dėl nusikalstamos veikos padarymo metu (2003–2004 metais) galiojusio BK negalėjo būti vertinama, nes BK 198 straipsnyje dar nebuvo numatyta tokia veiką kvalifikuojanti aplinkybė.

3. Subjektyvieji neteisėto elektroninių duomenų perėmimo ir panaudojimo sudėties požymiai

Ankstesniuose skyriuose atkreiptas dėmesys į tai, kad nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumo inkriminavimo apribojimus rodo ne tik objektyvieji, bet ir subjektyvieji požymiai, o tiksliau – tyčinės kaltės nustatymo reikalavimas. Į tokio pobūdžio nusikalstamų veikų sudėtis įtraukus tik tyčinę kaltės formą, išvengiama jų, kaip „sugaunančių viską“[505] – nuo pavojingo iki bet kokio netinkamo elgesio su informacinėmis technologijomis – konstrukcijos. Ne išimtis ir neteisėto elektroninių duomenų perėmimo bei panaudojimo nusikalstama veika – dėl tyčinės kaltės požymio apribojamos baudžiamosios atsakomybės taikymo galimybės, *pirma,* kai dėl netinkamo taikomų informacinių technologijų funkcionavimo gaunama nenumatytų jų veiklos rezultatų; *antra*, kai atliekami teisėti informacinės sistemos testavimo veiksmai, siekiant nustatyti jos saugumo silpnąsias vietas.

[505] Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum,* 2011, 22: 167.

Vertinant minėtuosius ir panašius atvejus iš baudžiamosios teisės pozicijų, aktualios tampa svarbiausios baudžiamosios atsakomybės nuostatos – tai, kad asmuo pagal baudžiamąjį įstatymą atsako tik tuo atveju, jei jis yra kaltas padaręs nusikalstamą veiką (BK 2 straipsnio 3 dalis) ir kad baudžiamoji atsakomybė galima tik tuo atveju, jei padaryta veika atitinka baudžiamojo įstatymo numatytą nusikalstamos veikos sudėtį (BK 2 straipsnio 4 dalis). Dėl šių nuostatų probleminiais informacinių technologijų taikymo atvejais (pavyzdžiui, gavus nenumatytą jų veiklos rezultatą) atsiranda galimybė išvengti objektyvaus pakaltinimo, kai elektroninių duomenų konfidencialumo pažeidimų padaryta nesant šių technologijų vartotojo kaltės arba baudžiamosios atsakomybės taikymo veikoje nustačius kitą nei sudėtyje numatytą kaltės formą ir kita.

Pati kaltės formų apribojimo galimybė kildinama iš Konvencijos dėl elektroninių nusikaltimų 3 straipsnio, kuriame aprašant neteisėtos perimties nusikalstamą veiką tiesiogiai numatoma galimybė susiaurinti atsakomybę iki *sąmoningos* neteisėtos kompiuterinių duomenų perimties. Į šią baudžiamosios atsakomybės kilimo sąlygą atkreiptas dėmesys ir Konvencijos dėl elektroninių nusikaltimų aiškinamojoje ataskaitoje, kurioje teigiama, kad baudžiamoji atsakomybė už neteisėtą perimtį galima tada, jei neteisėta perimtis padaryta tyčia (58 punktas). Tik tyčinė kaltės forma numatoma ir Direktyvos 2013/40/ES 6 straipsnyje pateiktoje neteisėto duomenų perėmimo apibrėžtyje. Į tai atsižvelgdamas įstatymų leidėjas irgi numatė tik tyčinę kaltę BK 198 straipsnyje esančios neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos sudėtyje. Kadangi minėtajame straipsnyje nėra tiesioginių nuorodų į neatsargią kaltės formą, tai remiantis esamu baudžiamuoju teisiniu reguliavimu baudžiamoji atsakomybė už dėl neatsargumo padarytą tokio pobūdžio veiką yra negalima (BK 16 straipsnio 4 dalis). Į tai atkreiptas dėmesys ir teismų praktikoje nurodant, kad BK 198 straipsnyje *numatytas nusikaltimas padaromas tiesiogine tyčia, nes kaltininkas, paskleisdamas elektroninius duomenis, supranta, kad veikia neteisingai ir taip nori veikti*[506]. Vadinasi, konstatuojant tyčinę kaltę būtina nustatyti, kad kaltininkas suvokė, jog darydamas žalą elektroninių duomenų konfidencialumui neteisė-

[506] Kauno apygardos teismo 2017 m. rugsėjo 27 d. nuosprendis baudžiamojoje byloje Nr. N1-173-319/2017.

tai stebėjo, fiksavo, perėmė, įgijo, laikė, pasisavino, paskleidė ar kitaip panaudojo neviešus elektroninius duomenis ir norėjo taip veikti.

Kaip teigiama literatūroje, „<...> asmens, tyčia darančio nusikalstamą veiką, suvokimo dalykas yra <...> visi baudžiamojo įstatymo specialiosios dalies straipsnio dispozicijoje įvardyti objektyvieji požymiai ir iš įstatymo išplaukiančios jų ypatybės <...>“[507]. Taigi BK 198 straipsnio dispozicijoje tiesiogiai numačius elektroninių duomenų neviešumo ir alternatyvių pavojingų veikų neteisėtumo požymius tampa akivaizdu, kad tyčinė kaltė galėtų būti konstatuojama *inter alia* nustačius ir šių objektyviųjų požymių suvokimą. Beje, jei nusikalstama veika padaroma elektroninėje erdvėje, toks suvokimas turėtų būti vertinamas remiantis asmens patirtimi būtent šioje erdvėje.

Ankstesniuose skyriuose prieita prie išvados, kad i*nterneto kaip vietos* (angl. *Internet-as-place)* metafora ir *vidinės perspektyvos* pozicija bene geriausiai parodo, kaip elektroninės erdvės vartotojai įgyja patirties šioje erdvėje, suvokia įvairias jos vietas ir taikomus apribojimus. Šia, kaip ir literatūroje[508] minima kita – *informacijos kaip daikto* (angl. *Information-as-thing),* metaforomis gali būti remiamasi aiškinant prieigos prie elektroninių duomenų apribojimų (neteisėtumo ir duomenų neviešumo) numatomumą. Pati prieiga prie informacijos „<...> reiškia, kad egzistuoja prieigos tarpusavio santykių objektas, kažkas, kas gali būti gaunama“[509]. Siekiant šį santykį paaiškinti taikant fizinės erdvės analogiją, elektroniniai ištekliai, esantys virtualiojoje erdvėje arba tiksliau apčiuopiamoje informacinėje sistemoje (ar laikmenoje), bendriausia prasme metaforiškai prilyginami „daiktui“, prie kurio asmuo turi prieigą arba jos neturi, gali arba negali jo naudoti[510]. Dėl to prieigos prie elektroninių duomenų bei kitų veiksmų su jais atlikimo atveju, kaip ir esant prieigai prie materialaus daikto fizinėje erdvėje,

---

[507] Bikelis, S. Tyčinė kaltė baudžiamosios teisės teorijoje ir praktikoje: daktaro disertacija. Vilnius: Mykolo Romerio universitetas, 2007, p. 56.

[508] Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2): 438–446; Wong, M. W. S. Cyber-trespass and "Unauthorized Access" as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1): 102–103.

[509] Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2): 442.

[510] *Ibid*., p. 434.

svarbu nustatyti, ar elektroninių duomenų disponavimo apribojimai buvo tinkamai nurodyti ir leido elektroninės erdvės vartotojams suvokti, kad atliekant su jais tam tikrus veiksmus peržengiamos leidžiamos ribos. Reikėtų pripažinti, kad toks aiškių ribų nustatymo poreikis yra būtinas visų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui padarymo atvejais (pavyzdžiui, aiškinant neteisėto prisijungimo prie informacinės sistemos probleminius inkriminavimo aspektus, buvo svarbu aiškiai atskirti privačias ir viešąsias erdves). Toks aiškinimas yra gana natūralus, nes vartotojas elektroninę erdvę dažniausiai suvokia būtent kaip virtualiąją realybę ir jai taiko fizinės erdvės kriterijus – „mes gyvenam, suprantam ir kontroliuojam savo „vietas" mintyse sudarydami jų „žemėlapius", priklausančius nuo ribų, orientyrų, ir kitų matomų orientavimuisi svarbių vietų"[511]. Taigi suvokiant vietas ir erdvių ribas nesvarbu, kur – elektroninėje ar fizinėje erdvėje – asmuo atlieka veiksmus.

Aiškinant neteisėto elektroninių duomenų perėmimo ir panaudojimo subjektyviuosius požymius matyti, kad su tinkamų ribų nustatymu yra tiesiogiai susijusios galimybės įrodyti neviešų elektroninių duomenų ir kaltininko atliekamų veiksmų neteisėtumo suvokimą. Galima pritarti literatūroje išsakomai minčiai, kad „kol turimas faktines žinias, jog kaltininkas neturėjo leidimo, daugeliu atvejų yra sunku įrodyti, tol tai padės pabrėžti aiškių apribojimų nustatymo svarbą"[512]. Net ir tada, kai konstatuojama neteisėta prieiga prie neviešų elektroninių duomenų, baudžiamoji atsakomybė už tokią veiką yra galima tik tuo atveju, jei kaltininkas atpažino ir suvokė esamus apribojimus – šis aspektas siejamas su tyčinės kaltės nustatymo reikalavimu. Kaip matyti, atskiriant viešus ir neviešus elektroninius duomenis, teisėtus ir reikalavimų neatitinkančius veiksmus būtina, be kita ko, konstatuoti, ar elektroninės erdvės vartotojas buvo veiksmingai informuotas apie elektroninėje erdvėje esamas ribas.

Šiuo aspektu svarbus minėtasis nustatytų apribojimų numatomumo kriterijus, kuris leidžia į elektroninėje erdvėje nustatytas ribas pažvelgti iš jos vartotojo, elektroninę erdvę suvokiančio kaip virtualiąją

---

511 Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2): 437.

512 Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum,* 2011, 22: 167.

realybę, pozicijos. Pats numatomumo kriterijus bendriausia prasme reiškia idėją, kad siekiant nustatyti disponavimo elektroniniais duomenimis apribojimų, t. y. duomenims suteikti neviešų duomenų statusą, potencialūs pažeidėjai, vadovaujantis elektroninės erdvės kaip vietos metafora, turėtų būti veiksmingai informuojami, kad jų atliekamais veiksmais pažeidžiamas elektroninių duomenų konfidencialumas. Remiantis šiuo kriterijumi, atitinkamai reikia nustatyti, kad elektroninių duomenų buvimo aplinkoje buvo sukurtos „ryškios, matomos ribos tarp atviros, viešos informacijos ir informacijos, kuriai nustatyti prieigos apribojimai“[513]. Dėl pakankamo teisiškai reikšmingų apribojimų informatyvumo tampa lengviau įrodyti, kad nesilaikydamas aiškiai nustatytų ribų kaltininkas suvokė, jog jis nepaiso esamų apribojimų ir elgiasi neteisėtai. Priešingu atveju nustatyti apribojimai bus nepakankami, nesuteikiantys jokios prasmingos informacijos elektroninės erdvės vartotojui, taigi žvelgiant iš *vidinės perspektyvos* pozicijų šie apribojimai nedarys įtakos jo patyrimui bei atliekamų veiksmų suvokimui elektroninėje erdvėje.

Nors prieigos prie neviešų elektroninių duomenų apribojimų gali būti įvairių, bet visi jie rodo priemones, kurių buvo imtasi elektroninių duomenų konfidencialumui užtikrinti. Tokiais atvejais kartu taikomos ir teisinės, ir techninės priemonės „suteikia galimybių interneto vartotojams nustatyti privatumo ir saugumo zoną, apsaugotą nuo pašalinių įsikišimo“[514]. Pavyzdžiui, vienas iš neviešų elektroninių duomenų konfidencialumo nesant asmens kaltės pažeidimo atvejų pasitaiko tada, kai dėl priemonių, kuriomis nustatoma tam tikrų apribojimų, netinkamo veikimo suteikiama prieiga prie minėtųjų duomenų, sudaromos sąlygos peržiūrėti jų turinį, daryti tokių duomenų kopijas ir pan. Tokią situaciją padeda apibūdinti minėtoji dilema, ar naudojantis informacinėmis technologijomis nusikalstama veika buvo padaryta tyčia, ar vis dėlto sąlygos pažeisti elektroninių duomenų konfidencialumą atsirado dėl nenumatytų pačių technologijų veiklos sutrikimų. Nustačius, kad asmens veiksmais nebuvo iškreiptos programinės įrangos atliekamos funkcijos, jis nesiekė pažeisti

[513] Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2): 491.

[514] Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *NYU Law Review*, 2003, 78(5): 1650.

nustatytų apribojimų, o tik naudojosi programinės įrangos suteiktomis galimybėmis pagal paskirtį (numatytas funkcijas), jo veiksmuose nebus įmanoma nustatyti kaltės. Jei prieiga prie neviešų elektroninių duomenų suteikiama dėl netinkamo programinės įrangos veikimo, žiūrint iš *vidinės perspektyvos*, elektroninės erdvės vartotojui nustatyti prieigos apribojimai nebus suvokiami, tokie apribojimai neatitiks jų numatomumo kriterijaus, atitinkamai nebus suvoktas ir pats atliktų veiksmų neteisėtumas. Dėl to akivaizdu, kad tokiais atvejais baudžiamoji atsakomybė pagal BK 198 straipsnį yra negalima.

Apibendrinant galima teigti, kad kiekvienu konkrečiu atveju konstatuojant elektroninių duomenų konfidencialumo pažeidimų suvokimą, būtiną tyčinei kaltei nustatyti, įvairūs apribojimai elektroninėje erdvėje turėtų būti vertinami nuosekliai, atsižvelgiant į vartotojo patirtį šioje erdvėje. Vienas iš tokio vertinimo kriterijų – nustatytų apribojimų, padedančių atskirti viešus ir neviešus duomenis, numatomumas. Remiantis minėtuoju kriterijumi, tinkamai išreiškiamas elektroninės erdvės vartotojo patyrimas šioje erdvėje pirmiausia kaip virtualiojoje realybėje (laikantis *vidinės perspektyvos* požiūrio), taip pat gali būti pagrindžiama išvada, kad kaltininkas atpažino aiškiai nustatytas ribas ir jų nesilaikydamas suvokė, jog pažeidžia elektroninių duomenų konfidencialumą.

Pagrindinė taisyklė yra ta, kad nusikalstamoms veikoms aprašyti yra būtini aiškūs žodžiai, kuo specifiškesnė teisėkūra, tuo aiškiau išreikštas ketinimas pašalinti tai, kas tiksliai nepatenka į šio reguliavimo sritį.

C. Tapperis

IV SKYRIUS

NUSIKALSTAMŲ VEIKŲ ELEKTRONINIŲ DUOMENŲ IR INFORMACINIŲ SISTEMŲ KONFIDENCIALUMUI ATSKYRIMAS NUO PANAŠIŲ NUSIKALSTAMŲ VEIKŲ

IV SKYRIAUS TURINYS

Dėl informacinių technologijų taikymo pakitus nusikalstamų veikų padarymo galimybėms, baudžiamojoje teisėje kilo esminių veikų kriminalizavimo pakankamumo problemų, kurias bandyta įvairiai spręsti: buvo kuriamos naujos, gana abstrakčiai apibrėžtos nusikalstamos veikos, pradėtos naujai aiškinti tradicinių nusikalstamų veikų sudėtys. Kita vertus, dėl tokių bandymų buvo sukurta ir baudžiamojo įstatymo normų tarpusavio santykio problemų. Nustačius tradicinių nusikalstamų veikų sąlytį su elektronine erdve, neišvengiamai tenka atkreipti dėmesį į baudžiamojo įstatymo normų konkurenciją ir spręsti, ar padarytai veikai kvalifikuoti taikytina tradicinės veikos požymius nustatanti, ar išimtinai tik elektroninei erdvei sukurta norma. Beje, abi šios normos, iš dalies sutapdamos, visada tarsi dubliuos viena kitą. Be to, normų konkurencijos įveikimo klausimas sprendžiamas ir analizuojant pačių nusikalstamų veikų elektroninių duomenų bei informacinių sistemų saugumui tarpusavio santykį.

Tinkamai išsprendus normų konkurencijos klausimą, sudaromos sąlygos ne tik formuotis nuosekliai baudžiamojo įstatymo taikymo praktikai, bet ir užtikrinamas ekvivalentinio vertinimo principo reikalavimų įgyvendinimas, taigi ir vienodas tų pačių vertybių apsaugos lygis abiejose erdvėse. Šio principo pažeidimai, kai veikai kvalifikuoti pasirenkama ne ta baudžiamojo įstatymo norma, turėtų įtakos teisiniams padariniams: elektroninėje erdvėje padaryta tradicinė veika būtų laikoma pavojingesne arba ne tokia pavojinga nei analogiška veika fizinėje erdvėje. Pavyzdžiui, jei neteisėtam informacijos, kuri sudaro tarnybos paslaptį ir kuri kaltininkui buvo patikėta ar kurią jis sužinojo dėl savo tarnybos ar darbo (jei nebuvo BK 118 ir 119 straipsniuose numatytų požymių), įgijimui kvalifikuoti pasirenkamas ne BK 296 straipsnis, o 198 straipsnis (tuo atveju, jei tarnybos paslaptis yra elektroninių duomenų formos), padaryta veika yra laikoma ne nesunkiu, o apysunkiu nusikaltimu.

Lietuvos Respublikos Konstitucinio Teismo jurisprudencijoje baudžiamojo įstatymo vidinės darnos poreikis yra susijęs su konstituciniu teisinės valstybės principu, lemiančiu reikalavimą įstatymų leidėjui sukurti vientisą baudžiamąjį įstatymą, kuriame visos teisės normos sudarytų darnią visumą (Konstitucinio Teismo 2006 m. sausio 16 d. nutarimas). Kita vertus, tokios dermės pasigendama analizuojant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialu-

mui santykį su kitomis veikomis, ypač tais atvejais, kai lyginamas baudžiamajame įstatyme nustatytas nusikalstamų veikų baudžiamumas. Bene daugiausia problemų kyla siekiant atriboti iš pirmo žvilgsnio nesusijusias nusikalstamas veikas elektroninių duomenų ir informacinių sistemų saugumui, taip pat konfidencialumo pažeidimus bandant atskirti nuo nusikalstamų veikų finansų sistemai ar asmens privataus gyvenimo neliečiamumui.

1. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų konfidencialumui tarpusavio ryšys (BK 196, 198, 198[1] straipsniai)

Nusikalstamomis veikomis elektroninių duomenų ir informacinių sistemų saugumui gali būti padaroma žalos ne tik elektroninių duomenų arba informacinės sistemos konfidencialumui, bet ir jų integralumui ar prieinamumui. BK XXX skyriuje atskirai kriminalizavus elektroninių duomenų ir informacinės sistemos saugumo pažeidimus, o baudžiamajame įstatyme veikų padarymo mechanizmą suskaidžius į smulkesnes dalis, neretai tenka aiškintis šiame skyriuje numatytų nusikalstamų veikų tarpusavio ryšį. Viena iš aktualesnių problemų, susijusių su neteisėto prisijungimo prie informacinės sistemos teisiniu vertinimu, kai vykdant tokią veiką neteisėtai pasinaudojama neviešais elektroniniais duomenimis arba padaroma realios žalos informacinės sistemos apsaugos priemonėms. Tokiais atvejais galėtų kilti klausimų, ar kaltininkui, be neteisėto prisijungimo prie informacinės sistemos, atsižvelgiant į jo panaudotą neteisėto prisijungimo būdą, turėtų būti inkriminuojamos ir nusikalstamos BK 198 ar 196 straipsniuose numatytos veikos.

Jau minėta, kad galimybių ribos elektroninėje erdvėje, be kita ko, gali būti apibrėžiamos taikant *kompiuterio kodą*, kuris padeda nustatyti atitinkamo lygio prieigos prie informacinės sistemos apribojimus. Tokių apribojimų nepaisymas rodo informacinės sistemos apsaugos priemonių pažeidimus ir atitinka BK 198[1] straipsnyje numatytą nusikalstamos veikos padarymo būdą, dėl kurio, beje, ir kyla BK 198[1], 198 bei 196 straipsnių santykio problema. Vienam iš prieigos kontrolės pažeidimų – autentifikavimo procedūros apėjimui – būdingas neviešų

elektroninių duomenų (pavyzdžiui, teisėto vartotojo prisijungimo vardo, slaptažodžio, kodo ar pan.)[515] neteisėtas panaudojimas, taip suklaidinant informacinę sistemą, kuri kaltininką identifikuoja kaip teisėtą sistemos vartotoją ir suteikia prie jos prieigą. Vadinasi, tokie atvejai, kai apeinamos informacinės sistemos apsaugos priemonės, iš dalies atitinka ir BK 198 straipsnyje numatytos nusikalstamos veikos požymius. Antrasis būdas yra susijęs su pasinaudojimu silpnosiomis informacinės sistemos apsaugos priemonių vietomis, kurių gali atsirasti ir dėl tikslingų kaltininko veiksmų. Toks spragų sukūrimas, be kita ko, galimas padarius neteisėtą poveikį elektroniniams duomenims, kartu ir žalos pačioms informacinės sistemos apsaugos priemonėms, o šie veiksmai atitiktų BK 196 straipsnyje aprašytą nusikalstamą veiką. Tokiais atvejais reikėtų spręsti, kuri iš BK 198[1], 198, 196 straipsniuose numatytų normų taikytina kvalifikuojant neteisėto prisijungimo prie informacinės sistemos veiksmus.

Vertinant informacinės sistemos konfidencialumo pažeidimus matyti, kad ir neteisėtas neviešų elektroninių duomenų panaudojimas, ir neteisėtas poveikis elektroniniams duomenims tik iš dalies atitinka padarytą veiką, nes rodo vien tik neteisėtą prisijungimo prie informacinės sistemos būdą – informacinės sistemos apsaugos priemonių pažeidimą. Kaltininkui inkriminavus tik minėtąsias veikas, liktų neįvertintas pats neteisėto prisijungimo prie informacinės sistemos veiksmas. Dėl to keltinos baudžiamosios teisės normų konkurencijos, apibūdinamos kaip atvejis, kai vieną padarytą nusikalstamą veiką atitinka kelios normos[516], išsprendimo problemos. Tiksliau, šiuo

[515] Analizuojant šį klausimą reikėtų atkreipti dėmesį ir į BK 198 bei 198[2] straipsniuose aprašytų nusikalstamų veikų tarpusavio santykio klausimą. Svarbiausia priežastis, dėl kurios kyla šių veikų inkriminavimo problemų, yra ta, kad BK 198[2] straipsnyje numatytas nusikalstamos veikos dalykas: slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys, tiesiogiai skirti nusikalstamoms veikoms daryti, gali būti ir BK 198 straipsnyje numatytu dalyku, jei jiems bus būdingi neviešų elektroninių duomenų požymiai. Sprendžiant šių normų taikymo klausimą, turėtų būti atsižvelgiama į tai, kad BK 198[2] straipsnyje tiesiogiai nurodžius slaptažodžius, prisijungimo kodus ar kitokius panašius duomenis suformuluotas konkretesnis nusikalstamos veikos dalykas, palyginti su neviešais elektroniniais duomenimis. Įstatymų leidėjui nustačius specifinį neteisėto disponavimo tokiais dalykais atvejį, teigtina, kad BK 198[2] straipsnyje įtvirtinta specialioji norma, palyginti su esančia BK 198 straipsnyje.

[516] Girdenis, T. Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: Mykolo Romerio universi-

atveju turėtų būti kalbama apie vieną iš jos rūšių – normos-visumos ir normos-dalies konkurenciją bei jos įveikimo sunkumus. Tokiais atvejais baudžiamosios teisės teorijoje pripažįstama, kad kaltininko veikoms vertinti taikytina norma, kurioje išsamiai aprašyti padarytos veikos požymiai[517], t. y. norma-visuma. Minėtuoju atveju būtent BK 198[1] straipsnyje numatyta nusikalstama veika visapusiškai atitinka kaltininko atliktus neteisėto prisijungimo prie informacinės sistemos veiksmus, o neteisėtas neviešų elektroninių duomenų panaudojimas ir jiems padarytas neteisėtas poveikis tokius veiksmus atspindi tik iš dalies. Vadinasi, tokiais atvejais kaip visuma turėtų būti laikoma ta norma, kuri yra numatyta BK 198[1], o ne BK 197 ar 198 straipsniuose.

Kita vertus, tokiai visumos ir dalies konkurencijos įveikimo taisyklei reikia tam tikro patikslinimo – jai esant būtina įvertinti ir visumą sudarančių nusikalstamų veikų baudžiamumą. Nustačius, kad bet kuri visumai priskiriama nusikalstama veika yra pavojingesnė nei pati visuma, ji turėtų būti kvalifikuojama atskirai, t. y. pagal nusikalstamų veikų sutaptį. Lyginant BK 198[1], 198 ir 196 straipsnių sankcijas matyti, kad neteisėto prisijungimo prie informacinės sistemos (BK 198[1] straipsnis) ir neteisėto poveikio elektroniniams duomenims (BK 196 straipsnio 1 dalis) nusikalstamos veikos yra laikomos nesunkiu nusikaltimu (BK 11 straipsnio 3 dalis), o neteisėto elektroninių duomenų perėmimo ir panaudojimo (BK 198 straipsnis) bei BK 196 straipsnio 2 dalyje numatytos neteisėto poveikio elektroniniams duomenims veikos priskiriamos apysunkių nusikaltimų kategorijai (BK 11 straipsnio 4 dalis). Nors paprastai norma-visuma turėtų būti pavojingesnė nei ją sudarančios dalys, bet pagal esamą teisinį reguliavimą informacinės sistemos konfidencialumo pažeidimą numatanti norma neapima normos dalies – neteisėto elektroninių duomenų panaudojimo (BK 198 straipsnis) ar neteisėto poveikio elektroniniams duomenims (BK 196 straipsnio 2 dalis). Vadovaujantis minėtąja taisykle, neteisėtas prisijungimas prie informacinės sistemos, atsižvel-

tetas, 2010, p. 26.; Baudžiamoji teisė. Bendroji dalis. 3-iasis pataisytas ir papildytas leidimas. Abramavičius, A., *et al*. (sud.). Vilnius: Eugrimas, 2001, p. 335.

[517] Girdenis, T. Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: Mykolo Romerio universitetas, 2010, p. 27; Baudžiamoji teisė. Bendroji dalis. 3-iasis pataisytas ir papildytas leidimas. Abramavičius, A., *et al*. (sud.). Vilnius: Eugrimas, 2001, p. 342.

giant į kaltininko pasirinktą šios sistemos apsaugos priemonių pažeidimo būdą, atitinkamai turėtų būti kvalifikuojamas pagal nusikalstamų veikų sutaptį, t. y. BK 198[1] ir 198 straipsnius ar 196 straipsnio 2 dalį. Be abejo, dėl tokio nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumo tarpusavio ryšio matyti nemažai baudžiamajame įstatyme numatytų bausmių (jų ribų) problemų. Abejotina, ar įstatymų leidėjas, nustatydamas bausmes už nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui padarymą, iš tikrųjų siekė sukurti būtent tokį šių nusikalstamų veikų santykį.

Remiantis teismų praktika galima teigti, kad tokia normų konkurencijos problema joje nesprendžiama, o kaltininko neteisėto prisijungimo prie informacinės sistemos veiksmai kvalifikuojami tik pagal BK 198[1] arba tik pagal 198 straipsnį. Kaip pirmojo atvejo pavyzdį galima pateikti jau minėtus teismų sprendimus, kuriuose konstatuotas neteisėto prisijungimo prie informacinės sistemos faktas ir tokia veika kvalifikuota pagal BK 198[1] straipsnį. Tai tokie atvejai, kai baudžiamoji atsakomybė pagal minėtąjį BK straipsnį kilo nustačius neteisėtą prisijungimą prie interneto bankininkystės[518], interneto prekybos ir aukcionų sistemos[519], socialinio tinklalapio *Facebook* paskyros[520], elektroninio pašto paskyros[521], mokėjimo bendrovės *PayPal* kliento sąskaitos[522], interneto žaidimo paskyros[523] ir kt. naudojantis vartotoją sistemoje leidžiančiais atpažinti autentifikavimo kodais, slaptažodžiais ar kitais duomenimis. Neviešų elektroninių duomenų naudojimas neteisėtai prisijungiant prie informacinės sistemos teismų sprendimuose atskirai pagal BK 198 straipsnį nekvalifikuotas.

---

[518] Alytaus rajono apylinkės teismo 2017 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-68-297/2017.

[519] Klaipėdos miesto apylinkės teismo 2009 m. birželio 29 d. baudžiamasis įsakymas byloje Nr. 1-740-93/2009.

[520] Klaipėdos apygardos teismo 2017 m. spalio 12 d. nutartis baudžiamojoje byloje Nr. 1A-279-651/2017.

[521] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2015 m. sausio 6 d. nutartis baudžiamojoje byloje Nr. 2K-138/2015.

[522] Vilniaus apygardos teismo 2017 m. gegužės 15 d. nuosprendis baudžiamojoje byloje Nr. 1-101-190/2017.

[523] Kėdainių rajono apylinkės teismo 2017 m. rugsėjo 28 d. baudžiamasis įsakymas byloje Nr. 1-308-188/2017.

Antruoju atveju matyti, kad pirmumas kvalifikuojant veiką teikiamas sudedamajai BK 198[1] straipsnyje esančios veikos daliai – jos padarymo būdui, t. y. neviešų elektroninių duomenų panaudojimui, todėl yra diskutuotinas. Pavyzdžiui, vienoje iš baudžiamųjų bylų konstatuota, kad M. Ž., be kitų veikų, padarė ir dvi numatytas BK 198 straipsnio 1 dalyje, t. y. *M. Ž. neteisėtai stebėjo, įgijo, laikė ir panaudojo neviešus elektroninius duomenis, o būtent: <...> M. Ž. neteisėtai įgijo V. L. internetinio tinklalapio „Gmail“ elektroninio pašto elektroninės prieigos slaptažodį (duomenys neskelbtini) bei vartotojo vardą (duomenys neskelbtini), kuriuos laikė <...> ir būdama savo namuose, adresu (duomenys neskelbtini), iš kompiuterinės sistemos <...> septynis kartus juos panaudojo, prisijungdama prie V. L. elektroninės pašto dėžutės <...>. Be to, M. Ž. neteisėtai stebėjo, įgijo, laikė ir panaudojo neviešus elektroninius duomenis, o būtent: <...> M. Ž. įgijo V. L. internetinio tinklalapio „Facebook“ profilio (duomenys neskelbtini) elektroninės prieigos slaptažodį (duomenys neskelbtini) bei vartotojo vardą (duomenys neskelbtini), kuriuos laikė <...> ir būdama savo namuose adresu (duomenys neskelbtini) <...> juos stebėjo ir panaudojo, prisijungdama prie V. L. profilio (duomenys neskelbtini) <...>*[524].

Reikėtų pripažinti, kad dėl tokio nusikalstamų veikų kvalifikavimo iš baudžiamosios teisės pozicijų lieka neįvertintas pats prisijungimo prie informacinės sistemos veiksmas. Į tai atkreiptas dėmesys kasacinės instancijos teismo praktikoje sprendžiant, kuri – BK 198[1] ar 198 straipsnyje numatyta – nusikalstama veika atitinka neteisėtą prisijungimą prie elektroninio pašto paskyros. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2015 m. sausio 6 d. nutartyje baudžiamojoje byloje Nr. 2K-138/2015 pabrėžiama, kad tokioms veikoms kvalifikuoti taikytinas BK 198[1] straipsnis:

BK 198[1] straipsnyje numatytos veikos inkriminavimui būtina nustatyti, kad prie IS buvo prisijungta pažeidžiant šios sistemos apsaugos priemones. Nagrinėjamos bylos kontekste aktualu tai, kad vartotoją elektroninio pašto sistemoje leidžianti nustatyti autentiškumo patvirtinimo procedūra gali būti laikoma viena iš šios sistemos saugumo (taip pat ir konfidencialumo) užtikrinimo priemonių. O teisėto vartotojo tapatybę patvirtinančių duomenų neteisėtas įvedimas, suklaidinant sistemą, laikytinas šios sistemos apsaugos priemonių pažeidimu ir atitinka tik netei-

[524] Ukmergės rajono apylinkės teismo 2012 m. gruodžio 17 d. baudžiamasis įsakymas byloje Nr. 1-312-627/2012.

sėto prisijungimo prie IS veikos padarymo būdą. Taigi, byloje nustatyto neteisėto prisijungimo prie elektroninio pašto paskyros j@yahoo.de vertinimui taikant tik BK 198 straipsnį, iš baudžiamosios teisės pozicijų liktų neįvertintas pats neteisėto prisijungimo prie paskyros veiksmas. Todėl, priešingai nei teigiama kasaciniame skunde, BK 198[1] straipsnio 1 dalies, o ne BK 198 straipsnio 1 dalies norma pripažintina norma-visuma ir taikytina kvalifikuojant neteisėtą prisijungimą prie informacinės sistemos, šiuo atveju – prie elektroninio pašto paskyros.

Kaip matyti, nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui atskyrimo sunkumų kyla ne tik dėl pasirinkto tokių veikų kriminalizavimo būdo, bet ir dėl nustatyto jų baudžiamumo. Dėl tarpusavyje nesuderintų minėtųjų nusikalstamų veikų sankcijų atsiranda neaiškumų kvalifikuojant visas kaltininko elektroninėje erdvėje padarytas nusikalstamas veikas. Atsižvelgiant į neteisėto prisijungimo prie informacinės sistemos mechanizmo ypatybes, tokią veiką vis dėlto siūlytina kvalifikuoti tik pagal BK 198[1] straipsnį.

2. Nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui (BK 198 ir 198[2] straipsniai) bei nusikalstamų veikų finansų sistemai (BK 214, 215 straipsniai) ryšys

Plečiantis elektroninės prekybos paslaugoms, jų teikimas tapo neatsiejamas nuo asmens tapatybės nustatymo elektroninėje erdvėje. Šis nustatymas – tai vartotojo identifikavimo tam tikroje informacinėje sistemoje procesas[525], per kurį sistemai pateikiami vartotojui suteikti ir sistemoje jį leidžiantys atpažinti duomenys. Dėl šių identifikavimo proceso ypatybių kaltininkui, siekiančiam informacinėje sistemoje save pateikti kaip kitą asmenį ir joje atlikti teisėtam vartotojui leidžiamus veiksmus (pavyzdžiui, mokėjimo operacijas)[526], konfidencialūs

[525] Štitilis, D.; Laurinaitis, M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*, 2009, 50: 242.

[526] Pagal Lietuvos Respublikos mokėjimų įstatymo (*Valstybės žinios*, 1999, Nr. 97-2775) 2 straipsnio 26 punktą, mokėjimo operacija – tai „mokėtojo, mokėtojo vardu arba gavėjo inicijuotas lėšų įmokėjimas, pervedimas arba išėmimas neatsižvelgiant į mokėtojo ir gavėjo pareigas, kuriomis grindžiama operacija“.

duomenys tampa būtini. Vertinant tokių duomenų konfidencialumo pažeidimus, atitinkamai tenka spręsti, pagal kokius baudžiamojo įstatymo straipsnius turėtų būti kvalifikuojamas neteisėtas duomenų gavimas ir jų panaudojimas.

Atsižvelgiant į teismų praktiką, tokie probleminiai aspektai geriausiai išryškėja analizuojant sukčiavimo elektroninėje erdvėje etapus[527], tiksliau – vieną iš jų, susijusį su neteisėtu duomenų, leidžiančių atpažinti vartotoją įvairiose elektroninių paslaugų sistemose, be kita ko, ir elektroninėje bankininkystėje, disponavimu. Tokiais atvejais spręstinas klausimas, ar šiais veiksmais yra pažeidžiamas elektroninių duomenų konfidencialumas ar vis dėlto jais yra kėsinamasi į elektroninių mokėjimo priemonių naudojimo ir disponavimo jomis tvarką. Minėtoji nusikalstamų veikų atskyrimo problema kyla dėl to, kad baudžiamoji atsakomybė už įvairius neteisėto elektroninių duomenų disponavimo veiksmus yra numatyta ne tik BK XXX skyriuje esančiuose 198 ir 198², bet iš dalies ir BK XXXII skyriuje numatytuose 214 bei 215 straipsniuose. Kadangi neteisėtas disponavimas elektroniniais duomenimis apibūdinamas remiantis įvairiomis alternatyviomis veikomis, siekiant aiškumo nusikalstamų veikų atribojimo klausimai galėtų būti aptariami atskirai dėl, *pirma*, elektroninių duomenų įgijimo ir laikymo; *antra*, šių duomenų panaudojimo.

Analizuojant neteisėtą elektroninių duomenų įgijimą ir laikymą, atkreiptinas dėmesys į tai, kad tokio pobūdžio neteisėti veiksmai taip pat yra kriminalizuoti BK 198, 198² ir BK 214 straipsnyje. Be įvairių alternatyvų, BK 198 straipsnyje minimas neviešų elektroninių duomenų įgijimas ir laikymas. BK 198² straipsnyje, be kitų veikų, kriminalizuotas ir neteisėtas slaptažodžių, prisijungimo kodų ar kitokių panašių duomenų įgijimas ar laikymas. Baudžiamoji atsakomybė pagal BK 214 straipsnį kyla ir tada, kai neteisėtai įgyjami ar laikomi svetimų elektroninių mokėjimo priemonių vartotojo tapatybės patvirtinimo priemonių duomenys, kurių pakanka finansinei operacijai inicijuoti. Vadinasi, akivaizdu, kad tokia padėtis yra susijusi su baudžiamosios teisės normų konkurencija, kai padarytos nusikalstamos veikos sudėties požymiai yra nustatomi ne vienos, o keleto baudžiamojo įstatymo normų. Analizuojant minėtuosius BK straipsnius

[527] Plačiau žr. Kalpokas, V.; Marcinauskaitė, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos*, 2012, Nr. 3(77): 30.

matyti, kad BK 198 straipsnyje esantys nusikalstamos veikos požymiai yra bendresniojo pobūdžio – konkrečiau nenurodoma, kokios rūšies elektroniniai duomenys yra neteisėtai įgyjami ir laikomi. BK 198[2] ir 214 straipsniuose minimi specifiniai, dalyko prasme siauresni požymiai: BK 198[2] straipsnyje konkrečiai įvardijami slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys, o BK 214 straipsnyje – elektroninių mokėjimo priemonių vartotojo tapatybės patvirtinimo priemonių duomenys, kurių pakanka finansinei operacijai inicijuoti. Šį kvalifikavimo klausimą padeda spręsti doktrinoje suformuluota baudžiamosios teisės normų konkurencijos įveikimo taisyklė – esant bendrosios ir specialiosios normos konkurencijai, taikoma specialioji norma[528]. Dėl to nustačius, kad kaltininkas neteisėtai įgijo visus BK 214 straipsnyje nurodytus požymius turinčius duomenis, jo veika kvalifikuotina ne pagal bendrąją BK 198 straipsnyje numatytą normą, o pagal specialiąją – esančią BK 214 straipsnyje. Beje, tokių nusikalstamos veikos baudžiamojo teisinio vertinimo pavyzdžių galima rasti ir teismų praktikoje. Kaip antai vienoje iš baudžiamųjų bylų konstatuota, jog *ištirtų įrodymų visuma neabejotinai patvirtina, kad kaltinamasis neteisėtai įgijo svetimus asmens duomenis, elektroninės bankininkystės prisijungimo duomenis, kurie buvo pakankami inicijuoti finansines operacijas ir tokie jo veiksmai turi būti kvalifikuojami pagal BK 214 straipsnio 1 dalį. Turėdamas neteisėtai įgytus nukentėjusiųjų (liudytojų) asmens duomenis, elektroninės bankininkystės prisijungimo duomenis, kaltinamasis juos neteisėtai panaudojo neteisėtai prisijungdamas prie informacinių sistemų ir nukentėjusiųjų (liudytojų) vardu atlikdamas finansines operacijas, todėl jo veiksmai kvalifikuojami pagal BK 215 straipsnio 1 dalį ir BK 198[1] straipsnio 1 dalį. Be to, kaltinamasis neteisėtai įgytus nukentėjusiųjų (liudytojų) duomenis panaudojo svetimo turto pasisavinimui, jų vardu sudarė sutartis su kredito bendrovėmis, su UAB „Bitė Lietuva“, pasisavino svetimą turtą, t. y. apgaule įgijo svetimą turtą, kurio vertė viršija 5 MGL (MGL dydis, galiojęs iki 2018-01-01, LAT nutartis Nr. 2K-348/2008), todėl tokie jo veiksmai kvalifikuojami pagal BK 182 straipsnio 1 dalį*[529].

---

[528] Pavilonis, V. Baudžiamosios teisės normų konkurencija. *Teisės problemos*, 1996, 2(12): 40.

[529] Kauno apylinkės teismo 2018 m. sausio 22 d. nuosprendis baudžiamojoje byloje Nr. 1-29-673/2018.

Kiek sudėtingesnė nei aptartoji yra BK 198[2] ir 214 straipsniuose numatytų nusikalstamų veikų santykio problema. Svarbiausia šios problemos priežastis yra ta, kad BK 198[2], kaip ir BK 214 straipsnyje, numatytas konkretesnis nei BK 198 straipsnio dispozicijoje minimas nusikalstamos veikos dalykas. Be to, BK 198[2] straipsnyje nurodyti slaptažodžiai, prisijungimo kodai ar kitokie panašūs duomenys gali būti ir BK 214 straipsnyje numatytas dalykas, jeigu jie yra elektroninės mokėjimo priemonės vartotojo tapatybės patvirtinimo priemonių duomenys, kurių pakanka finansinei operacijai inicijuoti. Vadinasi, sprendžiant BK 198[2] ir 214 straipsnių taikymo klausimą turėtų būti atsižvelgiama į tai, kad BK 214 straipsnyje yra kriminalizuota veika, kuria pirmiausia yra pažeidžiama elektroninių mokėjimo priemonių disponavimo tvarka[530], todėl nustačius, kad kaltininkas neteisėtai įgijo finansinei operacijai inicijuoti pakankamus elektroninius duomenis, jo veika turėtų būti kvalifikuojama taikant BK 214, o ne BK 198[2] straipsnį. Šiuo požiūriu svarbu atkreipti dėmesį ir į tai, kad pagal Lietuvos Respublikos mokėjimų įstatymo[531] 2 straipsnio 27 punktą mokėjimo priemonė nėra tapatinama tik su materialiąja priemone, o yra apibūdinama kaip personalizuota priemonė ir (arba) tam tikros procedūros, dėl kurių susitaria mokėjimo paslaugų vartotojas ir šių paslaugų teikėjas bei kurias mokėjimo paslaugų vartotojas taiko mokėjimo nurodymui inicijuoti. Dėl to elektronine mokėjimo priemone pripažintina ir banko paslaugų teikimo internetu elektroninė sistema, susijusi su tam tikromis procedūromis, kurios taikomos mokėjimo nurodymui inicijuoti bei pan., ir dėl jų susitarė mokėjimo paslaugų vartotojas bei mokėjimo paslaugų teikėjas. Kaip teigiama literatūroje, geriausias pavyzdys, „apibūdinantis sutartas procedūras elektroniniuose mokėjimuose ir plačiausiai taikomas Lietuvoje – elektroninė bankininkystė, kur vartotojo vardas, slaptažodžiai, kintamų slaptažodžių kortelės yra sutartos procedūros mokėjimams inicijuoti ir atlikti“[532].

Analizuojant BK 198[2] ir 214 straipsnių taikymo teismuose praktiką, vis dar pasitaiko atvejų, kai kvalifikuojant veiką (net ir nustačius,

---

530 Abramavičius, A., *et al*. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai). Vilnius: Registrų centras, 2010, p. 28.

531 Lietuvos Respublikos mokėjimų įstatymas. *Valstybės žinios*, 1999, Nr. 97-2775.

532 Laurinaitis, M. Elektroninių pinigų teisinis reguliavimas: daktaro disertacija. Vilnius: Mykolo Romerio universitetas, 2015, p. 47.

kad kaltininkas neteisėtai įgijo pakankamus duomenis finansinei operacijai elektroninės bankininkystės sistemoje inicijuoti) pirmumas teikiamas BK 198[2] straipsnyje esančiai normai. Pavyzdžiui, vienoje iš baudžiamųjų bylų konstatuota, kad kaltininkas įgijo minėtuosius duomenis, bet jam inkriminuota veika, numatyta ne BK 214, o 198[2] straipsnyje: *V. A. padarė jai inkriminuotas veikas, t. y. neteisėtai įgijo bei laikė A. Č. išduotus prisijungimo prie elektroninės bankininkystės sistemos duomenis (vartotojo vardą, laikiną slaptažodį, kortelę su prisijungimo kodais) ir juos panaudojo nusikalstamoms veikoms daryti – apgaule savo naudai įgijo UAB (duomenys neskelbtini) priklausantį turtą, UAB (duomenys neskelbtini) priklausantį turtą, A. Č. priklausantį turtą bei (duomenys neskelbtini) filialui priklausantį turtą. Taip pat savo sūnaus A. A. naudai įgijo A. Č. priklausantį turtą. Iš viso V. A. padarė penkias nusikalstamas veikas, numatytas BK 182 str. 1 d., bei vieną nusikalstamą veiką, numatytą BK 1982 str. 1 d.*[533]

Kitas probleminis klausimas yra susijęs su vartotoją elektroninės bankininkystės sistemoje leidžiančių nustatyti duomenų neteisėto naudojimo atliekant įvairias pinigines operacijas teisėto vartotojo banko sąskaitoje vertinimu. Kadangi baudžiamajame įstatyme atsakomybė už neteisėtą neviešų elektroninių duomenų naudojimą numatoma remiantis keletu BK straipsnių, tai kvalifikuojant tokio pobūdžio veikas būtina tinkamai išspręsti BK 198 ir 215 straipsniuose esančių normų konkurencijos klausimą.

Analizuojant BK 215 straipsnyje numatytą neteisėto finansinės operacijos inicijavimo, naudojantis svetimos elektroninės priemonės vartotojo tapatybės patvirtinimo priemonių duomenimis, požymį galima teigti, kad jis, palyginti su BK 198 straipsnyje numatytu neteisėto neviešų elektroninių duomenų panaudojimo požymiu, yra konkretesnis. Vadinasi, BK 215 straipsnyje, o ne BK 198 straipsnyje numatyta norma, vadovaujantis jau minėtos bendrosios ir specialiosios normų konkurencijos įveikimo taisykle, taikytina tuo atveju, jei finansinė operacija neteisėtai inicijuota ar atlikta panaudojus svetimos elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenis. Toks aiškinimas galėtų nuosekliai išplaukti ir iš šio BK straipsnio paskirties – kriminalizuojant tokią veiką pirmiausia

[533] Vilniaus miesto 1 apylinkės teismo 2011 m. kovo 25 d. nuosprendis baudžiamojoje byloje Nr. 1-68-203/2011.

siekiama apsaugoti elektroninių mokėjimo priemonių disponavimo tvarką. Šiuo atveju elektroninių mokėjimo priemonių duomenų ir kredito įstaigų informacinių sistemų saugumas laikomas tik papildoma baudžiamojo įstatymo saugoma vertybe, kuriai daroma žala arba kyla tokios žalos grėsmė[534].

Aiškinimas, kad BK 215 straipsnis taikytinas ir tais atvejais, kai neteisėtos mokėjimo operacijos inicijuojamos ar atliekamos elektroninėje sistemoje įvedus vartotojo tapatybės patvirtinimo priemonių duomenis, būdingas ir kasacinės instancijos teismo praktikai. Pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2012 m. birželio 26 d. nutartyje baudžiamojoje byloje Nr. 2K-375/2012 konstatuota, kad apeliacinės instancijos teismo išvada, jog BK 198 straipsnyje numatytos nusikalstamos veikos dalykas yra ir generatoriaus sukurtas kodas, neatitinka nei teismų praktikos, nei įstatyme suformuotos vartotojo tapatybės patvirtinimo priemonių duomenų sąvokos. Teismas šioje kasacinėje byloje atkreipė dėmesį į tai, kad *remiantis tokia teismo logika, mokėjimo instrumento panaudojimas turėtų būti baudžiamas pagal BK 215 straipsnio ir 198 straipsnio sutaptį, kaip mokėjimo instrumento panaudojimas ir neteisėtas PIN kodo panaudojimas. Tačiau taip nėra, nes BK 215 straipsnis apima ir tuos duomenis, kurie identifikuoja naudotoją. Taigi teismas visiškai nepagrįstai generatoriaus sukurtą kodą pripažino BK 198 straipsnio dalyku, nes slaptažodžių generatorius yra įtaisas, identifikuojantis sąskaitos valdytojo tapatybę ir leidžiantis inicijuoti finansinę operaciją (tokią pačią funkciją atlieka ir mokėjimo kortelės PIN kodas), o tai yra nusikalstamos veikos, numatytos BK 215 straipsnyje, dalykas.*

Neteisėtas mokėjimo operacijos inicijavimas naudojantis elektroninės bankininkystės vartotojo tapatybės patvirtinimo priemonių duomenimis pagal BK 215 straipsnį kvalifikuojamas ir žemesniųjų instancijų teismų praktikoje. Vis dėlto joje dar pasitaiko diskutuotinų BK 198 ir 215 straipsniuose esančių normų konkurencijos įveikimo būdų, kai kvalifikuojant veiką pirmumas teikiamas BK 198 straipsnio normai, kuria numatomi bendresnieji požymiai. Pavyzdžiui, vienoje iš baudžiamųjų bylų kaltininko padarytos nusikalstamos veikos perkvalifikuotos iš BK 214 straipsnio 1 dalies ir 215 straipsnio 1 dalies į

[534] Abramavičius, A., *et al*. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai). Vilnius: Registrų centras, 2010, p. 36.

BK 198 straipsnio 1 dalį: [*A. Š. – aut. pastaba*] *turėdamas tikslą apgaule savo naudai įgyti svetimą turtą – AB (duomenys neskelbtini) banko kliento J. M. pinigines lėšas, <...> prisijungęs prie AB (duomenys neskelbtini) banko elektroninės bankininkystės sistemos, pasinaudojęs svetimu – AB (duomenys neskelbtini) banko klientui J. M. priskirtu atpažinimo kodu Nr. (duomenys neskelbtini) ir slaptažodžiu, po ko įvedęs pastarojo vardu išduotos identifikavimo kodų kortelės Nr. (duomenys neskelbtini) duomenis – sistemos paprašytą kodą, neteisėtai prisijungė prie J. M. vardu atidarytos AB (duomenys neskelbtini) banko sąskaitos (duomenys neskelbtini) ir atliko nurodytoje sąskaitoje esančių piniginių lėšų – 775 JAV dolerių, kas sudaro 1710 Lt, pervedimo operacijai savo sąskaitą Nr. (duomenys neskelbtini), esančią AB (duomenys neskelbtini) banke, tokiu būdu savo naudai įgijo 775 JAV dolerius (1710 Lt), tuo padarydamas AB (duomenys neskelbtini) bankui 775 JAV dolerių (1710 Lt) turtinę žalą. <...> Bylos nagrinėjimo metu prokurorė pateikė naują kaltinimą A. Š., kvalifikuojant jo veiką dėl neteisėto neviešų elektroninių duomenų laikymo ir panaudojimo pagal Lietuvos Respublikos BK 198 str. 1 d., t. y. pagal lengvesnį Baudžiamojo kodekso straipsnį. Toks A. Š. veikos kvalifikavimas yra teisingas. Byloje nustatyta, kad A. Š. neteisėtai laikė ir panaudojo elektroninės bankininkystės sutartį, sudarytą kito asmens vardu ir priedą prie šios sutarties – kortelę su prisijungimo kodais, t. y. laikė ir panaudojo neviešus elektroninius duomenis. Šie A. Š. veiksmai turi visus Lietuvos Respublikos BK 198 str. 1 d. sudėties požymius. A. Š. veiksmai perkvalifikuotini iš Lietuvos Respublikos BK 214 str. 1 d. ir 215 str. 1 d. į BK 198 str. 1 d. A. Š. veiksmai apgaule įgyjant svetimą turtą teisingai kvalifikuoti pagal Lietuvos Respublikos BK 182 str. 1 d.*[535]

Atribojimo problemų gali kilti ir sprendžiant, kuris – BK 198[1] ar 215 straipsnis – taikytinas kvalifikuojant kaltininko neteisėto prisijungimo prie elektroninės bankininkystės sistemos veiksmus. Atsakymas į šį klausimą priklauso nuo to, ar toks neteisėtos prieigos gavimo veiksmas laikytinas finansinės operacijos inicijavimu ar jos atlikimu naudojantis svetimos mokėjimo priemonės vartotojo tapatybės patvirtinimo priemonių duomenimis pagal BK 215 straipsnį, ar vis dėlto tai yra autentifikavimo procedūrų pažeidimas pagal BK 198[1] straipsnį. Kasacinės instancijos teismo praktikoje pabrėžiama,

[535] Vilniaus miesto 3 apylinkės teismo 2010 m. sausio 27 d. nuosprendis baudžiamojoje byloje Nr. 1-182-498/10.

kad remiantis BK 215 straipsniu *baudžiama ne už duomenų panaudojimą, bet už neteisėtą finansinės operacijos atlikimą panaudojant tokius duomenis*[536]. Vadinasi, svarbu nustatyti ne tik minėtųjų duomenų panaudojimo faktą, bet ir tai, kad tokiu būdu buvo inicijuota būtent finansinė operacija. Tai, kad neteisėtas prisijungimas prie elektroninės bankininkystės paprastai neturėtų būti laikomas finansine operacija, be kita ko, galima motyvuoti atsižvelgiant į pačių šios sistemos apsaugos priemonių paskirtį. Autentifikavimo procedūra pirmiausia yra skirta nustatyti teisėtą sistemos vartotoją, t. y. asmenį, kuriam yra suteikta teisė atlikti sistemoje tolesnius veiksmus, be kita ko, inicijuoti ar atlikti finansines operacijas. Kasacinės instancijos teismo praktikoje išaiškinta, kad *svetimos elektroninio mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenų panaudojimas finansinei operacijai atlikti – tai svetimos elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių pateikimas kredito įstaigai, siekiant gauti informaciją apie elektroninius pinigus arba sudaryti nurodymą disponuoti kredito įstaigoje atidarytoje sąskaitoje esančiomis lėšomis*[537]. Nagrinėjamuoju požiūriu aktualu ir tai, kad elektroninės bankininkystės sistema gali būti naudojamasi ne tik finansinėms operacijoms inicijuoti ar atlikti, bet ir, pavyzdžiui, vartotojo tapatybei patvirtinti siekiant gauti kitokio pobūdžio elektroninių paslaugų (pavyzdžiui, prisijungti prie Elektroninės valdžios vartų, Registrų centro). Tokiais autentifikavimo procedūros pažeidimais pirmiausia yra kėsinamasi į informacinės sistemos konfidencialumą, kuriuo prieiga prie sistemos yra užtikrinama tik teisėtiems jos vartotojams. Vadinasi, aiškinantis, „kas padarė ką <...>?“[538] elektroninėje erdvėje, ir siekiant suprasti, „kaip internetas konstatuoja „kas“, reikėtų kiek atsargiau mąstyti apie tai, kaip vyksta „identifikavimas“ ir kaip jis galėtų vykti internete“[539].

---

[536] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2014 m. gruodžio 9 d. nutartis baudžiamojoje byloje Nr. 2K-508/2014.

[537] *Ibidem*.

[538] Lessig, L. Code and other laws of cyberspace. New York (N.Y.): Basic books, 1999, p. 39.

[539] *Ibidem*.

3. Neteisėto elektroninių duomenų perėmimo ir panaudojimo bei nusikaltimų privataus gyvenimo neliečiamumui ryšys

CIA triada, leidžianti į saugumą pažvelgti kaip į konfidencialumo, integralumo ir prieinamumo visumą, parodo ir BK 198 bei 166–168 straipsniuose esančių nusikalstamų veikų tarpusavio santykio problemą. Neteisėtas disponavimas neviešais elektroniniais duomenimis rodo elektroninių duomenų konfidencialumo pažeidimus, o BK XXIV skyriuje esančios veikos – neteisėtą įsikišimą į privatų asmens gyvenimą. Analizuojant minėtuosiuose BK straipsniuose numatytų nusikalstamų veikų sudėties požymius matyti, kad būtent teisinių gėrių (tiksliau – konfidencialumo ir asmens privataus gyvenimo neliečiamumo atribojimo kriterijai) galėtų padėti nustatyti BK 198 straipsnyje ir BK XXIV skyriuje esančių veikų skirtumus.

Lietuvos Respublikos Konstitucijos 22 straipsnyje įtvirtintas bendrasis principas, kad žmogaus privatus gyvenimas yra neliečiamas. Šios Konstitucijoje numatytos principinės nuostatos turinys yra išplėtotas Konstitucinio Teismo jurisprudencijoje, kartu joje suformuluojant ir privataus žmogaus gyvenimo koncepciją. Ne kartą pateikdamas nuomonę dėl Konstitucijos 22 straipsnyje numatytos asmens teisės į privatų gyvenimą ir jos ribojimų Konstitucinis Teismas pabrėžė, kad pagal Konstituciją „privatus žmogaus gyvenimas – tai individo asmeninis gyvenimas: gyvenimo būdas, šeiminė padėtis, gyvenamoji aplinka, santykiai su kitais asmenimis, individo pažiūros, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas ir kt. Konstitucijos 22 straipsnio normomis įtvirtintas žmogaus privataus gyvenimo neliečiamumas lemia asmens teisę į privatumą. Šiai teisei priskiriamas asmeninio, šeimos ir namų gyvenimo, garbės ir reputacijos neliečiamumas, asmens fizinė ir psichinė neliečiamybė, asmeninių faktų slaptumas, draudimas skelbti gautą ar surinktą konfidencia-lią informaciją ir kt.“ (Konstitucinio Teismo 1999 m. spalio 21 d., 2000 m. gegužės 8 d., 2002 m. rugsėjo 19 d., 2002 m. spalio 23 d., 2003 m. kovo 24 d. nutarimai). Gana abstrakčiai apie baudžiamojo įstatymo saugomą vertybę – žmogaus privataus gyvenimo neliečiamumą – užsimenama ir kasacinės instancijos teismo praktikoje:

Fizinių ir juridinių asmenų baudžiamosios atsakomybės įtvirtinimas BK 167 straipsnyje padeda siekti Konstitucijoje, Konvencijoje ir kituose teisės aktuose numatytų tikslų, t. y. saugoti privatų asmenų gyvenimą nuo pavojingos, neteisėtos kitų asmenų veiklos – neteisėto informacijos apie privatų asmens gyvenimą rinkimo, ir užtikrinti, kad būtų veiksmingai (realiai) gerbiamas privatus asmenų gyvenimas. Taigi šio nusikaltimo objektas – prigimtinė, konvencinė ir konstitucinė vertybė – žmogaus privataus gyvenimo neliečiamumas[540]. Šio teismo jurisprudencijoje atkreipiamas dėmesys ir į tai, kad *privataus gyvenimo sąvoka yra plati sąvoka, BK 167 straipsnyje nedetalizuojama, todėl apie tai, kas yra konkretaus asmens privataus gyvenimo dalis, kokia informacija patenka į baudžiamosios teisės priemonėmis saugotiną konkretaus asmens privataus gyvenimo erdvę, teismas sprendžia įvertinęs byloje nustatytų aplinkybių ir faktų visumą.*

Vertinant tokią visumą, svarbu taip pat atsižvelgti į renkamos informacijos ryšį su konkretaus asmens privačiu gyvenimu (ar ji susijusi su išties svarbiais asmens privataus gyvenimo aspektais arba nors savaime nėra intymi, bet yra surinkta privatumą ribojančiais, paprastai teismo sankcijos reikalaujančiais būdais; ar tai tik bendresnio pobūdžio, dažnai įvairiais atvejais paties asmens atskleidžiama informacija).

Galiausiai primintina ir tai, kad baudžiamoji teisė yra ultima ratio priemonė, todėl tokia atsakomybė vertinant BK 167 straipsnio 1 dalyje numatytą veiką turėtų būti taikoma už pačius sunkiausius asmens privataus gyvenimo pažeidimus. Šios rūšies atsakomybei esant ne vienintelei poveikio priemonei teisės pažeidėjui galimų pritaikyti teisinės atsakomybės formų sistemoje, svarbu nustatyti, ar konkreti kaltininko veika išties pasiekusi tokį pavojingumo laipsnį, kad, vertinant šią veiką pagal protingumo, proporcingumo, teisingumo ir kitų bendrųjų teisės principų nuostatas, taip pat BK 37 straipsnio nuostatų kontekstą, būtų pagrįstas baudžiamosios teisės priemonių taikymas[541].

Beje, plačią ir įvairias asmeninės nepriklausomybės sritis apimančią privataus gyvenimo sąvoką bandoma formuluoti ne tik teismų jurisprudencijoje, bet ir nacionaliniuose įstatymuose. Pavyzdžiui, pagal Lietuvos Respublikos visuomenės informavimo įstatymo 2 straips-

[540] Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2018 m. gegužės 31 d. nutartis baudžiamojoje byloje Nr. 2K-7-84-489/2018.

[541] *Ibid*.

nio 46 punktą[542], privatus gyvenimas – tai „asmeninis žmogaus, jo šeimos gyvenimas, gyvenamoji aplinka, kurią sudaro fizinio asmens gyvenamoji patalpa, jai priklausanti privati teritorija ir kitos privačios patalpos, kurias fizinis asmuo naudoja savo ūkinei, komercinei ar profesinei veiklai, taip pat fizinio asmens psichinė ir fizinė neliečiamybė, garbė ir reputacija, slapti asmeniniai faktai, fizinio asmens fotonuotraukos ar kiti atvaizdai, informacija apie fizinio asmens sveikatą, privatus susirašinėjimas ar kitoks ryšio palaikymas, fizinio asmens pažiūros, įsitikinimai, įpročiai ir kiti duomenys, kuriuos galima naudoti tik jam sutikus“.

Šiais privataus gyvenimo apibrėžimais parodoma, kad neįmanoma pateikti išsamios privataus gyvenimo apibrėžties ir nustatyti griežtų jo ribų, todėl tam tikrų duomenų statusas priklauso nuo daugelio vertintinų aplinkybių. Kadangi „nei Konstitucijoje, nei Konvencijos nuostatose nepateikiama privataus gyvenimo apibrėžtis, todėl konkrečiu atveju teismai turi plačią diskreciją spręsti, ar tam tikri faktai laikytini privačiu gyvenimu, kuriam taikytina apsauga, ar ne“[543].

Kaip matyti, išsamiai apibrėžti asmens privatumo srities beveik neįmanoma, bet tam tikrus jos kontūrus, vidinę privatumo struktūrą, nors ir abstrakčiai, vis dėlto leidžia nustatyti pačios teisės į privatumą aprašymas tarptautiniuose ir nacionaliniuose teisės aktuose. Vadinasi, tarpusavyje susijusiomis asmeninės nepriklausomybės sritimis gali būti laikomas, pavyzdžiui, privatus, šeimos gyvenimas, būstas ar asmens susirašinėjimas[544], be to, literatūroje pasitaiko ir kiek kitokių, bet panašių skirstymų, pavyzdžiui, joje kalbama apie informacinį, fizinį, komunikacinį ar teritorinį privatumą[545] ir pan. Nors šie kate-

---

[542] Lietuvos Respublikos visuomenės informavimo įstatymas. *Valstybės žinios*, 1996, Nr. 71-1706.

[543] Lankauskas, M.; Mulevičius, M.; Zaksaitė, S. Teisės į privatumą, minties, sąžinės, religijos laisvę ir saviraišką užtikrinimo problemos: mokslo studija. Vilnius: Lietuvos teisės institutas, 2013, p. 10.

[544] Pagal Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnį.

[545] Panomariovas, A. Asmens privataus gyvenimo paslaptis ir su ja susijusios problemos baudžiamajame procese. *Jurisprudencija*, 2001, 23(15): 99.; Kiškis, M., *et al.* Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006, p. 115–116.

gorizavimai yra daugiau teorinio, metodologinio pobūdžio, bet jais remiantis galima aiškiau suvokti BK XXIV skyriaus vidinę struktūrą. Pavyzdžiui, teritorinio privatumo pažeidimai yra kriminalizuoti BK 165 straipsnyje, kuriuo numatoma atsakomybė už neteisėtą asmens būsto neliečiamumo pažeidimą; atsakomybė už komunikacinio privatumo pažeidimus nustatyta BK 166 straipsnyje, kuriame aprašyti asmens susižinojimo neliečiamumo pažeidimo požymiai ir pan. Dėl to, pavyzdžiui, apsikeitimu asmeninio pobūdžio informacija nelaikomas tarnybinis, oficialus, dalykinis susirašinėjimas[546]. Tai pabrėžiama ir teismų praktikoje: *Asmens susižinojimo neliečiamumo objektas – privataus žmonių bendravimo viešojo ryšio priemonėmis tvarka ir slaptumas. Tai pasikeitimas privataus pobūdžio informacija tarp privačių asmenų. Ne privačių asmenų, taip pat – įmonių vadovų tarpusavio profesinis susirašinėjimas, tarnybinis bendravimas – nėra šio straipsnio* [*BK 166 straipsnis – aut. pastaba*] *saugoma socialinių santykių sritis*[547].

Žvelgiant iš baudžiamosios teisės pozicijų, toks aiškinimas kelia problemų, nes dėl abstrakčių privatumo ribų neįmanoma aiškiai atskirti BK 198 ir BK 166–168 straipsniuose numatytų nusikalstamų veikų – atsižvelgiant į tai, ar duomenys bus siejami su privačiu asmens gyvenimu, ar vadovaujantis *CIA triada* jie vis dėlto bus laikomi konfidencialiais, kvalifikuojant kaltininko veiką bus taikomas skirtingas BK straipsnis. Vadinasi, susiklosčius tokiai situacijai kyla baudžiamojo įstatymo normų konkurencijos problema, kai kelios normos, esančios BK 166, 167, 168 ir BK 198 straipsniuose, gali būti taikomos tai pačiai nusikalstamai veikai, padarytai elektroninėje erdvėje, kvalifikuoti. Sprendžiant šį klausimą, pirmiausia reikėtų atsižvelgti į tai, kad BK XXIV skyriuje yra kriminalizuotos įvairios asmens privatumo pažeidimo apraiškos, be kita ko, ir elektroninėje erdvėje. Dėl to neteisėto privatumo pažeidimo veiksmams kvalifikuoti turėtų būti taikomi BK 166, 167 ar 168 straipsniai, kuriuose esančios normos laikytinos *lex specialis* normai, numatytai BK 198 straipsnyje. Iš esmės kiekvienam privatumo pažeidimui elektroninėje erdvėje vertinti taikomi BK 166, 167 ar 168 straipsniuose esančiai normai būdingi visi

[546] Lietuvos Respublikos Konstitucijos komentaras. Jovaišas, K. (ats. red.). Vilnius: Teisės institutas, 2000, p. 165.

[547] Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendis baudžiamojoje byloje Nr. 1-680-530/2013.

BK 198 straipsnio normos požymiai. Kaip minėta, neviešiems elektroniniams duomenims (neteisėto disponavimo elektroniniais duomenimis dalykui) priskiriami ir įvairių rūšių konfidencialumo aspektą turintys duomenys, todėl galima tvirtinti, kad su asmens privatumu susiję duomenys kartu yra ir nevieši duomenys. Be to, BK 198 straipsnyje numatytos beveik analogiškos pavojingos veikos, kaip ir BK 166, 167 ar 168 straipsniuose: stebėjimas, fiksavimas, perėmimas, įgijimas, BK 167 straipsnyje minimas rinkimas, taip pat paskleidimas ar kitoks panaudojimas. Kartu matyti, kad BK 166, 167 ir 168 straipsniuose, palyginti su BK 198 straipsniu, numatyti tam tikri specifiniai atvejai ir juos atitinkančios normos, kurios taikytinos būtent privatumo pažeidimams elektroninėje erdvėje kvalifikuoti.

Mokslinėje literatūroje pasitaiko ir kitokių baudžiamojo įstatymo saugomų vertybių aiškinimo variantų, kuriais remiantis gali būti formuojama diskutuotina BK 198 straipsnio taikymo praktika. Pavyzdžiui, joje teigiama, kad BK 198 straipsnis „<...> skirtas apsaugoti fizinio ir juridinio asmens privatumą elektroninėje erdvėje, todėl neteisėta veika su elektroniniais duomenimis yra baudžiama. Priklausomai nuo konteksto, sąvoka *nevieši elektroniniai duomenys* gali būti suprantama skirtingai“[548]. Tokiais atvejais kaip neviešų elektroninių duomenų pavyzdys pateikiami privataus asmens elektroniniai laiškai – tai leidžia su jais atliekamus neteisėtus veiksmus laikyti neteisėtu disponavimu neviešais elektroniniais duomenimis ir tokiai veikai kvalifikuoti taikyti BK 198 straipsnį. Iš tikrųjų tokio pobūdžio laiškai atitinka elektroninių duomenų požymius, bet asmens komunikavimo privatumas pirmiausia siejamas su asmens privatumu, todėl neteisėtas įsikišimas į susižinojimo neliečiamumo sritį laikytinas asmens privataus gyvenimo neliečiamumo pažeidimu. Vadinasi, įvairiems neteisėtiems veiksmams, kuriais, pavyzdžiui, perimami, fiksuojami ar stebimi asmens elektroninių ryšių tinklais siunčiami privatūs pranešimai ar kitaip pažeidžiamas asmens susižinojimo neliečiamumas, kvalifikuoti taikytinas ne BK 198, o 166 straipsnis. Šiuo požiūriu vienas iš aktualesnių kasacinės jurisprudencijos pavyzdžių – jau minėta kasacinė nutartis baudžiamojoje byloje Nr. 2K-138/2015, kurioje, be kitų, buvo sprendžiamas ir BK 168 ir 198 straipsniuose numatytų nusikalstamų

[548] Goranin, N.; Mažeika, D. Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos: mokomoji knyga. Kaunas: TEV [i. e. Technologija], 2011, p. 25–26.

veikų atribojimo klausimas. Kasacinės instancijos teismas šioje byloje priėjo prie išvados, kad veika, kuriai būdingas privačių elektroniniu paštu siunčiamų laiškų neteisėtas gavimas ir šios neteisėtai gautos informacijos paskelbimas, kvalifikuotina tik pagal BK 168 straipsnį:

Sprendžiant BK 168 ir 198 straipsniuose numatytų nusikalstamų veikų atribojimo klausimą, visų pirma pažymėtina, kad BK 168 straipsnyje kriminalizuotas asmens privataus gyvenimo pažeidimas ne tik fizinėje, bet taip pat ir elektroninėje erdvėje. Šiame straipsnyje nurodyti neteisėto informacijos apie asmens privatų gyvenimą atskleidimo ar panaudojimo veiksmai, palyginus su BK 198 straipsnyje numatytaisiais, yra konkretesni, tiesiogiai susiję būtent su asmens privataus gyvenimo neliečiamumo pažeidimais. BK 168 straipsnio 1 dalyje numatyta norma turi ir visus bendrojoje normoje (BK 198 straipsnio 1 dalis) nurodytus požymius, tačiau reguliuoja įstatymo leidėjo specialiai išskirtus privataus gyvenimo neliečiamumo pažeidimo atvejus. Todėl BK 168 straipsnio 1 dalyje nurodyta norma laikytina specialiąja, o BK 198 straipsnio 1 dalyje esanti – bendrąja. <...>

<...> L. B., pažeisdamas asmens susižinojimo neliečiamumą, neteisėtai perėmė ir įgijo (nukopijuodamas) privataus pobūdžio susirašinėjimą tarp D. J. ir D. Č., kurį laikė jam priklausančiose elektroninio pašto paskyrose [*duomenys neskelbiami*]. *Teisėjų kolegija atkreipia dėmesį į tai, kad pagal BK 168 straipsnio 1 dalį baudžiamoji atsakomybė kyla ir tais atvejais, kai be asmens sutikimo viešai paskelbiama informacija apie kito žmogaus privatų gyvenimą, jeigu ji buvo surinkta darant BK 165–167 straipsniuose, taigi ir BK 166 straipsnyje, numatytą veiką. Tokiais atvejais, vadovaujantis normų visumos ir dalies konkurencijos sprendimo taisyklėmis, padaryta veika kvalifikuotina taikant tik BK 168 straipsnį. Minėtieji L. B. veiksmai neteisėtai gaunant privataus pobūdžio susirašinėjimą tarp D. J. ir D. Č. atitinka BK 166 straipsnyje nurodytos veikos požymius, taigi šie veiksmai ir tolesnis neteisėtas gautos informacijos paskelbimas kvalifikuotini tik pagal BK 168 straipsnį.*

Bendriausia prasme galima teigti, kad BK 198 straipsnyje esanti norma yra tarsi „rezervinė“ tiems atvejams, kurie nepatenka į specialiųjų normų taikymo sritį. Tokį bendrosios ir specialiosios normų konkurencijos įveikimo taisyklės taikymo pavyzdį galima detaliau aptarti analizuojant BK 166 ir 198 straipsniuose esančių normų tarpusavio santykį. BK 166 ir 198 straipsnių atskyrimo problema kyla spren-

džiant, pagal kurį straipsnį kvalifikuotina veika, jei neteisėtai gauti elektroninių ryšių tinklais siunčiami ar po perdavimo saugomi asmens pranešimai, kurie gali būti laikomi ir neviešais elektroniniais duomenimis. Šiuo požiūriu *komunikacinį privatumą*[549] – vieną iš teisės į privatumo turinį sudarančių elementų – galima analizuoti atskirai pasisakant apie informacinėje sistemoje *perduodamus* ir po perdavimo *saugomus* (*nejudamus*) pranešimus.

Pirmuoju atveju rodomi asmens susižinojimo neliečiamumo pažeidimai neteisėtai gavus asmens pranešimus tuo metu, kai jie buvo perduodami informacinėje sistemoje. Elektroninių ryšių įstatymo 61 straipsnio 1 dalyje įtvirtinta ryšio konfidencialumo užtikrinimo principinė nuostata, kad „draudžiama be faktinių elektroninių ryšių paslaugų naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti pranešimų turinį ir srauto duomenis ar su jais susipažinti, išskyrus atvejus, kai tai galima teisėtai daryti pagal šio įstatymo 66 ir 77 straipsnius. Be faktinių elektroninių ryšių paslaugų naudotojų sutikimo draudžiama atskleisti elektroninių ryšių tinklais perduodamų pranešimų turinį ir (ar) susijusius srauto duomenis arba sudaryti sąlygas sužinoti tokią informaciją ir (ar) susijusius srauto duomenis, išskyrus įstatymo nustatytus atvejus“. Kaip teigiama literatūroje, „ši nuostata detalizuoja Konstitucijos 22 straipsnyje įtvirtinto privataus gyvenimo apsaugos principą elektroninių ryšių kontekste“[550]. Žiūrint iš baudžiamosios teisės pozicijų, susižinojimo slaptumo pažeidimai galėtų būti kvalifikuojami ir pagal BK 198, ir pagal 166 straipsnį. BK 198 straipsnyje kriminalizuotas neteisėtas neviešų elektroninių duomenų stebėjimas, fiksavimas ir perėmimas, o BK 166 straipsnyje atsakomybė numatyta už neteisėtą asmens elektroninių ryšių tinklais siunčiamų pranešimų perėmimą, fiksavimą ar stebėjimą, taip pat neteisėtą asmens pokalbių elektroninių ryšių tinklais fiksavimą, klausymą ar stebėjimą. Sprendžiant šią kvalifikavimo problemą, BK 166 ir 198 straipsniuose numatytas nusikalstamas veikas siūlytina atskirti remiantis tuo, ar kalbama apie susižinojimo slaptumo kaip garantuotos galimybės „laisvai keistis asmeninio pobūdžio informacija jos neat-

[549] Kiškis, M., *et al.* Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006, p. 116.

[550] Jarukaitis, I., *et al*. Elektroninių ryšių teisė. Vilnius: Eugrimas, 2005, p. 340.

skleidžiant tretiesiems asmenims“[551] pažeidimus, ar vis dėlto perimami kiti elektroniniai duomenys, kuriems būdingas konfidencialumo aspektas, bet jie nepriskiriami asmens privatumo sričiai (beje, elektroninių ryšių vartotojai yra ne tik fiziniai, bet ir juridiniai asmenys). Vadinasi, šiuo atveju dėl nusikalstamos veikos dalyko specifikos apie BK 166 straipsnyje numatytą normą galima kalbėti kaip apie specialiąją, palyginti su BK 198 straipsnyje esančia norma. BK 166 straipsnis galėtų būti taikomas, pavyzdžiui, tais atvejais, kai neteisėtai perimami asmens elektroniniai laiškai, trumposios žinutės, naudojantis balso pašto (VoIP) paslauga perduodami duomenys, jei tokia komunikacija yra priskirta asmens privatumo sričiai.

Tokių padarytos nusikalstamos veikos baudžiamojo teisinio vertinimo pavyzdžių, nors ir nedaug, galima rasti teismų praktikoje. Pavyzdžiui, vienoje iš baudžiamųjų bylų konstatuota, kad *A. J., būdamas valstybės tarnautoju (duomenys neskelbtini) ir turėdamas savo žinioje operatyvinio sekimo bylą (duomenys neskelbtini), siekdamas asmeninių tikslų – klausytis asmeniškai pažįstamo J. V. telefoninių pokalbių, suklastojęs <...> [pažymą ir raštą – aut. pastaba] <...> suklaidino <...> prokuroro pavaduotoją, o šis <...> teikimu kreipėsi į <...> teismo pirmininką dėl techninių priemonių panaudojimo specialiąja tvarka. <...> pirmininkas <...> nutartimi <...> sankcionavo operatyvinius veiksmus. Taip pasinaudojęs tarnybiniu pasitikėjimu A. J. nuo 2007-04-12 iki 2007-04-26 <...> patalpose, esančiose (duomenys neskelbtini), neteisėtai klausėsi J. V. pokalbių telefonu, peržiūrėjo telefonu siunčiamus pranešimus. <...> Tokiais veiksmais A. J. diskreditavo valstybės tarnautojo vardą, sumenkino valstybinės institucijos <...> autoritetą ir, suvaržydamas asmens konstitucines teises, padarė didelę žalą valstybės interesams ir fiziniam asmeniui J. V. Tai yra A. J. padarė nusikalstamas veikas, numatytas LR BK 166 str. 1 d. ir 228 str. 2 d.*[552] Šis nuosprendis buvo skųstas apeliacine tvarka, bet Vilniaus apygardos teismas 2008 m. spalio 13 d. nutartimi baudžiamojoje byloje Nr. 1A-791/2008 panaikino tik BK 75 straipsnio 2 dalies 1 punkto taikymą, tačiau nekeitė A. J. padarytų nusikalstamų veikų teisinio vertinimo.

---

[551] Jarukaitis, I., *et al*. Elektroninių ryšių teisė. Vilnius: Eugrimas, 2005, p. 333.

[552] Vilniaus miesto 2 apylinkės teismo 2008 m. liepos 2 d. nuosprendis baudžiamojoje byloje Nr. 1-5-655/2008.

Analizuojant elektroninių ryšių tinklais siunčiamų pranešimų neteisėto stebėjimo, fiksavimo ir perėmimo inkriminavimo probleminius aspektus, gali kilti klausimas, kuris – BK 198 ar 166 straipsnis – turėtų būti taikomas, jei buvo neteisėtai fiksuojami asmens siunčiamų pranešimų srauto duomenys, bet siunčiamo pranešimo turinio duomenys nebuvo perimti. Abejonių, ar BK 166 straipsnis taikytinas ir kvalifikuojant neteisėtą srauto duomenų fiksavimą, kyla dėl pačios šiame straipsnyje vartojamos terminijos – jame yra minimas *pranešimų* perėmimas, fiksavimas ar stebėjimas. Sprendžiant šį klausimą, siūlytina atsisakyti technologiškai specifinio požiūrio į patį pranešimų siuntimo procesą ir į pranešimus žiūrėti kaip į vieną turinio ir srauto duomenų visumą, nes ir turinio, ir srauto duomenys yra būtini siekiant užtikrinti asmenų komunikavimą. Elektroninių ryšių tinklais siunčiami turinio duomenys rodo asmenų bendravimą, o šiems duomenims perduoti sukurti srauto duomenys leidžia tarpusavyje „bendrauti“ ir informacinės sistemos komponentams, kuriais siekiama pristatyti turinio duomenis numatytam adresatui. Toks elektroninių ryšių tinklais siunčiamo pranešimo technologiškai neutralus interpretavimas padėtų užtikrinti ir nuoseklų asmens susižinojimo neliečiamumo pažeidimų baudžiamąjį teisinį vertinimą – BK 166 straipsnis būtų taikomas ir neteisėtai perėmus su asmens privatumu susijusius turinio duomenis, ir fiksavus šiems duomenims perduoti tiesiogiai skirtus srauto duomenis.

Be to, manytina, kad galimybę taikyti BK 166 straipsnį kvalifikuojant neteisėtą srauto duomenų gavimą gali rodyti ir jame numatyta viena iš alternatyvių veikų – pranešimų fiksavimas. Analizuojant BK 198 straipsnį, šią pavojingą veiką siūlyta susieti būtent su neteisėtu srauto duomenų gavimu. Siekiant nuoseklumo, toks fiksavimo aiškinimas galėtų būti taikomas atskleidžiant ir BK 166 straipsnyje numatyto fiksavimo turinį. Dar pabrėžtina, kad nors šiuo klausimu literatūroje pasigendama išsamesnės diskusijos, pavieniais atvejais, kalbant apie BK 166 straipsnio pritaikomumą minėtiesiems atvejams, vis dėlto prieinama prie išvados, kad šiame straipsnyje yra numatyta atsakomybė ne tik už turinio, bet ir srauto duomenų neteisėtą gavimą. Pavyzdžiui, analizuojant Konvencijos dėl elektroninių nusikaltimų 3 straipsnio nuostatas ir įvairius su jomis susijusius nacionalinės teisės suderinamumo aspektus teigiama, kad „įstatymų leidėjas siekė apimti

ir neteisėtą srauto duomenų perėmimą, ir, nors kol kas teismų praktikos nėra, Baudžiamojo kodekso 166 straipsnis taikytinas ir neteisėto srauto duomenų perėmimo atžvilgiu“[553].

Pereinant prie antrojo komunikacijos privatumo pažeidimo atvejo, kai neteisėtai gaunama prieiga prie pranešimų, saugomų po perdavimo elektroninių ryšių tinklais (pavyzdžiui, elektroninio pašto serveryje, mobiliajame telefone ar pan.), galima pabrėžti, kad sunkumų galėtų kilti ne tiek dėl BK 198 ir 166 straipsnių atribojimo, kiek dėl tinkamo BK 166 straipsnyje numatytų požymių inkriminavimo. Analizuojant teismų praktiką matyti, kad saugomiems *(nejudamiems)* pranešimams neabejotinai yra taikomi privatumo apsaugos principai, o neteisėti įsikišimai į susižinojimo neliečiamumo sritį kvalifikuojami pagal BK 166 straipsnį. Pavyzdžiui, vienoje iš baudžiamųjų bylų S. G. pripažinta kalta pagal BK 284 straipsnio 1 dalį ir 166 straipsnio 1 dalį, nes nustatyta, kad *Šilutės mieste (duomenys neskelbtini), stadione, S. G. neteisėtai, prieš nukentėjusiosios valią, paėmė iš V. B. mobiliojo ryšio telefoną „Samsung X640“ ir skaitė mobiliojo ryšio telefone esančias trumpąsias žinutes, toliau tęsdama savo nusikalstamą veiką, <...> būdama Šilutės mieste (duomenys neskelbtini), skaitė nukentėjusiosios mobiliojo ryšio telefone „Samsung X640“ esančias trumpąsias žinutes ir tuo pažeidė V. B. susirašinėjimo techninėmis priemonėmis siunčiamų pranešimų slaptumą*[554]. Susižinojimo slaptumo pažeidimai neteisėtai gavus prieigą prie mobiliojo ryšio telefone esančių pranešimų pagal BK 166 straipsnį kvalifikuoti ir kituose teismų sprendimuose[555]. Taigi nustačius, kad saugomi pranešimai yra susiję su asmens privatumu, įvairiems įsikišimams į susižinojimo neliečiamumo sritį kvalifikuoti taikytinas ne BK 198, o 166 straipsnis. Beje, tokiais atvejais siūlytina inkriminuoti ne perėmimo, fiksavimo ar stebėjimo veikas, kurios straipsnio dispozicijoje yra tiesiogiai siejamos su elektroninių ryšių tinklais *siunčiamų (perduodamų)* pranešimų privatumo pažeidimais, o dispozicijoje minimą požymį – *kitokį asmens susižinojimo neliečiamumo pažeidimą*. Šis, atsižvelgiant į BK 166 straipsnyje nurodytus nusikalstamos veikos

---

553 Jarukaitis, I., *et al*. Elektroninių ryšių teisė. Vilnius: Eugrimas, 2005, p. 348.

554 Šilutės rajono apylinkės teismo 2006 m. birželio 28 d. nuosprendis baudžiamojoje byloje Nr. N1-249-299/2005.

555 Šiaulių rajono apylinkės teismo 2010 m. liepos 19 d. baudžiamasis įsakymas byloje Nr. 1-199-776/2010.

požymius, laikytinas tikslesniu kalbant apie neteisėtą prieigą prie pranešimų ne tada, kai jie yra siunčiami, o kai yra saugomi (laikomi) po jų pristatymo gavėjui.

Vadinasi, remiantis BK 198 ir 166 straipsniuose aprašytų nusikalstamų veikų požymiais, galima nustatyti ribą, kuriais atvejais kaltininko veika pažeidžiamas asmens susižinojimo neliečiamumas, o kuriais – neviešų elektroninių duomenų konfidencialumas. Nors lyginant abu šiuos straipsnius ir kyla nemažai sudėtingų klausimų, susijusių su juose numatytų nusikalstamų veikų baudžiamumu, būtent BK 198 ir 166 straipsniuose nustatytos sankcijos parodo asmens susižinojimo neliečiamumo pažeidimo ir neteisėto disponavimo neviešais elektroniniais duomenimis nusikalstamų veikų disbalansą. Įstatymų leidėjui neatsižvelgus į šių veikų ryšį buvo sukurta situacija, kai dėl asmens privatumo pažeidimų yra taikoma perpus švelnesnė baudžiamoji atsakomybė nei neviešų elektroninių duomenų konfidencialumo pažeidimų atveju – BK 166 straipsnyje esanti nusikalstama veika yra nesunkus nusikaltimas, o BK 198 straipsnio 1 dalyje numatyta veika – apysunkis nusikaltimas. Beje, tinkamai nenustatytas ir kitų nusikalstamų veikų ryšys – neteisėtas disponavimas neviešais elektroniniais duomenimis (BK 198 straipsnio 1 dalis) yra baudžiamas griežčiau nei, pavyzdžiui, neteisėtas disponavimas informacija, kuri yra valstybės paslaptis (BK 124 straipsnis), tarnybos paslapties pagrobimas ar kitoks neteisėtas įgijimas (BK 296 straipsnis), tarnybos paslapties atskleidimas (BK 297 straipsnis), neteisėtas informacijos apie privatų asmens gyvenimą rinkimas (BK 167 straipsnis) ir daugelis kitų. Toks teisinis reguliavimas reikštų, kad daugeliu BK 198 straipsnyje esančiai bendrajai normai sukurtų specialiųjų normų numatomos privilegijuotos nusikalstamų veikų sudėtys, o pačios veikos pavojingumas dažniausiai mažinamas dėl nusikalstamos veikos dalyko specifikos: pavyzdžiui, mažesnį veikos pavojingumą rodo neteisėtas disponavimas duomenimis, sudarančiais valstybės, tarnybos paslaptį, asmens siunčiamais pranešimais ar pan. Atsižvelgiant į tai teigtina, kad toks teisės normų ryšys neparodo tikrosios baudžiamojo įstatymo saugomų vertybių tarpusavio sąsajos ir negali būti laikomas tinkamu.

Apibendrinant galima teigti, kad privatumo, jo vidinės struktūros analizė suteikė galimybę suformuluoti nors ir bendrojo pobūdžio, bet kartu ir orientacinį, tiesiogiai su baudžiamojo įstatymo vertybe

susijusį BK XXIV skyriuje ir 198 straipsnyje numatytų nusikalstamų veikų atskyrimo kriterijų. Tais atvejais, kai nusikalstama veika elektroninėje erdvėje pažeidžiamas asmens privataus gyvenimo neliečiamumas, teisiškai vertinant šią veiką taikytini BK XXIV skyriuje esantys BK straipsniai, o kitais atvejais, nustačius neviešų elektroninių duomenų disponavimo pažeidimus, inkriminuotina kita – BK 198 straipsnyje nurodyta nusikalstama veika (jei šiame straipsnyje esančiai normai netaikytina specialioji norma).

1. Nusikalstamos veikos elektroninėje erdvėje yra tradicinės nusikalstamos veikos, kurios gali būti padaromos ir fizinėje, ir elektroninėje erdvėje, taip pat veikos, kurios išimtinai priskiriamos informacinių technologijų veiklos rezultatui ir fizinėje erdvėje neegzistuoja. Šių nusikalstamų veikų įvairovė yra susijusi su kiekybiškai daug ir kokybiškai naujomis baudžiamosios teisės problemomis, t. y. tinkamu tokių veikų kriminalizavimu, sisteminimu ir aiškinimu.

1.1. Elektroninės erdvės saugumas, padedantis atskleisti įvairias elektroninėje erdvėje kylančias grėsmes, yra baudžiamojo įstatymo saugoma vertybė, kuria remiantis nustatomos tradicinės nusikalstamos veikos, padaromos elektroninėje erdvėje. Techninis kompiuterių saugumas, kaip baudžiamojo įstatymo saugoma vertybė, yra siejamas su *CIA triada* ir suteikia galimybių BK XXX skyriuje numatytas nusikalstamas veikas grupuoti į elektroninių duomenų ir informacinių sistemų konfidencialumo, integralumo bei prieinamumo pažeidimus.

Neviešų elektroninių duomenų ir informacinių sistemų, kurioms būdinga apribota (ar atsieta) prieiga, konfidencialumas rodo esant tam tikrų prieigos prie šių duomenų ir sistemų apribojimų, t. y. elektroniniai duomenys ir informacinės sistemos yra prieinamos tik asmenims (ar procesams), turintiems tokią teisę, ir tik tiek, kiek apima jiems suteikta teisė.

1.2. Vadovaujantis ekvivalentinio vertinimo principu, tradicinė nusikalstama veika, padaryta elektroninėje erdvėje, kvalifikuotina tik pagal šią tradicinę veiką įtvirtinantį BK straipsnį – tokiais atvejais kaltininkui BK XXX skyriuje numatyti straipsniai papildomai neinkriminuotini. Remiantis lygiaverčio vertinimo idėja siūloma kiek įmanoma lanksčiau pažvelgti į tradicinių nusikalstamų veikų sudėties požymius, jų aiškinimą pritaikant ir analogiškoms nusikalstamoms veikoms, padarytoms elektroninėje erdvėje.

Baudžiamoji atsakomybė už išimtinai tik elektroninėje erdvėje padaromas nusikalstamas veikas, kurioms nėra tiesiogiai pritaikomų analogų fizinėje erdvėje, nustatoma taikant BK XXX skyriuje įtvirtintas atskiras baudžiamojo įstatymo normas.

1.3. Aiškinant nusikalstamų veikų, padarytų elektroninėje erdvėje, sudėties požymius yra svarbios informacines technologijas apibrėžiančios sąvokos. Su tuo susijusios problemos paprastai sprendžiamos taikant technologinio neutralumo principą, kuriuo draudžiama teikti prioritetą kuriai nors vienai technologijai. Kita vertus, atsisakius technologijų specifiškumo, baudžiamajame įstatyme numatyti ne taip konkrečiai apibrėžti ir lanksčiau taikomi sudėties požymiai gali lemti nenuspėjamą jų apimtį, taigi ir baudžiamosios atsakomybės taikymo ribų nustatymo sunkumus. Vadinasi, elektroninėje erdvėje padarytoms nusikalstamoms veikoms kvalifikuoti itin aktualūs baudžiamosios teisės principai, leidžiantys išvengti pernelyg plataus bei nepagrįsto veikų kriminalizavimo, atitinkamai ir nepagrįsto baudžiamosios atsakomybės ribų išplėtimo.

2. Baudžiamoji atsakomybė už informacinės sistemos konfidencialumo pažeidimus numatyta BK 198[1] straipsnyje. Šiame straipsnyje neteisėtas prisijungimas prie informacinės sistemos yra kriminalizuotas kaip pavojingas pats savaime *(per se)*, nesant tiesioginės sąsajos su kitomis sistemoje padaromomis nusikalstamomis veikomis. Kadangi galimybių padaryti nusikalstamas veikas sistemoje, kuriai būdinga apribota (ar atsieta) prieiga, dažniausiai atsiranda dėl pirminių neteisėtų kaltininko prisijungimo veiksmų, todėl neturėtų stebinti dažni BK 198[1] straipsnyje numatytos veikos inkriminavimo atvejai. Toks šios nusikalstamos veikos kriminalizavimas turi įtakos atskleidžiant ir jos sudėties požymių turinį.

2.1. Neteisėtą prisijungimą prie informacinės sistemos kriminalizavus *per se,* suteikiamos ribotos galimybės neteisėtą prieigą pripažinti ir kaip teisėtumo ribas peržengiančią prieigą. Siauresnis aiškinimas leidžia išvengti perteklinio veikų kriminalizavimo ir padeda užtikrinti, kad baudžiamosios teisės reguliavimo sričiai nebūtų priskirti įvairūs civiliniai ar drausminiai teisiniai santykiai.

2.2. Prisijungimo prie informacinės sistemos neteisėtumas konstatuotinas nustačius ir autentifikavimo procedūrų pažeidimą, ir pasinaudojimą silpnosiomis informacinės sistemos apsaugos priemonių vietomis.

2.3. BK 198[1] straipsnyje numatytas nusikalstamos veikos dalykas – informacinė sistema (jos dalis) iš baudžiamosios teisės pozicijų turėtų būti suvokiama neatsižvelgiant į jos funkcionavimo kontekstą ir bendriausia prasme galėtų būti laikoma informacinių technologijų (apimančių ir komunikacijos technologijas) arba kompiuterinės sistemos sinonimu. Strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turinti informacinė sistema yra neteisėtą prisijungimą prie informacinės sistemos kvalifikuojanti aplinkybė (BK 198[1] straipsnio 2 dalis). Nustatant ypatingą informacinės sistemos svarbą valstybės valdymui, ūkiui ar finansų sistemai, taikytini *nukentėjusiųjų*, *ekonominio poveikio* ir *poveikio visuomenei* kriterijai.

2.4. Aiškinant prisijungimą prie informacinės sistemos taikytinas *vidinės perspektyvos* požiūris, kuriuo remiantis elektroninė erdvė apibūdinama kaip virtualioji realybė. Dėl to, neatsižvelgiant į tai, ar prisijungimas yra interpretuojamas kaip komanda, kuria pradedamas darbo su informacine sistema seansas, ar jis suvokiamas kaip galimybė prieiti prie informacinės sistemos išteklių, ši pavojinga veika yra metaforiškai prilyginama *virtualiajam įėjimui* į sistemą. Toks aiškinimas reikštų, kad neteisėto prisijungimo veiksmui konstatuoti nepakanka tik sąveikos su informacine sistema.

Neteisėto prisijungimo prie informacinės sistemos baigtumo momentui neturi įtakos tai, ar kaltininkas atliko ar ketino atlikti kitus neteisėtus veiksmus sistemoje.

2.5. Siekiant išvengti akivaizdžiai nepavojingų veikų kriminalizavimo, neteisėto prisijungimo prie informacinės sistemos veikos taikymo galimybės susiaurinamos į šios veikos sudėtį įtraukiant ir jos padarymo būdą – informacinės sistemos apsaugos priemonių pažeidimą. Šioms priemonėms aiškinti taikytina technologinė informacinių sistemų apsaugos priemonių koncepcija. Platesnis šių priemonių interpretavimas

galimas tik tuo atveju, jei prieš tai įvertinama neteisėto prisijungimo prie informacinės sistemos perteklinio kriminalizavimo grėsmė.

Informacinės sistemos apsaugos priemonių pažeidimas interpretuotinas ne tik kaip žalos apsaugos priemonėms padarymas, bet ir kaip tokioms priemonėms nustatytų apribojimų (reikalavimų) pažeidimas, kai žalos pačioms apsaugos priemonėms gali būti ir nepadaroma.

2.6. Neteisėto prisijungimo prie informacinės sistemos veika gali būti padaroma tik tiesiogine tyčia (BK 15 straipsnio 2 dalies 1 punktas). Šiai kaltei pagrįsti yra svarbus *vidinės perspektyvos* požiūris į elektroninę erdvę, leidžiantis į nustatytų ribų ir jų peržengimo neteisėtumą pažvelgti pirmiausia iš elektroninės erdvės vartotojo pozicijos. Vadinasi, šioje erdvėje nustatytų apribojimų suvokimui vertinti taikytinas tokių apribojimų ir jų pažeidimo *numatomumo* kriterijus – jis suteikia galimybių atsižvelgti į asmens patyrimą elektroninėje erdvėje kaip *vietoje*.

3. Baudžiamoji atsakomybė už neviešų elektroninių duomenų konfidencialumo pažeidimus numatyta BK 198 straipsnyje. Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstama veika kriminalizuota gana plačiai – BK 198 straipsnyje nustatyta atsakomybė ir už neteisėtą disponavimą informacinėje sistemoje *perduodamais,* ir joje *laikomais* duomenimis. Šiai veikai baudžiamajame įstatyme nepriskiriama jokių papildomų požymių (pavyzdžiui, techninių priemonių taikymo, kaltininko nusikalstamų ketinimų), galinčių padėti išvengti jos perteklinio kriminalizavimo problemų.

3.1. Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstamos veikos dalykas apibūdinamas remiantis dviem – teisiniu ir technologiniu – aspektais. Teisinis aspektas siejamas su elektroninių duomenų neviešumu. Elektroninių duomenų neviešumas rodo, kad šie duomenys priskiriami duomenų, kuriems taikomas tam tikras apsaugos lygis – atitinkami konfidencialumo apsaugos reikalavimai, rūšiai. Neviešumo pagrindas gali būti objektyvus – kildinamas iš įstatymų ar kitų teisės aktų reikalavimų, ir subjektyvus – kylantis iš asmenų susitarimų, privačių tikslų ir kt.

Technologinis elektroninių duomenų aspektas yra siejamas su tokių duomenų elektronine forma. Duomenų elektroninei formai nustatyti taikytini jų *tinkamumo apdoroti informacinėje sistemoje* arba tokių *duomenų buvimo informacinėje sistemoje* kriterijai.

Strateginę reikšmę nacionaliniam saugumui arba didelę reikšmę valstybės valdymui, ūkiui ar finansų sistemai turintys elektroniniai duomenys yra neteisėto elektroninių duomenų perėmimo ir panaudojimo veiką kvalifikuojanti aplinkybė. Jai nustatyti taikytini *nukentėjusiųjų*, *ekonominio poveikio* ir *poveikio visuomenei* kriterijai. Ypatingą elektroninių duomenų svarbą, be kita ko, gali rodyti ne tik tokių duomenų turinys, bet ir itin didelis jų kiekis. Tokiais atvejais pavieniai duomenys, dėl savo turinio nelaikomi ypatingos svarbos, šią savybę gali įgyti dėl neteisėto disponavimo jais kiekio.

3.2. Aiškinant BK 198 straipsnyje numatytas alternatyvias veikas problemų kyla dėl to, kad šio straipsnio dispozicijoje nusikalstamos veikos dalykas – nevieši elektroniniai duomenys – nėra sukonkretinti iki informacinėje sistemoje *laikomų* ir informacinėje sistemoje *perduodamų* duomenų. Dėl to kyla neaiškumų, su kuria iš minėtųjų duomenų rūšių sietina kiekviena iš alternatyvių BK 198 straipsnyje įtvirtintų stebėjimo, fiksavimo, perėmimo, įgijimo, laikymo, pasisavinimo, paskleidimo ar kitokio panaudojimo veikų. Siūlytina stebėjimo, fiksavimo ir perėmimo veikas sieti tik su neteisėtu informacinėje sistemoje *perduodamų* duomenų gavimu. Atitinkamai elektroninių duomenų įgijimo veika inkriminuotina tik tais atvejais, kai neteisėtai gaunami informacinėje sistemoje *laikomi* elektroniniai duomenys.

3.3. Neteisėto elektroninių duomenų perėmimo ir panaudojimo nusikalstama veika gali būti padaroma tik tyčia (BK 15 straipsnis). Konstatuojant tyčinę kaltę ir elektroninių duomenų konfidencialumo pažeidimo suvokimą, elektroninėje erdvėje taikomi apribojimai vertintini vadovaujantis *vidinės perspektyvos* požiūriu, leidžiančiu atsižvelgti į elektroninės erdvės vartotojo patirtį šioje erdvėje kaip *vietoje*. Tokiais atvejais vertinant prieigos prie elektroninių duomenų nustaty-

tus apribojimus taikytinas jų *numatomumo kriterijus*, kuriuo remiantis reikalaujama nustatyti, kad asmuo suvokė esamus apribojimus ir jų nesilaikydamas pažeidė elektroninių duomenų konfidencialumą.

4. Kadangi nusikalstamomis veikomis elektroninėje erdvėje yra laikomos ir tradicinės nusikalstamos veikos, pakitusios dėl informacinių technologijų taikymo, ir specifinės nusikalstamos veikos elektroninių duomenų bei informacinių sistemų saugumui, tai kvalifikuojant kaltininko padarytas veikas elektroninėje erdvėje kyla tokių veikų atskyrimo sunkumų.

4.1. Nustačius, kad prie informacinės sistemos buvo neteisėtai prisijungta naudojantis neviešais elektroniniais duomenimis arba padarytas neteisėtas poveikis elektroniniams duomenims, būtina spręsti, ar, be BK 198[1] straipsnyje numatytos veikos, inkriminuotinos ir BK 196 ar 198 straipsniuose nurodytos veikos. Atsižvelgiant į neteisėto prisijungimo prie informacinės sistemos mechanizmo ypatybes, tokią veiką siūlytina kvalifikuoti tik pagal BK 198[1] straipsnį.

4.2. Baudžiamoji atsakomybė už įvairaus pobūdžio neteisėto disponavimo elektroniniais duomenimis veiksmus numatyta ne tik BK 198 straipsnyje, bet iš dalies ir BK 198[2] bei 214, 215 straipsniuose. Nustačius, kad kaltininkas įgijo visus BK 214 straipsnyje nurodytus požymius atitinkančius duomenis, jo veikai kvalifikuoti taikytinos ne BK 198 ar 198[2] straipsniuose numatytos normos, o specialioji, esanti BK 214 straipsnyje. Pavojinga veika, kuriai būdingas neteisėtas finansinės operacijos inicijavimas naudojantis elektroninės mokėjimo priemonės vartotojo tapatybės patvirtinimo priemonių duomenimis, kvalifikuojama taikant ne BK 198, o 215 straipsnį.

4.3. BK XXIV skyriuje kriminalizuotos įvairios asmens privatumo pažeidimo apraiškos, be kita ko, ir elektroninėje erdvėje, dėl to kyla BK 198 straipsnyje ir minėtajame BK skyriuje aprašytų nusikalstamų veikų atskyrimo sunkumų. Nustatyti neteisėti privatumo pažeidimo veiksmai yra kvalifikuojami pagal BK 166, 167 ar 168 straipsnius. Šiuose straipsniuose esančios normos laikytinos specialiosiomis lyginant su BK 198 straipsnyje numatyta norma.

Literatūra

Lietuvos Respublikos norminiai teisės aktai

1. Lietuvos Respublikos Konstitucija. *Valstybės žinios,* 1992, Nr. 33-1014.
2. Lietuvos Respublikos baudžiamojo proceso kodeksas. *Valstybės žinios,* 2002, Nr. 37-1341.
3. Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios,* 2000, Nr. 89-2741.
4. Lietuvos Respublikos kriminalinės žvalgybos įstatymas. *Valstybės žinios,* 2012, Nr. 122-6093.
5. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. *Valstybės žinios,* 2011, Nr. 163-7739.
6. Lietuvos Respublikos baudžiamojo kodekso 7, 38, 47, 63, 66, 70, 75, 82, 93, 129, 166, 167, 172, 178, 180, 181, 182, 183, 184, 185, 189, 194, 196, 197, 198, 198^1, 198^2, 199, 202, 213, 214, 215, 225, 227, 228, 231, 233, 235, 252, 256, 257, 262, 284, 285, 312 straipsnių, priedo pakeitimo ir papildymo, XXVI, XXX skyrių pavadinimų pakeitimo ir kodekso papildymo 256^1, 257^1 straipsniais įstatymas. *Valstybės žinios,* 2007, Nr. 81-3309.
7. Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios,* 2004, Nr. 69-2382.
8. Lietuvos Respublikos baudžiamojo kodekso 13, 162, 191, 197, 203, 206, 216, 219, 221, 309 straipsnių pakeitimo ir papildymo 198^1 ir 198^2 straipsniais įstatymas. *Valstybės žinios,* 2004, Nr. 25-760.
9. Lietuvos Respublikos strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas. *Valstybės žinios,* 2002, Nr. 103-4604.
10. Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios,* 2000, Nr. 61-1827.
11. Lietuvos Respublikos mokėjimų įstatymas. *Valstybės žinios,* 1999, Nr. 97-2775.
12. Lietuvos Respublikos civilinės saugos įstatymas. *Valstybės žinios,* 1998, Nr. 115-3230.
13. Lietuvos Respublikos visuomenės informavimo įstatymas. *Valstybės žinios,* 1996, Nr. 71-1706.
14. Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“. *Valstybės žinios,* 2011, Nr. 83-4033.

15. Lietuvos Respublikos Vyriausybės 2011 m. rugpjūčio 17 d. nutarimu Nr. 943 patvirtintas Europos ypatingos svarbos infrastruktūros objektų nustatymo, priskyrimo šiems objektams ir jų saugumui užtikrinti būtinų priemonių parengimo tvarkos aprašas. *Valstybės žinios,* 2011, Nr. 105-4950.
16. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. spalio 21 d. įsakymas Nr. 1V-1013 „Dėl viešųjų ryšių tinklų ir viešųjų elektroninių ryšių paslaugų saugumo ir vientisumo užtikrinimo taisyklių patvirtinimo". *Valstybės žinios,* 2011, Nr. 130-6174.
17. Lietuvos Respublikos Vyriausybės 2010 m. birželio 7 d. nutarimas Nr. 717 „Dėl objektų pripažinimo valstybinės reikšmės objektais tvarkos aprašo patvirtinimo". *Valstybės žinios,* 2010, Nr. 69-3442.

Užsienio valstybių norminiai teisės aktai

1. Computer Misuse Act [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://www.legislation.gov.uk/ukpga/1990/18/section/1*>.
2. Cyprus Law No. 22(III)04 [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: <*https://www.coe.int/en/web/cybercrime/country-profiles*>.
3. Criminal Code of the Republic of Bulgaria [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: <*https://www.coe.int/en/web/cybercrime/country-profiles*>.
4. Penal Code of the Republic of Estonia [interaktyvus. Žiūrėta 2018-05-02]. Prieiga per internetą: <*https://www.riigiteataja.ee/en/eli/ee/522012015002/consolide/current*>.
5. Penal Code of the French Republic [interaktyvus. Žiūrėta 2018-04-23]. Prieiga per internetą: <*http://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations*>.
6. Criminal Code of the Federal Republic of Germany [interaktyvus. Žiūrėta 2018-04-23]. Prieiga per internetą: <*http://www.gesetze-im-internet.de/englisch_stgb/index.html*>.
7. Criminal Code of the Republic of Latvia [interaktyvus. Žiūrėta 2018-08-10]. Prieiga per internetą: <*www.vvc.gov.lv/export/sites/default/docs/LRTA/Citi/The_Criminal_Law.doc*>.
8. Criminal Code of the Republic of Poland [interaktyvus. Žiūrėta 2018-04-23]. Prieiga per internetą: <*http://www.legislationline.org/documents/section/criminal-codes/country/10*>.
9. Criminal Code Russian Federation [interaktyvus. Žiūrėta 2018-04-23]. Prieiga per internetą: <*http://www.russian-criminal-code.com*>.
10. The Code of the United States [interaktyvus. Žiūrėta 2018-04-14]. Prieiga per internetą: <*http://www.law.cornell.edu/uscode/text/18/1030*>.

11. The Code of Maryland [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://law.justia.com/codes/maryland/2010/criminal-law/title-7/subtitle-3/7-302*>.
12. Regulation of Investigatory Powers Act [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: <*http://www.legislation.gov.uk/ukpga/2000/23/section/1*>.

Tarptautiniai ir Europos Sąjungos teisės aktai

1. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios,* 1995, Nr. 40-987.
2. Europos Tarybos konvencija dėl elektroninių nusikaltimų. *Valstybės žinios,* 2004, Nr. 36-1188.
3. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR [2013] OL L 218/8.
4. 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos 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.
5. Europos Sąjungos Tarybos 2008 m. gruodžio 8 d. direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo [2008] OL L345/76.
6. Europos Sąjungos Tarybos 2005 m. vasario 24 d. pagrindų sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas [2005] OL L 69/67.
7. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions of 10 November 1999. Towards a new framework for Electronic Communications infrastructure and associated services - The 1999 Communications Review (COM/99/0539 final) [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:1999:0539:FIN*>.

Lietuvos Respublikos Konstitucinio Teismo jurisprudencija

1. Lietuvos Respublikos Konstitucinio Teismo 2006 m. sausio 16 d. nutarimas.
2. Lietuvos Respublikos Konstitucinio Teismo 2005 m. rugsėjo 29 d. nutarimas.
3. Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 13 d. nutarimas.
4. Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas.
5. Lietuvos Respublikos Konstitucinio Teismo 2003 m. kovo 24 d. nutarimas.
6. Lietuvos Respublikos Konstitucinio Teismo 2003 m. birželio 10 d. nutarimas.

7. Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas.
8. Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas.
9. Lietuvos Respublikos Konstitucinio Teismo 2000 m. gegužės 8 d. nutarimas.
10. Lietuvos Respublikos Konstitucinio Teismo 1999 m. spalio 21 d. nutarimas.

Specialioji literatūra

1. A Dictionary of Computing. 5-asis leidimas. Daintith, J. (gen. ed.). Oxford: Oxford University Press, 2004.
2. Abramavičius, A., *et al*. Baudžiamoji teisė. Bendroji dalis. 3-iasis pataisytas ir papildytas leidimas. Vilnius: Eugrimas, 2001.
3. Abramavičius, A., *et al*. Lietuvos baudžiamojo kodekso komentaras. Specialioji dalis (99–212 straipsniai). Vilnius: Registrų centras, 2009.
4. Abramavičius, A., *et al*. Lietuvos Respublikos baudžiamojo kodekso komentaras. Specialioji dalis (213–330 straipsniai). Vilnius: Registrų centras, 2010.
5. Ali, R. Technological Neutrality. *Lex Electronica*, 2009, 14(2).
6. Bainbridge, D. Introduction to Computer Law. 5-asis leidimas, Harlow: Pearson: Longman, 2004.
7. Baudžiamasis procesas: nuo teorijos iki įrodinėjimo (prof. Eugenijaus Palskio atminimui): mokslo studija. Vilnius: Mykolo Romerio universitetas, 2011.
8. *Baudžiamoji justicija ir verslas: recenzuotų mokslinių straipsnių rinkinys.* Švedas, G. (vyr. red.). Vilnius: Vilniaus universiteto Teisės fakultetas, 2016.
9. Beynon-Davies, P. Business information systems. Basingstoke; New York (N.Y.): Palgrave Macmillan, 2013.
10. Bikelis, S. Tyčinė kaltė baudžiamosios teisės teorijoje ir praktikoje: daktaro disertacija. Vilnius: Mykolo Romerio universitetas, 2007.
11. Bishop, M. Computer Security: Art and Science. Addison Wesley Professional, 2003.
12. Black's Law Dictionary. 9-asis leidimas. Garner, B. A. (ed. in chief). St. Paul (Minn.): West: Thomson Reuters business, 2009.
13. Blundell, B. G. Computer Systems and Networks. London: Thomson: Middesex University Press, 2007, p. 244.
14. Blunn, A. S. Report of the Review of the Regulation of Access to Communications. Australija, 2005 [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: *<http://www.ag.gov.au/Publications/Documents/Blunn%20report%20of%20the%20review%20of%20the%20regulation%20of%20access%20to%20communications%20-%20August%202005/xBlunn%20Report%2013%20Sept.pdf>*.

15. Brenner, S. W. Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology*, 2004, 9(13).
16. Brian, Ch. J. The Online/Offline Cognitive Divide: Implications for Law. *SCRIPTed*, 2016, 13(1).
17. Brunner, E. M.; Suter, M. International CIIP Handbook 2008/2009 [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf*>.
18. Budnikas, A., *et al*. Elektroninės valdžios sauga. Kaunas: Vitae Litera, 2008.
19. Bukelienė, D. Baudžiamoji atsakomybė už turto pasisavinimą ir turto iššvaistymą (teoriniai ir praktiniai aspektai). Vilnius: Eugrimas, 2008.
20. Civilka, M., *et al*. Informacinių technologijų teisė. Vilnius: NVO Teisės institutas, 2004.
21. Cybercrime and Jurisdiction: a global survey. Koops, B. J.; Brenner, S. (eds). The Hague: T.M.C. Asser Press, 2006.
22. Cybercrime: Digital Cops in a Networked Environment. Balkin, J., *et al*. (edit.). New York (N.Y.): New York University Press, 2007.
23. Cybercrimes: A Multidisciplinary Analysis. Ghosh, S.; Turrini, E. (eds). Berlin: Springer, 2010.
24. Clough, J. Data Theft? Cybercrime and the Increasing Criminalization of Access to Data. *Criminal Law Forum,* 2011, 22.
25. Clough, J. Principles of Cybercrime. Cambridge: Cambridge University Press, 2010.
26. Comprehensive Study on Cybercrime. UNODC, 2013 [interaktyvus. Žiūrėta 2018-05-01].
27. Computer and Information security handbook. Vacca, J. R. (ed.). Amsterdam: Elsevier: Morgan Kaufmann, 2009.
28. Computer law. Reed, C. (ed). Oxford: Oxford University Press, 2011.
29. Computer Law: The Law and Regulation of Information Technology. 6-asis leidimas. Reed, C.; Angel, J. (eds.). Oxford: Oxford University Press, 2007.
30. Computer security handbook. 4-oji laida. Hutt, A. E.; Bosworth, S.; Hoyt, D. B. (eds). New York, *et al*. Wiley, 2002.
31. Convention on Cybercrime Explanatory Report [interaktyvus. Žiūrėta 2018-04-07]. Prieiga per internetą: <*http://conventions.coe.int/Treaty/en/Reports/Html/185.htm*>.
32. Česnys, A.; Juknius, J. Saugumo patikros ir etiško įsilaužimo technologijos. Kaunas: Technologija, 2011.
33. Dabartinės lietuvių kalbos žodynas. Keinys, S., *et al*. (red). 4-asis leidimas. Lietuvių kalbos institutas, 2000.

34. Prieiga per internetą: <*http://www.unodc.org/unodc/en/cybercrime/egm-on-cybercrime.html*>.
35. Dabartinės lietuvių kalbos žodynas. Keinys, S. (vyr. red.). 7-asis pataisytas ir papildytas leidimas. Vilnius: Lietuvių kalbos institutas, 2012.
36. Dagienė, V., *et al*. Enciklopedinis kompiuterijos žodynas. Vilnius: TEV, 2008.
37. Dictionary of Information Science and Technology. I tomas. Khosrow-Pour, M. (ed.). Hershey, Pa., *et al*. Idea Group Reference, 2007.
38. Dictionary of Information Technology. 2-asis leidimas. Greasby, L.; Green, Th. (eds). Teddington: Peter Collin Publishing, 1996.
39. Digital anonymity and the law: tensions and dimensions. Nicoll, C.; Prins, J. E. J.; van Dellen, M. J. M. (eds). The Hague: T.M.C. Asser Press, 2003.
40. Domeika, P. Apskaitos informacinė sistema. Kaunas: Spalvų kraitė, 2008.
41. Downing, R. W. Shoring up the Weakest Link: What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime. *Columbia Journal of Transnational Law*, 43(3).
42. Drakšienė, A. Baudžiamoji atsakomybė už vagystę. *Teisė,* 2000, Nr. 37.
43. Dulinskas, D.; Dulinskienė, J. ECDL visiems: kompiuterinio raštingumo pagrindai. Kaunas: Informacinių technologijų mokymo centras, 2006.
44. Dzemydienė, D.; Naujikienė, R. Informacinės sistemos. Duomenų struktūros ir valdymas. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2004.
45. El Gamal, A. A.; Kim, Y. H. Network Information Theory. Cambridge: Cambridge University Press, 2011.
46. Enciklopedinis kompiuterijos žodynas. 2-asis papildytas leidimas. Vilnius: TEV, 2008.
47. Erickson, J. Hakingas. Programų kodo narstymo menas. 2-asis pataisytas ir papildytas leidimas. Kaunas: Smaltija, 2010.
48. Fedosiuk, O. Baudžiamoji atsakomybė kaip kraštutinė priemonė (*ultima ratio*): teorija ir realybė. *Jurisprudencija*, 2012, 19(2).
49. Fedosiuk, O.; Marcinauskaitė, R. Criminalization of Cybercrime and Principle of Equivalence. *Administratīvā un krimināla justīcija,* 2013, 2(63): 8.
50. Funk & Wagnalls standard dictionary of the English language: combined with Britannica world language dictionary. I tomas. Chicago (III.): Encyclopaedia Britannica, 1960.
51. Girdenis, T. Nusikalstamų veikų daugetas Lietuvos baudžiamojoje teisėje: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: Mykolo Romerio universitetas, 2010.

52. Goranin, N.; Mažeika, D. Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos: mokomoji knyga. Kaunas: TEV [i.e. Technologija], 2011.
53. Gordon, J. R.; Gordon, S. R. Information systems. 2-asis leidimas. The Dryden Press: Harcourt Brace College Publisher, 1999.
54. Greenberg, B. A. Rethinking Technology Neutrality. *Minnesota Law Review*, 2016, 100(1495).
55. Gupta, U. Information Systems. Upper Saddle River, New Jersey: Prentice-Hall Inc., 2000.
56. Hughes, J. The Internet and the Persistence of Law. *Boston College Law Review*, 2003, 44(359).
57. Information technology and Moral Philosofy. Hoven, van den J.; Weckert, J. (eds). Cambridge, *et al*: Cambridge Univesity Press, 2008.
58. Jarukaitis, I., *et al*. Elektroninių ryšių teisė. Vilnius: Eugrimas, 2005.
59. Jonušauskas, S.; Bilevičienė, T.; Kažemikaitis, V. Įvadas į informatiką. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002.
60. Kalpokas, V.; Marcinauskaitė, R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas. *Teisės problemos,* 2012, 3(77).
61. Kanapeckas, P., *et al*. Kompiuterių elementai [elektroninis išteklius]. Kaunas: Technologija, 2011.
62. Kašėta, S.; Adomkus, T. Telefonijos informacijos ir VoIP sauga. Kaunas: Vitae Litera, 2008.
63. Kazanavičius, E., *et al*. Informacijos saugos vadyba. Kaunas: Vitae Litera, 2008.
64. Kazanavičius, E., *et al*. Programų sauga [elektroninis išteklius]: mokomoji knyga. Kaunas: TEV, 2011.
65. Kerr, O. S. Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse.
66. Kerr, O. S. Norms of Computer Trespass. *Columbia Law Review,* 2016, 116.
67. Kerr, O. S. The Problem of Perspective in Internet Law. *Georgetown Law Journal*, 2003, 91.
68. Kettemann, M. C. Ensuring Cybersecurity through International Law. *REDI*, 2017, 69(2).
69. Khokins, Dzh. M. The Oxford Dictionary of the English Language. Moskva: OOO «Izdatelstvo Actrel», OOO «Izdatelstvo AST», 2001.
70. Kinis, U. From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure procedure (hereinafter -RVDP): The Latvian approach. *Computer law & Security Review*, 2018, 34(3).

71. Kirby, C. A. Defining Abusive Software to Protect Computer Users from the Threat of Spyware. *Science and Law Review*, X(3).
72. Kiškis, M., *et al.* Teisės informatika ir informatikos teisė. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006.
73. Kohl, U. Legal Reasoning and Legal Change in the Age of the Internet – Why the Ground Rules are still Valid. *International Journal of Law and Information Technology*, 1999, 7(2).
74. Kompiuterija. Burgis, B.; Kulikauskas, A. (red.). Kaunas: Naujasis lankas, 2000.
75. Koops, B. J. Should ICT regulation be Technology-Neutral? [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746*>.
76. Kurs ugolovnogo prava: uchebnik [The course of criminal law: The textbook]. Kuznecoba, N. F.; Tjazhkova, I. M. (red). Moskva: Zercalo-M, 2002.
77. Lankauskas, M.; Mulevičius, M.; Zaksaitė, S. Teisės į privatumą, minties, sąžinės, religijos laisvę ir saviraišką užtikrinimo problemos: mokslo studija. Vilnius: Lietuvos teisės institutas, 2013.
78. Laučius, J.; Vasilecas, O. Informacinių technologijų projektų ir kokybės valdymas: mokomoji knyga. Vilnius: Technika, 2007.
79. Laudon, K. C.; Laudon, J. P. Essentials of Management Information Systems. 3-iasis leidimas. New Jersey: Prentice-Hall, Inc., 1999.
80. Laurinaitis, M. Elektroninių pinigų teisinis reguliavimas: daktaro disertacija. Vilnius: Mykolo Romerio universitetas, 2015.
81. Lessig, L. Code and other Laws of Cyberspace. New York (N.Y.): Basic books, 1999.
82. Lietuvos Respublikos civilinio kodekso komentaras. Antroji knyga. Asmenys. Mikelėnas, V., *et al.* Vilnius: Justitia, 2002.
83. Lietuvos Respublikos konstitucijos komentaras. Jovaišas, K. (ats. red.). Vilnius: Teisės institutas, 2000.
84. Linford, J. Improving Technology Neutrality through Compulsory Licensing. *Minnesota Law Review*, 2016, 100(126).
85. Linzer, P. From the Gutenberg Bible to Net Neutrality - How Technology Makes Law and Why English Majors Need to Understand It. *McGeorge Law Review*, 2008, 39.
86. Lyberis, A. Sinonimų žodynas. Vilnius: Lietuvos kalbos instituto leidykla, 2002.
87. Longman dictionary of Contemporary English. Summers, D. (edit. director). Berlin; München: Langenscheidt. Longman, 1987.

88. Madison, M. J. Authority and Authors and Codes. *The George Washington Law Review,* 2016, 84(6).
89. Madison, M. J. Rights of Access and the Shape of the Internet. *Boston College Law Review*, 2003, 44(2).
90. Manson, N. C.; O'Neill, O. Rethinking Informed Consent in Bioethics. Cambridge, *et al.* Cambridge University Press, 2007.
91. Marcinauskaitė, R. Nusikalstamomis veikomis elektroninėje erdvėje pažeidžiamos pagrindinės baudžiamojo įstatymo saugomos vertybės nustatymo problema. *Socialinių mokslų studijos*, 2011, 3(3).
92. Marcinauskaitė, R. Nusikalstamos veikos elektroninių duomenų ir informacinių sistemų konfidencialumui (Lietuvos Respublikos baudžiamojo kodekso 198 ir 198[1]) straipsniai: daktaro disertacija. Vilnius: Mykolo Romerio universitetas, 2014.
93. Marcinauskaitė, R. Technologinio neutralumo principo taikymo problemos aiškinant nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui sudėties požymius. *Socialinių mokslų studijos,* 2013, 5(1).
94. Mazurov, V. A. Kompiuternye prestuplenija: klasifikacija i sposoby protivodeistvija [Computer crime: classification and ways of countraction]. Moskva: Paletip, 2002.
95. McClure, S., *et al.* Apsauga nuo hakerių: tinklo saugumo palaikymo paslaptys ir sprendimai. Kaunas: Smaltija, 2006.
96. Mitra, A. From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces. *Journal of Computer – Mediated Communication,* 2001, 7(1).
97. Naumov, A. V. Rossijskoe ugolovnoe pravo: kurs lekcij [Russian criminal law: the course of lectures]. 4-asis leidimas. Moskva: Volters Kluver, 2007.
98. None-State Actors as Standard Setters. Peters, A.; Koechlin, L., *et al.* (eds). Cambridge: Cambridge University Press, 2009.
99. Ohm, P. The Arguments against Technology–Neutral Surveillance Laws. *Texas Law Review*, 2010, 88(7).
100. Panomariovas, A. Viešai neskelbiama informacija (paslaptis) baudžiamajame procese: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: Lietuvos teisės universitetas, 2001.
101. Panomariovas, A. Asmens privataus gyvenimo paslaptis ir su ja susijusios problemos baudžiamajame procese. *Jurisprudencija*, 2001, 23(15).
102. Paulauskas, K. V. Aiškinamasis kompiuterijos terminų santrumpų žodynas. Kaunas: Technologija, 2000.

103. Pavilonis, V. Baudžiamosios teisės normų konkurencija. *Teisės problemos*, 1996, 2(12): 38.
104. Piesliakas, V. Grobimas įsibraunant į butą, patalpą ar kitokią saugyklą. *Socialistinė teisė,* 1984, Nr. 1.
105. Pikelis, A. Baudžiamosios teisėkūros labirintai: Lietuvos Aukščiausiojo Teismo senato nutarimas ir teismų praktika taikant Baudžiamojo kodekso 178 ir 180 straipsnius. Vilnius: Petro ofsetas.
106. Plėštys, R., *et al.* Tinklų sauga. Kaunas: Vitae Litera, 2008.
107. Potter, R. T., *et al.* Introduction to Information Systems: Supporting and Transforming Business. John Wiley & Sons, Inc., 2007.
108. Pranka, D. Nusikalstamos veikos ir civilinės teisės pažeidimo atribojimo koncepcija Lietuvos baudžiamojoje teisėje: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: MRU, 2012.
109. Reed, C. Internet: law text and materials. Cambridge: Cambridge University Press, 2004.
110. Reed, C. Online and Offline Equivalence: Aspiration and Achievement. *International Journal of Law and Information Technology,* 2010, 18(3).
111. Reed, C. Taking Sides on Technology Neutrality. *SCRIPTed*, 2007, 4(3).
112. Reed, D. Should the English Legal System adopt the US Law of Cyber–Trespass? *SCRIPTed*, 2011, 8(1).
113. Regulating Technologies. Brownsword, R.; Yeung, K. (eds). Oxford; Portland (Or.): Hart Publishing, 2008.
114. Richardson, V. J.; Chang, C. J.; Smith, R. Accounting information systems. New York (N.Y.): McGraw-Hill : Education, 2014.
115. Rossijskoe ugolovnoe pravo: v dvukh tomakh: uchebnik [Russian criminal law: In two volumes: The textbook]. Rarog, A. I. (red). 5-asis pataisytas ir papildytas leidimas. Moskva: Proftekhobrazobanie, 2005.
116. Saulis, A.; Vasilecas, O. Informacinių sistemų projektavimo metodai: mokomoji knyga. Vilnius: Technika, 2008.
117. Sauliūnas, D. Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime. *Jurisprudencija,* 2010, 4(122).
118. Schellekens, M. What holds Off-Line, also holds On-Line? [interaktyvus. Žiūrėta 2018-04-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=952275*>.
119. Sciglimpaglia, R. J. Computer Hacking: A Global Offense. *Pace International Law Review*, 1991, 3(199).
120. Seeds of Disaster, Roots of Response: How Private Actions Can Reduce Public Vulnerability. Auerswald, P. E., *et al.* (eds). Cambridge: Cambridge University Press, 2006.

121. Sinkevičius, E. Neteisėtas banko kredito gavimas arba panaudojimas ir jų kvalifikavimas. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002.
122. Skersys, G. Informacijos sauga: mokomoji knyga. Kaunas: TEV [i.e. Technologija], 2011.
123. Skyrius, R.; Mikalauskienė, A.; Zalieckaitė, L. Informacijos ir komunikacijos technologijos. Vilnius: Vilniaus spauda, 2008.
124. Statutes. *NYU Law Review,* 2003, 78(5).
125. Stoneburner, G. Underlying Technical Models for Information Technology Security: recomendations of the National Institute of Standards and Technology [interaktyvus. Žiūrėta 2018-07-06]. Prieiga per internetą: <*http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf*>.
126. Sumit, K.; Nishit, N.; Sumita, N. Communication networks: principles and practice. New York: McGraw-Hill, 2007.
127. Štitilis, D. Elektroniniai nusikaltimai. Vilnius: Mykolo Romerio universitetas, 2011.
128. Štitilis, D. Teisinės atsakomybės pagrindų nustatymo už neteisėtas veikas elektroninėje erdvėje problemos: daktaro disertacija: socialiniai mokslai, teisė (01 S). Vilnius: LTU, 2002.
129. Štitilis, D., *et al.* Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai. Vilnius: Mykolo Romerio universitetas, 2011.
130. Štitilis, D.; Kiškis, M.; Limba, T., *et al.* Interneto ir technologijų teisė: vadovėlis. Vilnius: Registrų centras, 2016.
131. Štitilis, D.; Laurinaitis, M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*, 2009, 50.
132. Švedas, G. Baudžiamosios politikos pagrindai ir tendencijos Lietuvos Respublikoje. Vilnius: Teisinės informacijos centras, 2006.
133. Švedas, G. Veikos kriminalizavimo kriterijai: teorija ir praktika. *Teisė*, 2012, 82.
134. Tarptautinių žodžių žodynas. Sud. Bendorienė, A., *et al.* Ats. red. Kinderys, A. Vilnius: Alma littera, 2001.
135. Technikos enciklopedija. II tomas. Redaktorių taryba: pirmininkas Zavadskas, E. K., *et al.* Vilnius: Mokslo ir enciklopedijų leidybos institutas, 2003.
136. The History of Information Security: A Comprehensive Handbook. Leeuw, D. K.; Bergstra, J. (eds). Amsterdam, *et al.*: Elsevier, 2007.
137. Tompkins, Jr.; Mar, L. A. The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem, *Computer Law Journal*, 1986, 6(3).

138. Ugalovnoe pravo Rossijskoj Federacii. Osobennaja chast: uchebnik [Criminal Law of the Russian Federation. Special part: The textbook]. Inogamova-Khega, L. V.; Rarog, A. I.; Chuchaeva, A. I. (red.) Moskva: INFRA-M: KONTRAKT, 2005.
139. Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik [Russian criminal law. Special Part: The textbook]. Revina, V. P. 2-asis pataisytas ir papildytas leidimas. Moskva: Justicinform, 2010.
140. Ugolovnoe pravo Rossii. Osobennaja chast: uchebnik [Russian criminal law. Special Part: Textbook]. Borzenkova, G. N.; Komissarova, V. S. (red.), Moskva: Zercalo-M, 2005.
141. Vaitkevičiūtė, V. Tarptautinių žodžių žodynas. 4-asis pataisytas ir papildytas leidimas. Vilnius: Žodynas, 2007.
142. Van der Haar, I. M. Technological Neutrality: What Does It Entail? [interaktyvus. Žiūrėta 2018-07-05]. Prieiga per internetą: <*http://papers.ssrn.com/sol3/papers.cfm?abstract_id=985260*>.
143. Venčkauskas, A.; Toldinas, J. Kompiuterių ir operacinių sistemų sauga. Kaunas: Vitae Litera, 2008.
144. Vetrov, N. I. Ugolovnoe pravo. Osobennaja chast: uchebnik [Criminal law. Special Part: Textbook]. 2-oe izd. Moskva: JUNITI-DANA: Zakon i pravo, 2002.
145. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Computers & security*, 2013, 38.
146. Wacks, P. Personal Information: Privacy and the Law. Oxford: Clarendon Press, 1989.
147. Walden, I. Computer Crimes and Digital Investigations. Oxford: Oxford University Press, 2007.
148. Webster, M. Data protection in the financial services industry. Aldershot; Burlington (Vt.): Gower, 2006.
149. Whitman, M. E., *et al*. Principles of information security. 3-ioji laida. Boston: Thomson: Course Technology, 2009.
150. Wong, M. W. S. Cyber-trespass and "Unauthorized Access" as Legal Mechanism of Access Control: Lessons from the US Experience. *International Journal of Law and Information Technology*, 2006, 15(1).
151. Žėkas, T. Vaiko išnaudojimas pornografijai: baudžiamieji teisiniai ir kriminologiniai aspektai: daktaro disertacija. Vilnius: Vilniaus universitetas, 2011.
152. Žilinskas, A.; Leonavičius, G.; Valavičius, E. Informatika. Vilnius: Aldorija, 2000.

Lietuvos teismų praktika

1. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2018 m. gegužės 31 d. nutartis baudžiamojoje byloje Nr. 2K-7-84-489/2018.
2. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2018 m. sausio 9 d. nutartis baudžiamojoje byloje Nr. 2K-56-696/2018.
3. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2018 m. vasario 6 d. nutartis baudžiamojoje byloje Nr. 2K-9-719/2018.
4. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus išplėstinės septynių teisėjų kolegijos 2018 m. gegužės 31 d. nutartis baudžiamojoje byloje Nr. 2K-7-84-489/2018.
5. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2017 m. birželio 13 d. nutartis baudžiamojoje byloje Nr. 2K-161-696/2017.
6. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2016 m. sausio 26 d. nutartis baudžiamojoje byloje Nr. 2K-4-507/2016.
7. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2016 m. gruodžio 20 d. nutartis baudžiamojoje byloje Nr. 2K-424-696/2016.
8. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2015 m. sausio 6 d. nutartis baudžiamojoje byloje Nr. 2K-138/2015.
9. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2014 m. vasario 11 d. nutartis baudžiamojoje byloje Nr. 2K-57/2014.
10. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2014 m. gruodžio 9 d. nutartis baudžiamojoje byloje Nr. 2K-508/2014.
11. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2013 m. gruodžio 10 d. nutartis baudžiamojoje byloje Nr. 2K-508/2013.
12. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus išplėstinės septynių teisėjų kolegijos 2013 m. spalio 10 d. nutartis baudžiamojoje byloje Nr. 2K-7-251/2013.
13. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2012 m. gegužės 8 d. nutartis baudžiamojoje byloje Nr. 2K-P-78/2012.

14. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2012 m. birželio 26 d. nutartis baudžiamojoje byloje Nr. 2K-375/2012.
15. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. balandžio 5 d. nutartis baudžiamojoje byloje Nr. 2K-159/2011.
16. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. balandžio 19 d. nutartis baudžiamojoje byloje Nr. 2K-162/2011.
17. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2011 m. gruodžio 6 d. nutartis baudžiamojoje byloje Nr. 2K-482/2011.
18. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. balandžio 27 d. nutartis baudžiamojoje byloje Nr. 2K-263/2010.
19. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gegužės 11 d. nutartis baudžiamojoje byloje Nr. 2K-185/2010.
20. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 7 d. nutartis baudžiamojoje byloje Nr. 2K-555/2010.
21. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2010 m. gruodžio 21 d. nutartis baudžiamojoje byloje Nr. 2K-560/2010.
22. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. kovo 31 d. nutartis baudžiamojoje byloje Nr. 2K-76/2009.
23. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2009 m. gegužės 5 d. nutartis baudžiamojoje byloje Nr. 2K-104/2009.
24. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus plenarinės sesijos 2009 m. spalio 20 d. nutartis baudžiamojoje byloje Nr. 2K-P-218/2009.
25. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2008 m. gruodžio 9 d. nutartis baudžiamojoje byloje Nr. 2K-368/2008.
26. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2007 m. kovo 20 d. nutartis baudžiamojoje byloje Nr. 2K-123/2007.
27. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. balandžio 25 d. nutartis baudžiamojoje byloje Nr. 2K-396/2006.

28. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. gegužės 30 d. nutartis baudžiamojoje byloje Nr. 2K-330/2006.
29. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2006 m. sausio 24 d. nutartis baudžiamojoje byloje Nr. 2K-86/2006.
30. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegijos 2001 m. spalio 9 d. nutartis baudžiamojoje byloje Nr. 2K-682/2001.
31. Kauno apygardos teismo 2017 m. rugsėjo 27 d. nuosprendis baudžiamojoje byloje Nr. N1-173-319/2017.
32. Kauno apygardos teismo 2017 m. gruodžio 4 d. nuosprendis baudžiamojoje byloje Nr. 1-284-594/2017.
33. Kauno apygardos teismo 2015 m. gegužės 7 d. nutartis baudžiamojoje byloje Nr. 1A-432-594/2015.
34. Klaipėdos apygardos teismo 2018 m. kovo 1 d. nutartis baudžiamojoje byloje Nr. 1A-9-651/2018.
35. Klaipėdos apygardos teismo 2017 m. spalio 12 d. nutartis baudžiamojoje byloje Nr. 1A-279-651/2017.
36. Klaipėdos apygardos teismo 2015 m. vasario 19 d. nuosprendis baudžiamojoje byloje Nr. 1A-38-255/2015.
37. Klaipėdos apygardos teismo 2017 m. spalio 12 d. nutartis baudžiamojoje byloje Nr. 1A-279-651/2017.
38. Panevėžio apygardos teismo 2015 m. sausio 29 d. nuosprendis baudžiamojoje byloje Nr. 1A-23-366/2015.
39. Šiaulių apygardos teismo 2014 m. gegužės 7 d. nuosprendis baudžiamojoje byloje Nr. 1A-388-309/2014.
40. Vilniaus apygardos teismo 2017 m. gegužės 15 d. nuosprendis baudžiamojoje byloje Nr. 1-101-190/2017.
41. Vilniaus apygardos teismo 2014 m. birželio 5 d. nutartis baudžiamojoje byloje Nr. 1A-459-209/2014.
42. Vilniaus apygardos teismo 2011 m. gruodžio 23 d. nuosprendis baudžiamojoje byloje Nr. 1A-977/2011.
43. Kauno apylinkės teismo 2018 m. sausio 22 d. nuosprendis baudžiamojoje byloje Nr. 1-29-673/2018.
44. Kauno apylinkės teismo 2018 m. vasario 28 d. teismo baudžiamasis įsakymas byloje Nr. 1-1154-825/2018.
45. Kauno apylinkės teismo 2017 m. kovo 24 d. nuosprendis baudžiamojoje byloje Nr. 1-234-825/2017.
46. Kauno apylinkės teismo 2013 m. birželio 7 d. nuosprendis baudžiamojoje byloje Nr. 1-680-530/2013.

47. Klaipėdos miesto apylinkės teismo 2009 m. birželio 29 d. teismo baudžiamasis įsakymas byloje Nr. 1-740-93/2009.
48. Klaipėdos miesto apylinkės teismo 2009 m. liepos 1 d. teismo baudžiamasis įsakymas byloje Nr. 1-770-795/2009.
49. Šiaulių apylinkės teismo 2018 m. kovo 5 d. nuosprendis baudžiamojoje byloje Nr. 1-506-771/2018.
50. Šiaulių apylinkės teismo 2017 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-148-771/2017.
51. Šiaulių apylinkės teismo 2017 m. gruodžio 7 d. teismo baudžiamasis įsakymas byloje Nr. 1-995-899/2017.
52. Šiaulių apylinkės teismo 2016 m. gruodžio 21 d. nuosprendis baudžiamojoje byloje Nr. 1-957-771/2016.
53. Šiaulių miesto apylinkės teismo 2011 m. liepos 18 d. teismo baudžiamasis įsakymas byloje Nr. 1-617-885/2011.
54. Vilniaus miesto apylinkės teismo 2018 m. kovo 15 d. nuosprendis baudžiamojoje byloje Nr. 1-782-506/2018.
55. Vilniaus miesto apylinkės teismo 2013 m. sausio 25 d. nuosprendis baudžiamojoje byloje Nr. 1-258-716/2013.
56. Vilniaus miesto 1 apylinkės teismo 2011 m. gruodžio 6 d. nuosprendis baudžiamojoje byloje Nr. 1-1430-276/2011.
57. Vilniaus miesto 1 apylinkės teismo 2011 m. kovo 25 d. nuosprendis baudžiamojoje byloje Nr. 1-68-203/2011.
58. Vilniaus miesto 2 apylinkės teismo 2011 m. liepos 1 d. nuosprendis baudžiamojoje byloje Nr. 1-188-387/2011.
59. Vilniaus miesto 3 apylinkės teismo 2010 m. sausio 27 d. nuosprendis baudžiamojoje byloje Nr. 1-182-498/10.
60. Vilniaus miesto 1 apylinkės teismo 2010 m. kovo 5 d. teismo baudžiamasis įsakymas byloje Nr. N1-724-276/2010.
61. Vilniaus miesto 2 apylinkės teismo 2009 m. gegužės 27 d. teismo baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-515-487/2009.
62. Vilniaus miesto 1 apylinkės teismo 2009 m. rugsėjo 14 d. teismo baudžiamasis įsakymas baudžiamojoje byloje Nr. N1-1470-88/2009.
63. Vilniaus miesto 2 apylinkės teismo 2008 m. liepos 2 d. nuosprendis baudžiamojoje byloje Nr. 1-5-655/2008.
64. Alytaus rajono apylinkės teismo 2017 m. gegužės 22 d. nuosprendis baudžiamojoje byloje Nr. 1-68-297/2017.
65. Kupiškio rajono apylinkės teismo 2009 m. rugsėjo 2 d. nuosprendis baudžiamojoje byloje Nr. 1-53-100/2009.
66. Kėdainių rajono apylinkės teismo 2017 m. rugsėjo 28 d. teismo baudžiamasis įsakymas byloje Nr. 1-308-188/2017.

67. Mažeikių rajono apylinkės teismo 2009 m. rugpjūčio 12 d. nuosprendis baudžiamojoje byloje Nr. 1-188-785/2009.
68. Radviliškio rajono apylinkės teismo 2010 m. kovo 22 d. teismo baudžiamasis įsakymas baudžiamojoje byloje Nr. 1-116-632/2010.
69. Raseinių rajono apylinkės teismo 2017 m. kovo 22 d. nuosprendis baudžiamojoje byloje Nr. 1-9-237/2017.
70. Šakių rajono apylinkės teismo 2015 m. birželio 18 d. nuosprendis baudžiamojoje byloje Nr. 1-21-829/2015.
71. Šiaulių rajono apylinkės teismo 2010 m. liepos 19 d. teismo baudžiamasis įsakymas byloje Nr. 1-199-776/2010.
72. Šilalės rajono apylinkės teismo 2010 m. lapkričio 4 d. teismo baudžiamasis įsakymas byloje Nr. 1-121-799/2010.
73. Šilutės rajono apylinkės teismo 2015 m. sausio 9 d. nuosprendis baudžiamojoje byloje Nr. 1-20-351/2015.
74. Šilutės rajono apylinkės teismo 2006 m. birželio 28 d. nuosprendis baudžiamojoje byloje Nr. N1- 249-299/2005.
75. Tauragės rajono apylinkės teismo 2017 m. birželio 15 d. nuosprendis baudžiamojoje byloje Nr. 1-70-607/2017.
76. Ukmergės rajono apylinkės teismo 2012 m. gruodžio 17 d. teismo baudžiamasis įsakymas byloje Nr. 1-312-627/2012.
77. Vilniaus rajono apylinkės teismo 2009 m. rugsėjo 8 d. nuosprendis baudžiamojoje byloje Nr.1-278-298/2009.

Praktikos apibendrinimai ir metodinės analizės

1. 2016 m. balandžio 28 d. Teismų praktikos nagrinėjant baudžiamąsias bylas dėl sudėtingų pavienių nusikalstamų veikų ir nusikalstamų veikų sutapčių apžvalga. *Teismų praktika,* 2016, Nr. 44.
2. 2015 m. kovo 19 d. Teismų praktikos turto pasisavinimo ir turto iššvaistymo baudžiamosiose bylose apžvalga (BK 183 ir 184 straipsniai). *Teismų praktika,* 2015, Nr. 42.
3. Lietuvos Aukščiausiojo Teismo senato 2005 m. birželio 23 d. nutarimas Nr. 52 „Dėl teismų praktikos vagystės ir plėšimo baudžiamosiose bylose“. *Teismų praktika,* 2005, Nr. 23.
4. Lietuvos Aukščiausiojo Teismo senato 2005 m. gruodžio 29 d. nutarimas Nr. 55 „Dėl teismų praktikos nusikalstamų veikų finansų sistemai baudžiamosiose bylose (BK 214, 215, 219, 220, 221, 222, 223 straipsniai)“. *Teismų praktika*, 2005, Nr. 24.

Užsienio valstybių teismų praktika

1. *United States v. Bradford C. Councilman*, no. 03-1383, United States Court of Appeals, 1st Circuit, 2005 [interaktyvus. Žiūrėta 2018-07-24]. Prieiga per internetą: <*http://media.ca1.uscourts.gov/cgi-bin/getopn.pl?OPINION=03-1383EB.01A*>.
2. *United States v. Mitra*, no. 04-2328, April 18, 2005-US 7th Cir. [interaktyvus. Žiūrėta 2018-04-14]. Prieiga per internetą: <*http://caselaw.findlaw.com/us-7th-circuit/1031818.html*>.
3. *Briggs v. State of Maryland*, no. 24, Court of Appeals of Maryland, 1997 [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://law.justia.com/cases/maryland/court-of-appeals/1998/24a97-2.html*>.
4. *State of Kansas v. Anthony A. Allen*, no. 74,639, Soupreme Court of Kansas, 1996 [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://files.grimmelmann.net/cases/Allen.pdf*>.
5. *United States v. Morris*, no. 774, United States Court of Appeals, 2nd Circuit, 1991 [interaktyvus. Žiūrėta 2018-07-13]. Prieiga per internetą: <*http://www.loundy.com/CASES/US_v_Morris2.html*>.

Kiti šaltiniai

1. ISO/IEC 2382-1:1996 *Informacijos technologijos. Terminai ir apibrėžimai. 1-oji laida. Pagrindiniai terminai.*
2. LST ISO/IEC 27001:2006 *Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai*.

Protection of confidentiality of electronic data and information systems in criminal law

RENATA MARCINAUSKAITĖ

ABSTRACT OF THE MONOGRAPH

The development of computer IT in its broadest sense opened up an avenue for the dissemination of large datasets and new methods for accessing data; broadened the functioning and use of these technologies; and necessitated a closer look at the aspects of global transformation in the attempt to predict potential prospects of such development. These technologically and legally complex processes are related not only to a positive connection and interactions of cyberspace users (or processes) but also to the issues of vulnerability of information society. The cyberspace, although it seems distant from the physical space by its parameters, cannot avoid various threats to which legal values are exposed, including the emergence of criminal offences which are new by their nature or modified as a result of IT use. The monograph provides a study of one of the groups of criminal offences against security of electronic data and information systems as provided for in Chapter XXX of the Criminal Code of the Republic of Lithuania (hereinafter – the CC) – criminal offences against confidentiality of electronic data and information systems, as well as explores the issues of their criminal legal assessment. The offences of unlawful interception and use of electronic data (Article 198 of the CC) and illegal access to an information system (Article 198^1 of the CC) have been distinguished as a result of structuring of the criminal offences provided for in Chapter XXX of the CC: through the *CIA triad* they were researched as violations of confidentiality, integrity and availability.

A synthesis between IT developments and scope for criminal offences shows a large number of qualitatively new issues of criminal law arising in the protection of various legal goods – existing only in the cyberspace or others, 'moved' here from the physical space. Due to a large number of issues, which are new by their nature and should be discussed, the study of the criminal offences under this research

was not limited only to the analysis of their elements, identification of the existing legal regulation and formulation of the directions for interpreting these offence elements on this basis; violations of confidentiality of electronic data and information systems were studied in a wider context from the perspective of criminal law. The monograph explored the root causes of the criminal offences of this nature, the possibilities of their systematisation, the justification of criminalisation, their potential link with traditional offences, the criteria for delimiting them from other similar criminal offences. When formulating the principle approach to the interpretation of these offences, the issues of approximation of the terminology used in technologies and in criminal law in order to identify such technologies as well as the applicability of the principles developed outside criminal law were many times addressed. The analysis of the issues studied in the monograph is based on technology neutral approach, which aims at making it possible to adapt potential solutions of criminal legal problems both to the present-day and future technologies (to the extent that is possible due to the difficulties of forecasting technological developments).

The preconditions for analysing criminal offences against confidentiality of electronic data and information systems on the national level were created by the entry into force of the 2000 CC, which introduced *sui generis* criminalisation of the new offences that emerged with technology developments and no longer treated such offences as constituents of other offences. The introduction of such criminal offences in the CC brought about fundamental problems in legislation and in the application (and, accordingly, interpretation) of the criminal law provisions. These issues and their solutions remain relevant to date, in particular considering the absence of more extensive discussions concerning the established regulation and its suitability in Lithuania. Moreover, the time that has passed after the entry into force of the 2000 criminal law is more than enough to explore and identify the effectiveness of the established legal regulation, find out whether the provisions defining liability for criminal offences against confidentiality of electronic data and information systems are adequate and understandable, whether they have achieved the expected results and what the real result of their application is.

This monograph is the continuation of author's dissertation research – it has been updated in the light of the most recent amendments of the criminal law and case law developments, identifies newly emerging problems and potential solutions. The monograph provides a study of criminal offences against confidentiality of electronic data and information systems: explores the aspects of the elements of these offences which have not yet been researched in the doctrine of Lithuanian criminal law, speaks about the impact of technological/legal problems on the interpretation and incrimination of offences, provides a systemic analysis of the legal instruments adopted on the international and EU level and discusses the provisions of foreign and Lithuanian criminal law. Based on the analysis of these criminal offence elements, the criteria have been developed for delimiting criminal offences against confidentiality of electronic data and information systems and similar criminal offences. The attention is also drawn to the scope for and issues of application of the principle of technological neutrality and equivalence assessment in the context of criminal law. The research is not limited to the level of theory – the analysis of these criminal offences is underpinned by case law and its synthesis supports the specific offence qualification issues identified and the potential solutions offered. Moreover, the research also includes the relevant case law of foreign courts – the cases studied helped identify the problematic aspects unknown in Lithuania yet in relation to criminal offences against confidentiality of electronic data and information systems.

Criminal offences against confidentiality of electronic data and information systems have not been researched extensively and the elements of these criminal offences have not been in principle analysed in Lithuania. The topic of offences in the cyberspace in general with reference to the effective CC of 1961 and after the entry into force of the 2000 CC was explored by Darius Štitilis. The dissertation defended by this scholar in 2002 – 'Responsibility for Illegal Acts in Cyberspace' – and his later works paid considerable attention to the interpretation of such offences. These criminal offences (although at the time when the criminal law of 1961 was still in force) were also researched by Rimantas Petrauskas. After the CC of 2000 came into force, some issues of interpretation of criminal offences in the elec-

tronic space were discussed in educational publications (textbooks). The topic of harmonisation of criminal law with international legal acts in the area of regulation of electronic criminal offences was explored by Darius Sauliūnas. Some aspects of these offences and their investigation methodologies have been also discussed by Nikolaj Goranin and Dalius Mažeika. Mention should also be made of the commentary to criminal law which provides a concise theoretical interpretation of the offences violating the confidentiality of electronic data and information systems. Recently scientific literature started paying more attention to the issues of criminalisation of identify theft on the cyberspace, which is the object of interest of Darius Štitilis, Paulius Pakutinskas, Marius Laurinaitis and Inga Dauparaitė.

Different aspects of criminal offences against the security of electronic data and information systems and, in general, criminal offences in the cyberspace have been to a greater extent researched by foreign scholars of criminal law. The issues of criminalisation and interpretation of cybercrime of general nature and assessment of behaviour online were researched in the works of Jonathan Clough, Ian Walden, Chris Reed, Uta Kohl, Susan W. Brenner, Maurice Schellekens, Rajab Ali, Ilse M. van der Haar, Bert-Jaap Koops, Richard W. Downing, Paul Ohm and others. Criminalisation and incrimination of unauthorised access to information systems or electronic data, and also the interpretation of such criminal offences has been discussed by Orin S. Kerr, Mary W. S. Wong, Michael J. Madison, Ian Walden, David Bainbridge, John Angel, Jonathan Clough, Beryl A. Howell, Anthony S. Blunn, Diane Rowland, Elizabeth Macdonald.

The monograph consists of the following four chapters: Chapter I *Criminalisation, systematisation and interpretation of criminal offences in the cyberspace* discusses general aspects of criminal offences committed in the cyberspace in relation to the identification of values protected by criminal law, scope for and issues of application of the principles of equivalence assessment and technological neutrality in criminal law.

Chapter II *Illegal Access to an Information System (Article 198[1] of the CC)* explores the objective and subjective elements of this criminal offence against confidentiality of information systems, discusses the potential prospects of legal assessment of such offences.

Chapter III *Unlawful Interception and Use of Electronic Data (Article 198 of the CC)* analyses the elements of criminal offences which violate the confidentiality of non-public electronic data, discusses the 'scope' of criminalisation of this criminal offence and eventual issues of its interpretation and incrimination.

Chapter IV *Delimitation of criminal offences against confidentiality of electronic data and information systems and similar criminal offences* formulates the criteria for delimiting the criminal offences studied in the monograph and criminal offences against the financial system (Articles 214 and 215 of the CC) as well as criminal offences against inviolability of a person's private life (Article 166 of the CC).

RENATA MARCINAUSKAITĖ

NUSIKALSTAMOS VEIKOS ELEKTRONINĖJE ERDVĖJE

Elektroninių duomenų ir informacinių sistemų konfidencialumo apsauga baudžiamojoje teisėje

Monografija

Išleido VĮ Registrų centras
Redagavo Jūratė Juknevičiūtė
Maketavo Janina Kaminskaitė
Parengė leidybai Algis Švedas

SL 1613. 2019-04-05. 18 sąlyginių spaudos lankų
Tiražas 500 egz. Užsakymo Nr.

VĮ Registrų centro Teisinės informacijos departamentas
Tilto g. 17, 01101 Vilnius
tel./faksas (8 5) 261 2806
www.teisineliteratura.lt, *leidyba@teisineliteratura.lt*

Spausdino STANDARTŲ SPAUSTUVĖ
S. Dariaus ir S. Girėno g. 39, 02189 Vilnius

Kaina sutartinė

MYKOLO ROMERIO UNIVERSITETAS

2000-aisiais įsigaliojus Lietuvos Respublikos baudžiamajam kodeksui, kuriame dėl technologijų pokyčių atsiradusios naujos veikos buvo kriminalizuotos sui generis ir nebelaikomos kitų veikų sudedamąja dalimi, atsirado sąlygos jas analizuotinacionaliniu lygiu. Monografijoje tiriama viena iš Baudžiamojo kodeksoXXX skyriuje įtvirtintų nusikalstamų veikų elektroninių duomenų ir informacinių sistemų saugumui rūšių – nusikalstamos veikos, kuriomis pažeidžiamas elektroninių duomenų ir informacinių sistemų konfidencialumas, aptariamos jų baudžiamojo teisinio vertinimo problemos.Stengiamasi ieškoti tokių nusikalstamų veikų ištakų, jų sisteminimo galimybių, atskyrimo nuo kitų panašių veikų kriterijų. Monografija svarbi baudžiamosios teisės srityje dirbantiems teisininkams.

ISBN 978-9955-30-282-7